



Junos[®] OS

Broadband Subscriber Sessions Feature Guide

Release

14.1



Modified: 2016-05-11

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

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.

Junos[®] OS Broadband Subscriber Sessions Feature Guide

14.1

Copyright © 2016, Juniper Networks, Inc.
All rights reserved.

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	xxxv
	Documentation and Release Notes	xxxv
	Supported Platforms	xxxv
	Using the Examples in This Manual	xxxv
	Merging a Full Example	xxxvi
	Merging a Snippet	xxxvi
	Documentation Conventions	xxxvii
	Documentation Feedback	xxxix
	Requesting Technical Support	xxxix
	Self-Help Online Tools and Resources	xxxix
	Opening a Case with JTAC	xl
Part 1	Configuring AAA for Subscriber Management	
Chapter 1	AAA and RADIUS for Subscriber Access Overview	3
	AAA Service Framework Overview	3
	RADIUS Server Options for Subscriber Access	4
	Global RADIUS Options for Subscriber Access	7
	Subscriber Access Interface Description Storage and Reporting Through RADIUS	
	Overview	7
	Interface Description Precedence	8
	Example: Reporting Interface Descriptions on Non-Underlying Logical	
	Interfaces	8
	Reporting Interface Descriptions on Underlying Logical Interfaces	9
	Interface Descriptions on Aggregated Ethernet Physical Interfaces	10
	Interface Descriptions on a Combination of Dynamic and Static	
	Interfaces	10
	Example: Reporting Interface Descriptions on Dynamic VLANs	10
Chapter 2	Configuring RADIUS Attributes and Juniper Networks VSAs	13
	RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service	
	Framework	13
	RADIUS IETF Attributes Supported by the AAA Service Framework	14
	Juniper Networks VSAs Supported by the AAA Service Framework	21
	AAA Access Messages and Supported RADIUS Attributes and Juniper Networks	
	VSAs for Junos OS	31
	AAA Accounting Messages and Supported RADIUS Attributes and Juniper	
	Networks VSAs for Junos OS	37
	Configuring How RADIUS Attributes Are Used for Subscriber Access	40
	Junos OS Predefined Variables That Correspond to RADIUS Attributes and	
	VSAs	46

	DSL Forum Vendor-Specific Attributes	51
	DSL Forum VSAs Support in AAA Access and Accounting Messages for Junos OS	53
Chapter 3	Configuring RADIUS NAS-Port Attributes and Options	55
	Manual Configuration of the NAS-Port-ID RADIUS Attribute	55
	Configuring a NAS-Port-ID with Additional Options	56
	Configuring a Calling-Station-ID with Additional Attributes	58
	RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN Overview	60
	NAS-Port-Type RADIUS Attribute	60
	NAS-Port RADIUS Attribute	60
	NAS-Port Options Configuration and Subscriber Network Access Models	61
	NAS-Port Options Definition	61
	Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN	62
	Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN	63
	Manual Configuration of the NAS-Port-Type RADIUS Attribute	64
	Configuring the RADIUS NAS-Port-Type per Physical Interface	66
	Configuring the RADIUS NAS-Port-Type per VLAN	68
	Configuring the RADIUS NAS-Port-Type per Stacked VLAN	69
	Configuring the RADIUS NAS-Port Extended Format per Physical Interface	71
	Configuring the RADIUS NAS-Port Extended Format per VLAN	72
	Configuring the RADIUS NAS-Port Extended Format per Stacked VLAN	74
	Configuring the RADIUS NAS-Port Extended Format for ATM Interfaces	76
Chapter 4	Configuring RADIUS Authentication for Subscriber Access	79
	Retaining Authentication and Accounting Information During Session Startup	79
	Configuring Authentication and Accounting Parameters for Subscriber Access	80
	Specifying the Authentication and Accounting Methods for Subscriber Access	80
	Specifying RADIUS Authentication and Accounting Servers for Subscriber Access	81
	Example: Configuring RADIUS-Based Subscriber Authentication and Accounting	82
Chapter 5	Configuring RADIUS Accounting for Subscriber Access	85
	RADIUS Accounting Statistics for Subscriber Access Overview	85
	Understanding RADIUS Accounting Duplicate Reporting	87
	Layer 3 Wholesale Scenarios	87
	Other Scenarios	88
	Preservation of RADIUS Accounting Information During an Accounting Server Outage	88
	RADIUS Acct-On and Acct-Off Messages	91
	Configuring Per-Subscriber Session Accounting	92
	Configuring Per-Service Session Accounting	94

	Configuring Service Packet Counting	95
	Configuring Back-up Options for RADIUS Accounting	97
Chapter 6	Configuring Routers and RADIUS Servers for Subscriber Access	99
	Configuring Router or Switch Interaction with RADIUS Servers	99
	Forcing the Router to Contact the Accounting Server Immediately	101
	Configuring RADIUS Server Parameters for Subscriber Access	102
	Configuring RADIUS Server Options for Subscriber Access	102
	Configuring RADIUS Options for Subscriber Access Globally	105
Chapter 7	Configuring Access Profiles for Subscriber Access	107
	Configuring an Access Profile for Subscriber Management	107
	Attaching Access Profiles	108
Chapter 8	Configuring Session Options for Subscriber Access	109
	Understanding Session Options for Subscriber Access	109
	Configuring Subscriber Session Options	111
	Removing Inactive Dynamic Subscriber VLANs	112
Chapter 9	Receiving DHCP Options From a RADIUS Server	113
	Centrally Configured Opaque DHCP Options	114
	Data Flow for RADIUS-Sourced DHCP Options	116
	Multiple VSA 26-55 Instances Configuration	117
	DHCP Options That Cannot Be Centrally Configured	117
	Monitoring DHCP Options Configured on RADIUS Servers	118
Chapter 10	Configuring RADIUS Logical Line Identification	121
	RADIUS Logical Line Identifier (LLID) Overview	121
	RADIUS Attributes for LLID Preauthentication Requests	122
	Configuring Logical Line Identification (LLID) Preauthentication	124
Chapter 11	Configuring Domain Maps for Subscriber Management	127
	Domain Mapping Overview	128
	Default Domain Map	129
	Domain Map for Subscriber Usernames With No Domain or Realm Name	129
	Understanding Domain Maps and Logical System/Routing Instance Contexts	130
	Configuring a Domain Map	131
	Specifying an Access Profile in a Domain Map	132
	Specifying an Address Pool in a Domain Map	133
	Specifying a Dynamic Profile in a Domain Map	133
	Specifying an AAA Logical System/Routing Instance in a Domain Map	134
	Specifying a Target Logical System/Routing Instance in a Domain Map	135
	Configuring Domain and Realm Name Usage for Domain Maps	136
	Specifying Domain and Realm Name Delimiters	136
	Specifying the Parsing Order for Domain and Realm Names	137
	Specifying the Parsing Direction for Domain and Realm Names	138
	Enabling Domain Name Stripping	139
	Specifying a Tunnel Profile in a Domain Map	139
	Specifying a Tunnel Switch Profile in a Domain Map	140

	Configuring PADN Parameters for a Domain Map	140
Chapter 12	Configuring Dynamic Service Activation for Subscriber Access	143
	Using RADIUS Dynamic Requests for Subscriber Access Management	143
	Dynamic Service Activation During Login Overview	144
	Configuring RADIUS-Initiated Dynamic Request Support	144
	RADIUS-Initiated Change of Authorization (CoA) Overview	145
	CoA Messages	145
	Qualifications for Change of Authorization	145
	Message Exchange	147
	Usage Thresholds for Subscriber Services	147
	RADIUS-Initiated Disconnect Overview	148
	Disconnect Messages	148
	Qualifications for Disconnect	149
	Message Exchange	149
	Error-Cause Codes (RADIUS Attribute 101) for Dynamic Requests	149
Chapter 13	Configuring Terminate Reasons for Protocols	151
	Mapping Application Terminate Reasons and RADIUS Terminate Codes	151
	Configuring Custom Terminate Reason Mappings	153
	AAA Terminate Reasons	154
	DHCP Terminate Reasons	155
	L2TP Terminate Reasons	156
	PPP Terminate Reasons	172
Chapter 14	Monitoring and Managing AAA Information for Subscriber Access	181
	Verifying and Managing Subscriber AAA Information	181
	Monitoring Pending RADIUS Accounting Stop Messages	182
	Verifying and Managing the RADIUS Dynamic-Request Feature	183
	Verifying and Managing Domain Map Configuration	183
	Verifying and Managing LLID Preauthentication Configuration	184
Part 2	Configuring DHCP for Subscriber Management	
Chapter 15	Using DHCP Overview	187
	Extended DHCP Local Server Overview	188
	Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools	190
	Providing DHCP Client Configuration Information	190
	Minimal Configuration for Clients	192
	DHCP Local Server and Address-Assignment Pools	192
	Extended DHCP Relay Agent Overview	194
	Interaction Among the DHCP Relay Agent, DHCP Client, and DHCP Servers	195
	DHCP Liveness Detection	196
	DHCP Relay Proxy Overview	197
	Interaction Among DHCP Relay Proxy, DHCP Client, and DHCP Servers	197
Chapter 16	Configuring Default Services That are Activated at Subscriber Login	199
	Default Subscriber Service Overview	199
	Configuring a Default Subscriber Service	200

Chapter 17	Assigning IP Addresses	201
	DHCP Attributes for Address-Assignment Pools	201
	Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use	203
	Assign a Specific IP Address to a Client Using DHCP Option 50 and DHCPv6 IA_NA Option	204
	Configuring DHCP Client-Specific Attributes Applied When Clients Obtain an Address	205
	Specifying the Subnet for DHCP Client Address Assignment	206
	Example: Extended DHCP Local Server Configuration with Optional Pool Matching	206
	DNS Address Assignment Precedence	207
Chapter 18	Configuring Lease Times for IP Addresses	209
	Configuring a DHCP Lease-Time Threshold	209
	DHCP Lease-Time Validation Overview	210
	DHCPv6 Lease Timers	212
Chapter 19	Requesting DHCP Client Configuration Information From an Address Pool	213
	DHCP Local Server Handling of Client Information Request Messages	213
	Enabling Processing of Client Information Requests	214
Chapter 20	Authenticating DHCP Clients Using An External AAA Authentication Service	217
	Using External AAA Authentication Services with DHCP	217
	Creating Unique Usernames for DHCP Clients	218
	Configuring Passwords for Usernames	221
Chapter 21	Grouping Interfaces and Applying a Common DHCP Configuration to the Group	223
	Grouping Interfaces with Common DHCP Configurations	223
	Guidelines for Configuring Interface Ranges for Groups of DHCP Interfaces	224
	Configuring Group-Specific DHCP Local Server Options	225
	Configuring Group-Specific DHCP Relay Options	226
	Example: Configuring DHCP and DHCPv6 Relay Agent Group-Level Selective Traffic Processing	227
Chapter 22	Configuring the Number of DHCP Clients Per Interface	233
	Specifying the Maximum Number of DHCP Clients Per Interface	233
	Allowing Only One DHCP Client Per Interface	234
Chapter 23	Maintaining Subscribers During Interface Delete Events	237
	Subscriber Binding Retention During Interface Delete Events	237
	Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events	238
	Verifying and Managing the DHCP Maintain Subscribers Feature	238

Chapter 24	Forcing Dynamic Reconfiguration of Clients From a DHCP Local Server	241
	Understanding Dynamic Reconfiguration of Extended DHCP Local Server	
	Clients	241
	Default Client/Server Interaction	241
	Dynamic Client/Server Interaction for DHCPv4	242
	Dynamic Client/Server Interaction for DHCPv6	242
	Manually Forcing the Local Server to Initiate the Reconfiguration Process	243
	Action Taken for Events That Occur During a Reconfiguration	243
	Configuring Dynamic Client Reconfiguration of Extended Local Server	
	Clients	244
	Configuring Dynamic Reconfiguration Attempts for DHCP Clients	246
	Configuring Deletion of the Client When Dynamic Reconfiguration Fails	247
	Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect	247
Chapter 25	Conserving IP Addresses Using DHCP Auto Logout	249
	DHCP Auto Logout Overview	249
	Auto Logout Overview	249
	How DHCP Identifies and Releases Clients	250
	Option 60 and Option 82 Requirements	251
	Automatically Logging Out DHCP Clients	251
	How DHCP Relay Agent Uses Option 82 for Auto Logout	252
Chapter 26	Overriding Default DHCP Local Server Configuration Settings	255
	Overriding Default DHCP Local Server Configuration Settings	255
	Overriding the Default DHCP Relay Configuration Settings	256
	Deleting DHCP Local Server and DHCP Relay Override Settings	258
Chapter 27	Applying a Common DHCP Relay Agent Configuration to Groups of DHCP Servers	259
	Configuring Server Groups	259
	Configuring Active Server Groups	259
Chapter 28	Changing the Gateway IP Address (giaddr) Field and DHCP Relay Request and Release Packet Source Address	261
	Changing the Gateway IP Address (giaddr) Field to the giaddr of the DHCP Relay Agent	261
	Replacing the DHCP Relay Request and Release Packet Source Address	261
Chapter 29	Configuring DHCP Relay Agent	263
	Using Layer 2 Unicast Transmission for DHCP Packets	263
	Trusting Option 82 Information	264
	Sending Release Messages When Clients Are Deleted	264
	Disabling Automatic Binding of Stray DHCP Requests	265
	Using DHCP Relay Agent Option 82 Information	266
	Configuring Option 82 Information	267
	Including a Prefix in DHCP Options	269
	Including a Textual Description in DHCP Options	271

	Using DHCP Option Information to Selectively Process DHCP Client Traffic . . .	273
	Example: Minimum DHCP Relay Agent Configuration	274
	Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings	275
	Example: DHCP Relay Agent Configuration with Multiple Clients and Servers . .	279
	Disabling DHCP Relay	280
Chapter 30	Configuring DHCP Relay Proxy Mode	281
	Enabling DHCP Relay Proxy Mode	281
Chapter 31	Configuring DHCP Local Server Authentication	283
	Configuring a Token for DHCP Local Server Authentication	283
Chapter 32	Configuring a Minimum DHCP Local Server Configuration	285
	Example: Minimum Extended DHCP Local Server Configuration	285
Chapter 33	Configuring DHCPv6 Local Server	287
	DHCPv6 Local Server Overview	287
	Multiple Address Assignment for DHCPv6 Clients	289
	Multiple Address Assignment Using Local Address Pools or RADIUS	289
	Junos OS Predefined Variable for Multiple DHCPv6 Address Assignment . .	289
	DHCPv6 Options in a DHCPv6 Multiple Address Environment	290
	Specifying the Delegated Address Pool for IPv6 Prefix Assignment	290
	Enabling DHCPv6 Rapid Commit Support	291
	Preventing Binding of Clients That Do Not Support Reconfigure Messages . . .	292
	Example: Extended DHCPv6 Local Server Configuration	292
Chapter 34	Configuring DHCPv6 Relay Agent	295
	DHCPv6 Relay Agent Options	295
	Configuring DHCPv6 Relay Agent Options	296
	Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets	297
	Inserting DHCPv6 Remote-ID Option (Option 37) In DHCPv6 Packets	298
Chapter 35	Protecting the Routing Engine Using DHCP Firewall Filters	301
	Example: Configuring a DHCP Firewall Filter to Protect the Routing Engine . . .	301
	Port Number Requirements for DHCP Firewall Filters	305
Chapter 36	Monitoring and Managing DHCP	307
	Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings . .	307
	Clearing DHCP Bindings for Subscriber Access	308
	Displaying a Count of DHCP Packets That Are Dropped or Forwarded During Selective Processing That Is Based on DHCP Option Strings	310
	Monitoring DHCP Relay Server Responsiveness	310
	Verifying and Managing DHCP Local Server Configuration	311
	Verifying and Managing DHCPv6 Local Server Configuration	311
	Verifying and Managing DHCP Relay Configuration	312
	Verifying and Managing DHCPv6 Relay Configuration	312

Part 3	Configuring Address-Assignment Pools for Subscriber Management	
Chapter 37	Configuring Address-Assignment Pools for Dynamic and Static Addresses	315
	Address-Assignment Pools Overview	315
	Address-Assignment Pools Licensing Requirements	316
	Configuring Address-Assignment Pools	316
	Example: Configuring an Address-Assignment Pool	317
	Configuring an Address-Assignment Pool Name and Addresses	318
	Configuring a Named Address Range for Dynamic Address Assignment	319
	Configuring Address-Assignment Pool Usage Threshold Traps	320
	Configuring Address-Assignment Pool Linking	320
	Configuring Static Address Assignment	321
	Configuring Duplicate IPv4 Address Protection for AAA	322
Part 4	Configuring DNS Addresses for Subscriber Management	
Chapter 38	Configuring DNS Address Assignments and Session Options	325
	Configuring DNS Name Server Addresses for Subscriber Management	325
	Overriding How the DNS Server Address Is Returned in a DHCPv6 Multiple Address Environment	326
Part 5	Configuring CLI-Based Subscriber Services	
Chapter 39	Configuring CLI-Activated Subscriber Services	331
	CLI-Activated Subscriber Services	331
	Activating and Deactivating Subscriber Services Locally with the CLI	332
	Using the CLI to Modify Traffic-Control Profiles That Are Currently Applied to Subscribers	335
	Using the CLI to Globally Modify a Traffic-Control Profile Currently Applied to Multiple Subscribers	336
	Using the CLI to Modify a Traffic-Control Profile for a Specific Current Subscriber	336
Chapter 40	Configuring Subscriber Services with Multiple Instances	339
	Subscriber Services with Multiple Instances Overview	339
	Subscriber Service Instances and Service Parameters	339
	CLI Deactivation of Subscriber Services with Multiple Instances	340
	Subscriber Services with Multiple Instances in RADIUS Accounting Messages	340
	Deactivating a Single Instance of a Subscriber Service with Multiple Instances	341
	Deactivating All Instances of a Subscriber Service with Multiple Instances	343
Chapter 41	Monitoring and Managing Subscriber Services	347
	Verifying and Managing Subscriber Services with Multiple Instances	347

Part 6	Configuring ANCP and the ANCP Agent for Subscribers	
Chapter 42	Configuring ANCP Agent Neighbors and Operations	351
	ANCP and the ANCP Agent Overview	351
	Overview	352
	Topology Discovery	352
	Subscriber Services	353
	ANCP Interfaces and Access Loop Circuit Identifiers	353
	ANCP Neighbors	354
	Partitions	356
	Generic Response Messages and Result Codes	357
	ANCP Operations in Different Network Configurations	358
	ANCP Network Using N:1 and 1:1 Configuration Models without Interface Sets	362
	Sequence of ANCP Events: Static VLAN or VLAN Demux Interfaces over Ethernet Without Interface Sets	363
	ANCP Network Using N:1 Configuration Model with Interface Sets	364
	Sequence of ANCP Events: Static VLAN Interfaces over Ethernet with Interface Sets	365
	ANCP Network Using 1:1 Configuration Model with Interface Sets	366
	Sequence of ANCP Events: Static VLAN Demux Interfaces over Aggregated Ethernet with Interface Sets	367
	Configuring the ANCP Agent	368
	Configuring ANCP Neighbors	369
	Associating an Access Node with Subscribers for ANCP Agent Operations	370
	Specifying the Interval Between ANCP Adjacency Messages	371
	Specifying the Maximum Number of Discovery Table Entries	371
	Configuring the ANCP Agent for Backward Compatibility	372
	Specifying How Long Processes Wait for the ANCP Agent Restart to Complete	373
	Configuring the ANCP Agent to Learn ANCP Partition IDs	373
	Example: Configuring an ANCP Network with Interface Sets and N:1 Static Demux VLANs over Aggregated Ethernet	374
Chapter 43	Configuring the ANCP Agent Traffic and CoS	395
	Traffic Rate Reporting and Adjustment by the ANCP Agent	395
	Overview	395
	Traffic Rate Adjustment	396
	Recommended Traffic Shaping Rates	397
	ANCP Agent Keepalives for CoS	398
	Preservation of CoS Shaping Across ANCP Agent Restarts	398
	Configuring the ANCP Agent to Report Traffic Rates to CoS	399
	Setting a Recommended Shaping Rate for Traffic on ANCP Interfaces	400
	Setting a Global Adjustment Factor per DSL Subscriber Line for ANCP Agent-Reported Traffic Rates	402

Chapter 44	Configuring the ANCP Agent and AAA	403
	ANCP Agent Interactions with AAA	403
	ANCP DSL Attributes Mapped to Juniper Networks DSL Vendor-Specific Attributes	405
	Configuring AAA to Include Juniper Networks DSL VSAs in RADIUS Messages . .	407
	Configuring Immediate Interim Accounting Updates to RADIUS in Response to ANCP Notifications	408
Chapter 45	Monitoring and Managing ANCP for Subscriber Access	411
	Triggering ANCP OAM to Test the Local Loop	411
	Verifying and Monitoring ANCP Neighbors	412
	Clearing ANCP Neighbors	412
	Verifying and Monitoring ANCP Subscribers	413
	Clearing ANCP Subscribers	413
	Verifying and Monitoring CoS for ANCP Subscribers	414
	Clearing and Verifying ANCP Statistics	414
Part 7	Configuring the Diameter Base Protocol	
Chapter 46	Configuring Diameter and its Applications	419
	Diameter Base Protocol Overview	419
	Messages Used by Diameter Applications	421
	Diameter AVPs and Diameter Applications	426
	Configuring Diameter	434
	Configuring the Origin Attributes of the Diameter Instance	435
	Configuring Diameter Peers	435
	Configuring the Diameter Transport	436
	Configuring Diameter Network Elements	437
Chapter 47	Configuring Gx-Plus for Provisioning Subscribers	439
	Gx-Plus for Provisioning Subscribers Overview	439
	Understanding Gx-Plus Interactions Between the Router and the PCRF	441
	Subscriber Login	441
	Fault Tolerance and Event Notification	443
	PCRF-Generated Discovery	445
	Subscriber Accounting	445
	Subscriber Audit	445
	Subscriber Logout	446
	Configuring Gx-Plus	446
	Configuring the Gx-Plus Partition	447
	Configuring Gx-Plus Global Attributes	448
	Provisioning Subscribers with Gx-Plus	449
Chapter 48	Configuring JSRC in Subscriber Access Networks	451
	Juniper Networks Session and Resource Control (SRC) and JSRC Overview . .	451
	Hardware Requirements for JSRC for Subscriber Access	452
	Understanding JSRC-SAE Interactions	453
	Subscriber Login	453
	Subscriber Service Activation and Deactivation	454
	Subscriber Resynchronization	454

	Subscriber Session Terminated by the SAE	454
	Statistics Collection and Reporting per Service Rule	455
	Subscriber Logout	455
	Configuring JSRC	455
	Configuring the JSRC Partition	456
	Assigning a Partition to JSRC	457
	Authorizing Subscribers with JSRC	457
	Provisioning Subscribers with JSRC	458
Chapter 49	Configuring Service Accounting with JSRC	459
	Service Accounting with JSRC	459
	Configuring Service Accounting with JSRC	460
Chapter 50	Configuring Subscribers on Static Interfaces	463
	Subscribers on Static Interfaces Overview	463
	Configuring Subscribers over Static Interfaces	466
	Example: Configuring Static Subscribers for Subscriber Access	467
Chapter 51	Configuring the Static Subscribers Global Profile	471
	Specifying the Static Subscriber Global Access Profile	471
	Specifying the Static Subscriber Global Dynamic Profile	471
	Enabling Multiple Subscribers on a VLAN Logical Interface for All Static Subscribers	472
	Configuring the Static Subscriber Global Authentication Password	473
	Configuring the Static Subscriber Global Username	473
Chapter 52	Configuring the Static Subscribers Group Profile	475
	Creating a Static Subscriber Group	475
	Specifying the Static Subscriber Group Access Profile	476
	Specifying the Static Subscriber Group Dynamic Profile	476
	Enabling Multiple Subscribers on a VLAN Logical Interface for a Static Subscriber Group	477
	Configuring the Static Subscriber Group Authentication Password	477
	Configuring the Static Subscriber Group Username	478
Chapter 53	Configuring the PTSP Feature to Support Dynamic Subscribers	479
	PTSP Overview	479
	Hardware Requirements for PTSP for Subscriber Access	480
	Juniper Networks Session and Resource Control (SRC) and PTSP Overview	480
	Understanding PTSP-SAE Interactions	481
	Packet-Triggered Subscribers Services Overview	482
	Subscriber Identification Method for PTSP Partition	484
	PTSP Services on Aggregated and Redundant Services PICs	484
	Configuring the PTSP Application	486
	Configuring PTSP	486
Chapter 54	Configuring the PTSP Partition to Connect to the External Policy Manager	489
	Understanding the Subscriber Profiles for Client Sessions per PTSP Partition	489
	Configuring the PTSP Partition	491
	Assigning the PTSP Partition	492

Chapter 55	Configuring PTSP Services and Rules	493
	Configuring the Multiservices DPC for PTSP	493
	Enabling the PTSP Service Package on the Multiservices DPC	493
	Configuring Services Interface for PTSP	494
	Configuring PTSP Service Rules	494
	Configuring Static PTSP Rules	495
	Configuring PTSP Rule Sets	497
	Configuring PTSP Service Sets	497
	Configuring the PTSP Forwarding Instance	498
Chapter 56	Monitoring and Managing Diameter Information for Subscriber Access . .	501
	Verifying Diameter Node, Instance, and Route Information	501
	Verifying and Managing Diameter Function Information	502
	Verifying and Managing Diameter Peer Information	503
	Verifying Diameter Network Element Information	504
Chapter 57	Monitoring and Managing Subscriber Information on Static Interfaces . .	505
	Forcing a Static Subscriber to Be Logged Out	505
	Resetting the State of an Interface for Static Subscriber Login	505
	Forcing a Group of Static Subscribers to Be Logged Out	506
	Resetting the State of an Interface Group for Static Subscriber Login	506
	Verifying Information about Subscriber Sessions on Static Interfaces	506
Chapter 58	Monitoring and Managing Packet-Triggered Subscribers	507
	Verifying and Managing PTSP Configuration	507
Part 8	Configuring Router Advertisement for Subscriber Management	
Chapter 59	Configuring the Dynamic Router Advertisement Protocol	511
	Dynamic Router Advertisement and Subscriber Access	511
	Dynamic Router Advertisement Configuration Overview	511
	Configuring Dynamic Router Advertisement	512
Part 9	Troubleshooting	
Chapter 60	Configuring AAA Testing and Troubleshooting	515
	AAA Configuration Testing and Troubleshooting	515
	Testing a Subscriber AAA Configuration	515
Chapter 61	Tracing Extended DHCP Operations	521
	Tracing Extended DHCP Operations	521
	Configuring the Extended DHCP Log Filename	523
	Configuring the Number and Size of Extended DHCP Log Files	523
	Configuring Access to the Extended DHCP Log File	524
	Configuring a Regular Expression for Extended DHCP Messages to Be Logged	524
	Configuring the Extended DHCP Tracing Flags	524
	Configuring the Severity Level to Filter Which Extended DHCP Messages Are Logged	525
	Tracing Extended DHCP Operations for Specific Interfaces	526
	Tracing Extended DHCP Operations for Specific Interfaces	527

Chapter 62	Configuring Subscriber Management Database Log Files	529
	Configuring the Number and Size of Subscriber Management Database Log Files	529
	Configuring Access to the Subscriber Management Database Log File	530
	Configuring a Regular Expression for Subscriber Management Database Messages to Be Logged	530
Chapter 63	Configuring Subscriber Management Database Trace Flags and Operations	531
	Tracing Subscriber Management Database Operations for Subscriber Access	531
	Configuring the Subscriber Management Database Trace Log Filename	532
	Configuring the Subscriber Management Database Tracing Flags	532
Chapter 64	Configuring Subscriber Management Session Database Log Files	533
	Configuring the Number and Size of Subscriber Management Session Database Replication Log Files	533
	Configuring Access to the Subscriber Management Session Database Replication Log File	534
	Configuring a Regular Expression for Subscriber Management Session Database Replication Messages to Be Logged	534
Chapter 65	Configuring Subscriber Management Session Database Trace Flags and Operations	535
	Tracing Subscriber Management Session Database Replication Operations for Subscriber Access	535
	Configuring the Subscriber Management Session Database Replication Trace Log Filename	536
	Configuring the Subscriber Management Session Database Replication Tracing Flags	536
Chapter 66	Configuring Diameter Base Protocol Log Files	539
	Configuring the Number and Size of Diameter Base Protocol Log Files	539
	Configuring Access to the Diameter Base Protocol Log File	540
	Configuring a Regular Expression for Diameter Base Protocol Messages to Be Logged	540
	Configuring the Severity Level to Filter Which Diameter Base Protocol Messages Are Logged	540
Chapter 67	Configuring Diameter Base Protocol Trace Flags and Operations	543
	Tracing Diameter Base Protocol Processes for Subscriber Access	543
	Configuring the Diameter Base Protocol Trace Log Filename	544
	Configuring the Diameter Base Protocol Tracing Flags	544
Chapter 68	Troubleshooting Diameter Networks	547
	Troubleshooting Diameter Network Configuration	547
	Troubleshooting Diameter Network Connectivity	547
Chapter 69	Configuring ANCP Log Files	549
	Configuring the Number and Size of ANCP Log Files	549
	Configuring Access to the ANCP Log File	550

	Configuring a Regular Expression for ANCP Messages to Be Logged	550
	Configuring the Severity Level to Filter Which ANCP Messages Are Logged	550
Chapter 70	Configuring ANCP Trace Flags and Operations	553
	Tracing ANCP Agent Operations for Subscriber Access	553
	Configuring the ANCP Trace Log Filename	554
	Configuring the ANCP Tracing Flags	554
Chapter 71	Configuring General Authentication Service Log Files	557
	Configuring the Number and Size of General Authentication Service Processes Log Files	557
	Configuring Access to the Log File	558
	Configuring a Regular Expression for Lines to Be Logged	558
Chapter 72	Configuring General Authentication Service Trace Flags and Operations	559
	Tracing General Authentication Service Processes	559
	Configuring the General Authentication Service Processes Trace Log Filename	560
	Configuring the Number and Size of General Authentication Service Processes Log Files	560
	Configuring Access to the Log File	561
	Configuring a Regular Expression for Lines to Be Logged	561
	Configuring Subscriber Filtering for General Authentication Service Trace Operations	561
	Configuring the Trace Operation	562
	Configuring the General Authentication Service Processes Trace Log Filename	563
	Configuring the Trace Operation	564
	Configuring Subscriber Filtering for General Authentication Service Trace Operations	564
Chapter 73	Configuring Static Subscriber Interfaces Log Files	567
	Configuring the Number and Size of Static Subscribers Log Files	567
	Configuring Access to the Static Subscribers Log File	568
	Configuring a Regular Expression for Static Subscriber Messages to Be Logged	568
	Configuring the Severity Level to Filter Which Static Subscriber Messages Are Logged	568
Chapter 74	Configuring Static Subscriber Interfaces Trace Flags and Operations . . .	571
	Tracing Static Subscriber Operations	571
	Configuring the Static Subscribers Trace Log Filename	572
	Configuring the Static Subscribers Tracing Flags	572
Chapter 75	Configuring PTSP Tracing Operations	575
	Tracing Packet-Triggered Subscriber Operations	575
	Configuring the Packet-Triggered Subscribers Trace Log Filename	576
	Configuring the Size of Packet-Triggered Subscribers Log Files	576

	Configuring the Packet-Triggered Subscribers Tracing Flags	576
	Configuring a Statistics Profile for PTSP	577
	Configuring the File Properties for Statistics Data Output	577
	Configuring the Profile Properties for Statistics Data Output	578
	Configuring the Record Type for Statistics Data	578
	Tracing PTSP Operations	579
Chapter 76	Overriding PCRF Session Control to Troubleshoot a Session or Services	581
	Disabling PCRF Control of a Subscriber Session	581
Chapter 77	Contacting Juniper Technical Support	583
	Collecting Subscriber Access Logs Before Contacting Juniper Networks Technical Support	583
	Compressing Troubleshooting Logs from /var/logs to Send to Juniper Networks Technical Support	585
Part 10	Configuration Statements and Operational Commands	
Chapter 78	Configuration Statements	589
	[edit access address-assignment] Hierarchy Level	600
	[edit access domain] Hierarchy Level	601
	[edit access gx-plus] Hierarchy Level	601
	[edit access profile] Hierarchy Level	602
	[edit diameter] Hierarchy Level	604
	[edit dynamic-profiles] Hierarchy Level	605
	[edit forwarding-options dhcp-relay] Hierarchy Level	612
	[edit interfaces radius-options] Hierarchy Level	616
	[edit jsr] Hierarchy Level	616
	[edit protocols ancp] Hierarchy Level	616
	[edit system services dhcp-local-server] Hierarchy Level	617
	[edit system services packet-triggered-subscribers] Hierarchy Level	621
	[edit system services static-subscribers] Hierarchy Level	621
	[edit system services subscriber-management] Hierarchy Level	622
	aaa-logical-system (Domain Map)	623
	aaa-routing-instance (Domain Map)	624
	abated-utilization (Address-Assignment Pools)	625
	abated-utilization-v6 (Address-Assignment Pools)	625
	access-identifier	626
	access-loop-id-local	626
	access-profile (Domain Map)	627
	access-profile (Static Subscribers)	628
	access-profile-name (Duplicate Accounting)	629
	accounting (Access Profile)	630
	accounting-backup-options (Access Profile)	631
	accounting-order (Service Accounting)	631
	accounting-port	632
	accounting-retry (RADIUS)	633
	accounting-server	633
	accounting-session-id-format	634

accounting-stop-on-access-deny	634
accounting-stop-on-failure	635
accounting-timeout (RADIUS)	635
active-server-group	636
address (Diameter Peer)	637
address (Diameter Transport)	637
address-assignment (Address-Assignment Pools)	638
address-pool (Domain Map)	639
adjacency-timer	639
advisory-options (Traffic Shaping)	640
aggregate-clients (DHCP Relay Agent)	641
aggregate-clients (Static Subscribers)	642
always-write-giaddr	643
always-write-option-82	644
ancp	645
ancp-speed-change-immediate-update (ANCP)	646
application-group-any	646
application-groups	647
applications (Services PTSP)	647
attempts (DHCP Local Server)	648
attributes	649
authentication (DHCP Local Server)	650
authentication (DHCP Relay Agent)	651
authentication (Static Subscribers)	652
authentication-order	653
authentication-server	654
authorization-order	654
autonomous (Dynamic Router Advertisement)	655
boot-file	655
boot-server	656
calling-station-id-delimiter (Subscriber Management)	656
calling-station-id-format (Subscriber Management)	657
circuit-id (Address-Assignment Pools)	658
circuit-type (DHCP Local Server)	659
circuit-type (DHCP Relay Agent)	660
clear-on-abort (DHCP Local Server)	661
client-accounting-algorithm	662
client-authentication-algorithm	662
client-discover-match (DHCP Local Server)	663
client-discover-match (DHCP Relay Agent)	664
client-id (DHCP Local Server)	665
client-id (DHCP Relay Agent)	666
client-idle-timeout	666
client-session-timeout	667
coa-dynamic-variable-validation	668
coa-immediate-update	668
coa-no-override service-class-attribute	669
concurrent-data-sessions	669
connect-actively	670

count-type	671
current-hop-limit (Dynamic Router Advertisement)	672
database-replication (Subscriber Session Database)	672
default-action (DHCP Relay Agent Option)	673
default-lifetime (Dynamic Router Advertisement)	674
delay-authentication (DHCP Relay Agent)	674
delegated-pool (DHCP Local Server)	675
delimiter (DHCP Local Server)	676
delimiter (Domain Map)	677
delimiter (DHCP Relay Agent)	678
demux	679
destination (Diameter Network Element)	679
destination-host	680
destination-host (Gx-Plus)	680
destination-host (PTSP)	681
destination-realm (JSRC)	681
destination-realm (Gx-Plus)	682
destination-realm (PTSP)	682
dhcp-attributes (Address-Assignment Pools)	683
dhcp-local-server	684
dhcp-relay	689
dhcpv6 (DHCP Local Server)	695
dhcpv6 (DHCP Relay Agent)	698
diameter	701
diameter-instance (JSRC)	702
diameter-instance (Gx-Plus)	702
diameter-instance (PTSP)	703
disable	703
disable-relay	704
dns-server	704
domain (Domain Map)	705
domain-name (DHCP Local Server)	706
domain-name (DHCP Relay Agent)	708
domain-name (Address-Assignment Pools)	709
domain-name (Static Subscribers)	710
domain-name-server (Routing Instances and Access Profiles)	711
domain-name-server-inet (Routing Instances and Access Profiles)	712
domain-name-server-inet6 (Routing Instances and Access Profiles)	713
downstream-rate (Traffic Shaping)	714
drop (DHCP Relay Agent Option)	715
duplication (Access Profile)	715
duplication-vrf (Duplicate Accounting)	716
dynamic-profile (DHCP Local Server)	717
dynamic-profile (DHCP Relay Agent)	718
dynamic-profile (Domain Map)	719
dynamic-profile (Static Subscribers)	720
enable	721
equals (DHCP Relay Agent)	722
ethernet-port-type-virtual	723

exceed-action	723
exclude (RADIUS)	724
external-authority	728
family (Address-Assignment Pools)	729
forward-only (DHCP Relay Agent Option)	730
forward-rule (Configuring)	731
forward-rule (Including in Rule)	732
forwarding (Diameter Network Element)	732
from (Forward Rule)	733
from (Rule)	734
function (Diameter Network Element)	735
function (Diameter Route)	736
global (Gx-Plus)	736
grace-period	737
group (DHCP Local Server)	738
group (DHCP Relay Agent)	741
group (Static Subscribers)	744
gsmp-syn-timeout (ANCP)	745
gsmp-syn-wait (ANCP)	746
gx-plus (Gx-Plus)	747
hardware-address	747
high-utilization (Address-Assignment Pools)	748
high-utilization-v6 (Address-Assignment Pools)	748
host (Address-Assignment Pools)	749
host (Diameter Origin)	749
ietf-mode	750
ignore	751
immediate-update	752
include-ipv6 (Gx-Plus)	752
include-irb-and-l2	753
interface (DHCP Local Server)	755
interface (DHCP Relay Agent)	757
interface (Dynamic Router Advertisement)	759
interface (Static Subscriber Group)	760
interface (Static Subscriber Username)	761
interface-client-limit (DHCP Local Server)	762
interface-client-limit (DHCP Relay Agent)	764
interface-delete (Subscriber Management or DHCP Client Management)	765
interface-delete (Subscriber Management or DHCP Client Management)	766
interface-description-format	766
interface-name (DHCP Local Server)	767
interface-name (DHCP Relay Agent)	768
interface-set (ANCP)	769
interface-traceoptions (DHCP)	770
interfaces (ANCP)	772
ip-address	772
ip-address-first	773
jsrc (JSRC)	774
jsrc-partition	774

juniper-dsl-attributes	775
layer2-unicast-replies	776
lease-time-threshold (DHCP Local Server and DHCP Relay Agent)	777
lease-time-validation (DHCP Local Server and DHCP Relay Agent)	778
limit	778
link (Address-Assignment Pools)	779
local-address	780
local-address-range	781
local-port-range	781
local-ports	782
local-prefix-list	782
local-server-group (DHCP Relay Agent Option)	783
logical-system (Diameter Peer)	784
logical-system (Diameter Transport)	785
logical-system-name (Static Subscribers)	786
logical-system-name (DHCP Local Server)	787
logical-system-name (DHCP Relay Agent)	788
ltv-syslog-interval (System Process)	789
mac-address (DHCP Local Server)	790
mac-address (DHCP Relay Agent)	791
maintain-subscriber (Subscriber Management)	792
managed-configuration (Dynamic Router Advertisement)	793
map (Domain Map)	794
mask (Domain Map)	795
match-direction (Services PTSP)	795
max-advertisement-interval (Dynamic Router Advertisement)	796
max-data-sessions-per-subscriber	796
max-outstanding-requests	797
max-outstanding-requests (Gx-Plus)	798
max-pending-accounting-stops (Access Profile)	798
max-withhold-time (Access Profile)	799
maximum-discovery-table-entries	799
maximum-helper-restart-time	800
maximum-lease-time	800
metric (Diameter Route)	801
metric (Domain Map)	801
min-advertisement-interval (Dynamic Router Advertisement)	802
multi-address-embedded-option-response (DHCP Local Server)	803
name-server	803
nas-identifier	804
nas-port-extended-format (Access Profile)	805
nas-port-extended-format (Interfaces)	807
nas-port-id-delimiter (Subscriber Management)	808
nas-port-id-format (Subscriber Management)	809
nas-port-options (RADIUS Options)	810
nas-port-type (Subscriber Management)	811
nas-port-type (RADIUS Options)	813
neighbor (Define ANCP)	814
neighbor-discovery-router-advertisement (Address-Assignment Pools)	815

netbios-node-type	815
network	816
network-element (Diameter Base Protocol)	817
no-bind-on-request (DHCP Relay Agent)	818
on-link (Dynamic Router Advertisement)	819
no-vlan-interface-name	820
option	822
option-60 (DHCP Local Server)	823
option-60 (DHCP Relay Agent)	824
option-82 (DHCP Relay Agent)	825
option-82 (DHCP Local Server Authentication)	826
option-82 (DHCP Local Server Pool Matching)	827
option-82 (Address-Assignment Pools)	828
option-match	828
option-number (DHCP Relay Agent Option)	829
options (Access Profile)	830
order	831
origin (Diameter Base Protocol)	832
other-stateful-configuration (Dynamic Router Advertisement)	832
overhead-accounting (ANCP)	833
overrides (DHCP Local Server)	834
overrides (DHCP Relay Agent)	836
packet-triggered-subscribers	837
packet-triggered-subscribers-partition	838
padn (Domain Map)	838
parse-direction (Domain Map)	839
parse-order (Domain Map)	840
partition	841
partition (Gx-Plus)	841
partition (PTSP)	842
password (Static Subscribers)	843
password (DHCP Local Server)	844
password (DHCP Relay Agent)	845
peer (Diameter Base Protocol)	846
peer (Diameter Network Element)	846
pool (Address-Assignment Pools)	847
pool (DHCP Local Server Overrides)	848
pool-match-order	849
port	850
port (Diameter Peer)	850
pre-ietf-mode	851
preauthentication-order (Access Profile)	851
preauthentication-server (Access Profile)	852
preferred-lifetime (Address-Assignment Pools)	853
preferred-lifetime (Dynamic Router Advertisement)	854
prefix (DHCP Relay Agent)	855
prefix (Address-Assignment Pools)	856
prefix (Dynamic Router Advertisement)	856
priority (Diameter Peer)	857

profile (Access)	858
process-inform	862
protocol	863
protocols (Dynamic Profiles)	864
provisioning-order	866
proxy-mode	867
qos-adjust	868
qos-adjust-adsl	868
qos-adjust-adsl2	869
qos-adjust-adsl2-plus	869
qos-adjust-sdsl	870
qos-adjust-vdsl	870
qos-adjust-vdsl2	871
radius (Access Profile)	872
radius-disconnect (DHCP Local Server)	874
radius-options (Edit Access)	875
radius-options (Interfaces)	876
radius-server	877
range (Address-Assignment Pools)	878
rapid-commit (DHCPv6 Local Server)	879
reachable-time (Dynamic Router Advertisement)	880
realm (Diameter Origin)	880
realm-delimiter (Domain Map)	881
realm-parse-direction (Domain Map)	881
reconfigure (DHCP Local Server)	882
relay-agent-interface-id (DHCP Local Server)	883
relay-agent-interface-id (DHCPv6 Relay Agent)	884
relay-agent-interface-id (DHCPv6 Relay Agent Username)	885
relay-agent-remote-id (DHCP Local Server)	886
relay-agent-remote-id (DHCPv6 Relay Agent Username)	887
relay-agent-remote-id (DHCPv6 Relay Agent)	888
relay-agent-subscriber-id (DHCP Local Server)	889
relay-agent-subscriber-id (DHCPv6 Relay Agent)	890
relay-option (DHCP Relay Agent)	891
relay-option-82	892
relay-server-group (DHCP Relay Agent Option)	893
remote-address	894
remote-address-range	895
remote-id	895
remote-id (DHCP Relay Agent)	896
remote-port-range	898
remote-ports	898
remote-prefix-list	899
replace-ip-source-with	900
report-interface-descriptions (Edit Access)	901
request network-access aaa replay pending-accounting-stops	902
request network-access aaa subscriber add session-id	903
request network-access aaa subscriber delete session-id	905
request network-access aaa subscriber modify session-id	907

request-rate	908
requested-ip-network-match (DHCP Local Server)	909
retransmit-timer (Dynamic Router Advertisement)	910
retry	910
revert-interval	911
route (Diameter Network Element)	912
router (Address-Assignment Pools)	912
router-advertisement (Dynamic Profiles)	913
routing-instance	913
routing-instance (Diameter Peer)	914
routing-instance (Diameter Transport)	914
routing-instance-name (Static Subscribers)	915
routing-instance-name (DHCP Relay Agent)	916
routing-instance-name (DHCP Local Server)	917
rule (Configuring)	918
rule (Including in Rule Set)	919
rule-set (Services PTSP)	919
secret	920
send-acct-status-on-config-change (Access Profile)	921
send-release-on-delete (DHCP Relay Agent)	922
server-group	923
server-identifier (Address-Assignment Pools)	924
server-response-time (DHCP Relay Agent)	924
service (Service Accounting)	925
service-profile (DHCP Local Server)	926
service-profile (DHCP Relay Agent)	927
services (PTSP)	928
session-options	928
sip-server-address	929
sip-server-domain-name	929
source-address	930
stacked-vlan-ranges (RADIUS Options)	931
starts-with (DHCP Relay Agent Option)	932
static-subscribers	933
statistics (Access Profile)	934
strict (DHCP Local Server)	935
strip-domain (Domain Map)	936
subscriber-identification (PTSP)	937
subscriber-packet-idle-timeout	938
subscriber-management (Subscriber Management)	939
subscriber-profile	940
t1-percentage (Address-Assignment Pools)	941
t2-percentage (Address-Assignment Pools)	942
target-logical-system (Domain Map)	943
target-routing-instance (Domain Map)	944
term (Forward Rule)	945
term (Rule)	946
terminate-code	947
tftp-server	948

then (Forward Rule)	948
then (Rule)	949
timeout (RADIUS)	950
timeout (DHCP Local Server)	951
token (DHCP Local Server)	952
trace (DHCP Local Server)	953
traceoptions (ANCP)	954
traceoptions (Diameter Base Protocol)	956
traceoptions (DHCP)	958
traceoptions (General Authentication Service)	961
traceoptions (PTSP)	963
traceoptions (Static Subscribers)	965
traceoptions (Subscriber Management)	967
traceoptions (Subscriber Session Database Replication)	969
transport (Diameter Base Protocol)	970
transport (Diameter Peer)	971
trigger (DHCP Local Server)	972
trust-option-82	973
tunnel-profile (Domain Map)	974
underlying-interface (ANCP)	974
update-interval	975
upstream-rate (Traffic Shaping)	976
use-interface-description	977
use-option-82	979
use-primary (DHCP Relay Agent)	980
use-vlan-id	982
user-prefix (DHCP Relay Agent)	984
user-prefix (Static Subscribers)	985
user-prefix (DHCP Local Server)	986
username-include (Static Subscribers)	987
username-include (DHCP Local Server)	988
username-include (DHCP Relay Agent)	989
valid-lifetime (Dynamic Router Advertisement)	990
valid-lifetime (Address-Assignment Pools)	991
violation-action (DHCP Local Server and DHCP Relay Agent)	992
vlan-nas-port-stacked-format	993
vlan-ranges (RADIUS Options)	994
vrf-name (Duplicate Accounting)	995
wait-for-acct-on-ack (Access Profile)	995
wins-server (Access)	996
Chapter 79	
Operational Commands	997
clear ancp neighbor	1000
clear ancp statistics	1002
clear ancp subscriber	1004
clear dhcp relay binding	1006
clear dhcp relay statistics	1008
clear dhcpv6 relay binding	1011
clear dhcpv6 relay statistics	1014

clear dhcp server binding	1016
clear dhcp server statistics	1019
clear dhcpv6 server binding	1021
clear dhcpv6 server statistics	1023
clear diameter function statistics	1024
clear diameter peer	1025
clear ipv6 router-advertisement	1026
clear network-access aaa statistics	1027
clear network-access aaa subscriber	1029
clear network-access gx-plus replay	1030
clear network-access gx-plus statistics	1031
clear request services subscribers	1032
clear services subscriber sessions	1033
request ancp oam interface	1034
request ancp oam neighbor	1035
request dhcp server reconfigure	1036
request dhcpv6 server reconfigure	1038
request network-access aaa subscriber set session-id	1040
request services static-subscribers login group	1041
request services static-subscribers logout group	1042
request services static-subscribers login interface	1043
request services static-subscribers logout interface	1044
request system reboot	1045
set request services subscribers	1050
show accounting pending-accounting-stops	1051
show ancp cos	1055
show ancp neighbor	1058
show ancp statistics	1066
show ancp subscriber	1071
show ancp summary	1076
show ancp summary neighbor	1078
show ancp summary subscriber	1080
show database-replication statistics	1081
show database-replication summary	1083
show network-access aaa accounting	1085
show dhcp relay binding	1086
show dhcp relay statistics	1091
show dhcp server binding	1094
show dhcp server statistics	1099
show dhcpv6 relay binding	1102
show dhcpv6 relay statistics	1108
show dhcpv6 server binding	1111
show dhcpv6 server statistics	1117
show diameter	1120
show diameter function	1126
show diameter function statistics	1130
show diameter instance	1133
show diameter network-element	1135
show diameter network-element map	1138

show diameter peer	1141
show diameter peer map	1146
show diameter peer statistics	1149
show diameter route	1153
show ipv6 router-advertisement	1155
show network-access aaa accounting	1158
show network-access aaa radius-servers	1159
show network-access aaa statistics	1164
show network-access aaa statistics authentication	1169
show network-access aaa statistics pending-accounting-stops	1172
show network-access aaa statistics preauthentication	1173
show network-access aaa subscribers	1175
show network-access aaa subscribers session-id	1178
show network-access aaa terminate-code	1183
show network-access address-assignment pool	1186
show network-access domain-map	1187
show network-access gx-plus	1188
show route extensive	1190
show services subscriber bandwidth	1207
show services subscriber dynamic-policies	1209
show services subscriber flows	1212
show services subscriber sessions	1214
show services subscriber statistics	1217
show static-subscribers sessions	1219
show subscribers	1221
show subscribers summary	1239
show system subscriber-management summary	1244
test aaa authd-lite user	1246
test aaa dhcp user	1249
test aaa ppp user	1252

Part 11

Index

Index	1259
-------------	------

List of Figures

Part 1	Configuring AAA for Subscriber Management	
Chapter 5	Configuring RADIUS Accounting for Subscriber Access	85
	Figure 1: Topology with Loss of Access to Accounting Server	89
Chapter 9	Receiving DHCP Options From a RADIUS Server	113
	Figure 2: DHCP Options Data Flow	116
Part 6	Configuring ANCP and the ANCP Agent for Subscribers	
Chapter 42	Configuring ANCP Agent Neighbors and Operations	351
	Figure 3: Sample ANCP Topology Without Interface Sets (1:1 and N:1 Model) . .	362
	Figure 4: Sample ANCP Topology with Interface Sets (N:1 Model)	364
	Figure 5: Sample ANCP Topology with Interface Sets (1:1 Model)	366
	Figure 6: N:1 ANCP Topology with Interface Sets and VLAN Demux Interface over Aggregated Ethernet	375

List of Tables

	About the Documentation	xxxv
	Table 1: Notice Icons	xxxvii
	Table 2: Text and Syntax Conventions	xxxvii
Part 1	Configuring AAA for Subscriber Management	
Chapter 2	Configuring RADIUS Attributes and Juniper Networks VSAs	13
	Table 3: Supported RADIUS IETF Attributes	14
	Table 4: Supported Juniper Networks VSAs	22
	Table 5: AAA Access Messages—Supported RADIUS Attributes and Juniper Networks VSAs	31
	Table 6: AAA Accounting Messages—Supported RADIUS Attributes and Juniper Networks VSAs	37
	Table 7: Attributes That Can Be Ignored in RADIUS Access-Accept Messages . . .	41
	Table 8: Attributes That Can Be Excluded from RADIUS Messages	42
	Table 9: RADIUS Attributes and Corresponding Junos OS Predefined Variables	46
	Table 10: DSL Forum VSAs	52
	Table 11: DSL Forum VSAs—Supported RADIUS Messages	53
Chapter 3	Configuring RADIUS NAS-Port Attributes and Options	55
	Table 12: RADIUS NAS-Port-Type Values	65
Chapter 5	Configuring RADIUS Accounting for Subscriber Access	85
	Table 13: RADIUS Attributes and VSAs Used for Per-Subscriber Session Accounting	86
	Table 14: Duplicate RADIUS Accounting Reporting	87
	Table 15: Juniper Networks VSAs Used for Per-Service Session Accounting	94
Chapter 9	Receiving DHCP Options From a RADIUS Server	113
	Table 16: Unsupported Opaque DHCP Options	118
	Table 17: DHCP Options Description	119
Chapter 10	Configuring RADIUS Logical Line Identification	121
	Table 18: RADIUS Attributes for LLID Preauthentication Requests	123
Chapter 11	Configuring Domain Maps for Subscriber Management	127
	Table 19: Domain Map Options and Parameters	129
	Table 20: Precedence Rules for Applying Access Profiles	132
	Table 21: Precedence Rules for Determining the Address Pool to Use	133
	Table 22: Precedence Rules for Applying Dynamic Profiles	134
Chapter 12	Configuring Dynamic Service Activation for Subscriber Access	143

	Table 23: Identification Attributes	146
	Table 24: Session Attributes	146
	Table 25: Juniper Network VSAs Used for Service Thresholds	148
	Table 26: Error-Cause Codes (RADIUS Attribute 101)	150
Chapter 13	Configuring Terminate Reasons for Protocols	151
	Table 27: Supported RADIUS Acct-Terminate-Cause Codes	151
	Table 28: Default AAA Mappings	154
	Table 29: Default DHCP Mappings	155
	Table 30: Default L2TP Mappings	156
	Table 31: Default PPP Mappings	172
Part 2	Configuring DHCP for Subscriber Management	
Chapter 15	Using DHCP Overview	187
	Table 32: Comparing the Extended DHCP Local Server to the Traditional DHCP Local Server	189
	Table 33: Information in Authentication Grant	191
Chapter 17	Assigning IP Addresses	201
	Table 34: DHCP Attributes	201
	Table 35: DHCPv6 Attributes	202
Chapter 18	Configuring Lease Times for IP Addresses	209
	Table 36: Lease-Time Violation Event Logging	211
Chapter 24	Forcing Dynamic Reconfiguration of Clients From a DHCP Local Server	241
	Table 37: Action Taken for Events That Occur During a Reconfiguration	243
Chapter 25	Conserving IP Addresses Using DHCP Auto Logout	249
	Table 38: DHCP Relay Agent Option 82 Value for Auto Logout	252
Chapter 33	Configuring DHCPv6 Local Server	287
	Table 39: RADIUS Attributes and VSAs for DHCPv6 Local Server	288
Part 5	Configuring CLI-Based Subscriber Services	
Chapter 40	Configuring Subscriber Services with Multiple Instances	339
	Table 40: Subscriber Services and Service Parameters in RADIUS Accounting Messages	341
Part 6	Configuring ANCP and the ANCP Agent for Subscribers	
Chapter 42	Configuring ANCP Agent Neighbors and Operations	351
	Table 41: ANCP Failure Result Codes	357
	Table 42: ACI Mapping by Interface Type for the ANCP 1:1 Model	359
	Table 43: ACI Mapping by Interface Set Type for the ANCP N:1 Access Model	360
	Table 44: Configuration Components used in ANCP N:1 Topology Example with Interface Sets	376
Chapter 44	Configuring the ANCP Agent and AAA	403

	Table 45: Mapping ANCP DSL Attributes to Juniper Networks DSL VSAs and DSL Forum VSAs	406
Part 7	Configuring the Diameter Base Protocol	
Chapter 46	Configuring Diameter and its Applications	419
	Table 46: Diameter Messages and Diameter Applications	422
	Table 47: Standard Diameter AVPs	426
	Table 48: Juniper Networks Diameter AVPs	430
	Table 49: Tekelec Diameter AVPs	433
Chapter 47	Configuring Gx-Plus for Provisioning Subscribers	439
	Table 50: Differences Between Gx-Plus and Junos OS Terminology	439
	Table 51: Router Events, Router Actions, and PCRF Actions	444
Chapter 55	Configuring PTSP Services and Rules	493
	Table 52: PTSP Match Conditions	496
	Table 53: PTSP Actions	496
	Table 54: PTSP Forward Rule Match Conditions	499
Part 10	Configuration Statements and Operational Commands	
Chapter 78	Configuration Statements	589
	Table 55: Service Activation/Deactivation Error Messages	903
	Table 56: Service Activation/Deactivation Error Messages	905
	Table 57: Service Activation/Deactivation Error Messages	907
Chapter 79	Operational Commands	997
	Table 58: clear dhcp relay statistics Output Fields	1009
	Table 59: Service Activation/Deactivation Error Messages	1040
	Table 60: show accounting pending-accounting-stops Output Fields	1051
	Table 61: show ancp cos Output Fields	1055
	Table 62: show ancp neighbor Output Fields	1058
	Table 63: show ancp statistics Output Fields	1066
	Table 64: show ancp subscriber Output Fields	1071
	Table 65: show ancp summary Output Fields	1076
	Table 66: show ancp summary neighbor Output Fields	1078
	Table 67: show ancp summary subscriber Output Fields	1080
	Table 68: show database-replication statistics Output Fields	1081
	Table 69: show database-replication summary Output Fields	1083
	Table 70: show network-access aaa accounting Output Fields	1085
	Table 71: show dhcp relay binding Output Fields	1087
	Table 72: show dhcp relay statistics Output Fields	1092
	Table 73: show dhcp server binding Output Fields	1095
	Table 74: show dhcp server statistics Output Fields	1100
	Table 75: show dhcpv6 relay binding Output Fields	1103
	Table 76: show dhcpv6 relay statistics Output Fields	1108
	Table 77: show dhcpv6 server binding Output Fields	1112
	Table 78: show dhcpv6 server statistics Output Fields	1118
	Table 79: show diameter Output Fields	1120
	Table 80: show diameter function Output Fields	1126

Table 81: show diameter function statistics Output Fields	1130
Table 82: show diameter instance Output Fields	1133
Table 83: show diameter network-element Output Fields	1135
Table 84: show diameter network-element map Output Fields	1138
Table 85: show diameter peer Output Fields	1141
Table 86: show diameter peer map Output Fields	1146
Table 87: show diameter peer statistics Output Fields	1149
Table 88: show diameter route Output Fields	1153
Table 89: show ipv6 router-advertisement Output Fields	1155
Table 90: show network-access aaa accounting Output Fields	1158
Table 91: show network-access aaa radius-servers Output Fields	1159
Table 92: show network-access aaa statistics Output Fields	1164
Table 93: show network-access aaa statistics authentication Output Fields . .	1169
Table 94: show network-access aaa statistics pending-accounting-stops Output Fields	1172
Table 95: show network-access aaa statistics preauthentication Output Fields	1173
Table 96: show network-access aaa subscribers Output Fields	1175
Table 97: show network-access aaa subscribers session-id Output Fields . . .	1178
Table 98: show network-access aaa terminate-code Output Fields	1183
Table 99: show network-access address-assignment pool Output Fields . . .	1186
Table 100: show network-access domain-map Output Fields	1187
Table 101: show network-access gx-plus Output Fields	1188
Table 102: show route extensive Output Fields	1190
Table 103: show services subscriber bandwidth Output Fields	1207
Table 104: show services subscriber dynamic-policies Output Fields	1209
Table 105: show services subscriber flows Output Fields	1212
Table 106: show services subscriber sessions Output Fields	1215
Table 107: show services subscriber statistics Output Fields	1217
Table 108: show static-subscribers sessions Output Fields	1219
Table 109: show subscribers Output Fields	1224
Table 110: show subscribers summary Output Fields	1240
Table 111: show system subscriber-management summary Output Fields . . .	1244

About the Documentation

- Documentation and Release Notes on page xxxv
- Supported Platforms on page xxxv
- Using the Examples in This Manual on page xxxv
- Documentation Conventions on page xxxvii
- Documentation Feedback on page xxxix
- Requesting Technical Support on page xxxix

Documentation and 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/>.

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

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

Supported Platforms

For the features described in this document, the following platforms are supported:

- MX Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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


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

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

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

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

Documentation Conventions

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

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure

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

Convention	Description	Examples
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none">Introduces or emphasizes important new terms.Identifies guide names.Identifies RFC and Internet draft titles.	<ul style="list-style-type: none">A policy <i>term</i> is a named structure that defines match conditions and actions.<i>Junos OS CLI User Guide</i>RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none">To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i>>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none">In the Logical Interfaces box, select All Interfaces.To cancel the configuration, click Cancel.

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

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <http://www.juniper.net/techpubs/feedback/>.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service 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:
<http://kb.juniper.net/InfoCenter/>
- 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

Configuring AAA for Subscriber Management

- [AAA and RADIUS for Subscriber Access Overview on page 3](#)
- [Configuring RADIUS Attributes and Juniper Networks VSAs on page 13](#)
- [Configuring RADIUS NAS-Port Attributes and Options on page 55](#)
- [Configuring RADIUS Authentication for Subscriber Access on page 79](#)
- [Configuring RADIUS Accounting for Subscriber Access on page 85](#)
- [Configuring Routers and RADIUS Servers for Subscriber Access on page 99](#)
- [Configuring Access Profiles for Subscriber Access on page 107](#)
- [Configuring Session Options for Subscriber Access on page 109](#)
- [Receiving DHCP Options From a RADIUS Server on page 113](#)
- [Configuring RADIUS Logical Line Identification on page 121](#)
- [Configuring Domain Maps for Subscriber Management on page 127](#)
- [Configuring Dynamic Service Activation for Subscriber Access on page 143](#)
- [Configuring Terminate Reasons for Protocols on page 151](#)
- [Monitoring and Managing AAA Information for Subscriber Access on page 181](#)

CHAPTER 1

AAA and RADIUS for Subscriber Access Overview

- [AAA Service Framework Overview on page 3](#)
- [RADIUS Server Options for Subscriber Access on page 4](#)
- [Global RADIUS Options for Subscriber Access on page 7](#)
- [Subscriber Access Interface Description Storage and Reporting Through RADIUS Overview on page 7](#)

AAA Service Framework Overview

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

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

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

- **Authentication**—Authentication parameters defined in the access profile determine the authentication component of the AAA processing. For example, subscribers can be authenticated using an external authentication service such as RADIUS.
- **Accounting**—Accounting parameters in the access profile specify the accounting part of the AAA processing. For example, the parameters determine how the router collects and uses subscriber statistics. You can also configure AAA to enable the router to collect statistics on a per-service session basis for subscribers.

- **RADIUS-initiated dynamic requests**—A list of authentication server IP addresses in the access profile specify the RADIUS servers that can initiate dynamic requests to the router. Dynamic requests include CoA requests, which specify VSA modifications and service changes, and disconnect requests, which terminate subscriber sessions. The list of authentication servers also provide RADIUS-based dynamic service activation and deactivation during subscriber login.
- **Address assignment**—The AAA Service Framework assigns addresses to subscribers based on the configuration of local address-assignment pools. For example, the AAA framework collaborates with RADIUS servers to assign addresses from the specified pools.
- **Subscriber secure policy**—RADIUS VSAs and attributes provide RADIUS-initiated traffic mirroring on a per-subscriber basis.

Related Documentation

- [Configuring Router or Switch Interaction with RADIUS Servers on page 99](#)
- [RADIUS Acct-On and Acct-Off Messages on page 91](#)
- [Configuring Authentication and Accounting Parameters for Subscriber Access on page 80](#)
- [Address-Assignment Pools Overview on page 315](#)
- [RADIUS Accounting Statistics for Subscriber Access Overview on page 85](#)
- [Using RADIUS Dynamic Requests for Subscriber Access Management on page 143](#)
- [Subscriber Secure Policy Overview](#)

RADIUS Server Options for Subscriber Access

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

The following list describes the RADIUS options you can configure:

- **accounting-session-id-format**—The format the router uses to identify the accounting session. The identifier can be in one of the following formats. The router uses **decimal** format by default.
 - **decimal**—For example, **435264**
 - **description**—In the format, **jnpr interface-specifier:subscriber-session-id**. For example, **jnpr fastEthernet 3/2.6:1010101010101**
- **calling-station-id-delimiter**—The character that the router uses as the separator between concatenated values in the Calling-Station-ID string (RADIUS attribute 31).
- **calling-station-id-format**—Optional information that the router includes in the Calling-Station-ID (RADIUS attribute 31).
- **client-accounting-algorithm** and **client-authentication-algorithm**—The method the router uses to access RADIUS accounting and RADIUS authentication servers. You can specify the following methods:

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



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

- **coa-dynamic-variable-validation**—The optional method that the router uses when processing CoA requests that include changes to a client profile dynamic variable that cannot be applied. The optional configuration specifies that when a CoA operation is unable to apply a requested change to a client profile dynamic variable, subscriber management does not apply any changes to client profile dynamic variables in the CoA request and then responds with a NACK. In the default method, subscriber management does not apply the incorrect update but does apply the other changes to the client profile dynamic variables, and then responds with an ACK message.
- **access-loop-id-local**—The Agent-Remote-Id and Agent-Circuit-Id are generated locally when these values are not present in the client database. The interface description of the logical interface is used as the Agent-Remote-Id and the interface description portion of the NAS-Port-Id using the format **<underlying-interface-name>:<outer-tag>-<inner-tag>** is used as the Agent-Circuit-Id.



NOTE: The NAS-Port-Id format changes (established by `[set access profile profile-name radius options interface-description-format]`) are applied before generating the Agent-Circuit-Id.

The NAS-Port-Id format (established by `[set access profile profile-name radius options interface-description-format]`) leverages the locally generated Agent-Remote-Id and Agent-Circuit-Id.

- **ethernet-port-type-virtual**—The physical port type of **virtual** that the router uses to authenticate clients. The port type is passed in RADIUS attribute 61 (NAS-Port-Type). By default the router passes a port type of **ethernet** in RADIUS attribute 61.
- **interface-description-format**—The information that is excluded from the interface description that the router passes to RADIUS for inclusion in the RADIUS attribute 87 (NAS-Port-Id). By default, the router includes both the **subinterface** and the **adapter** in the interface description. You can specify:

- **exclude-adapter**—Exclude the adapter.
- **exclude-subinterface**—Exclude the subinterface.
- **nas-identifier**—The value for the client RADIUS attribute 32 (NAS-Identifier), which is used for authentication and accounting requests. You can specify a string in the range 1 through 64 characters.
- **nas-port-extended-format**—The extended format for RADIUS attribute 5 (NAS-Port) and for the width of the fields in the NAS-Port attribute that the RADIUS client uses. You can specify:
 - **adapter-width *width***—Number of bits in the adapter field.
 - **port-width *width***—Number of bits in the port field.
 - **slot-width *width***—Number of bits in the slot field.
 - **stacked-vlan-width *width***—Number of bits in the SVLAN ID field.
 - **vlan-width *width***—Number of bits in the VLAN ID field.



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

You can configure an extended format for the NAS-Port attribute for both Ethernet subscribers and ATM subscribers. For ATM subscribers, you can specify:

- **adapter-width**—Number of bits in the ATM adapter field, in the range 0 through 32
- **port-width**—Number of bits in the ATM port field, in the range 0 through 32
- **slot-width**—Number of bits in the ATM slot field, in the range 0 through 32
- **vpi-width**—Number of bits in the ATM virtual path identifier (VPI) field, in the range 0 through 32
- **vci-width**—Number of bits in the ATM virtual circuit identifier (VCI) field, in the range 0 through 32



NOTE: For ATM subscribers, the combined total of the widths of all fields must not exceed 32 bits, or the configuration fails. The router may truncate the values of individual fields depending on the bit width you specify.

- **nas-port-id-delimiter**—The character used as the separator between values in the NAS-Port-ID string.
- **nas-port-id-format**—Optional information included in RADIUS attribute 87 (NAS-Port-ID).
- **nas-port-type**—The port type used to authenticate subscribers.
- **revert-interval**—The number of seconds that the router waits after a server has become unreachable. The router rechecks the connection to the server when the **revert-interval**

expires. If the server is then reachable, it is used in accordance with the order of the server list. You can configure from 0 (off) through 604800 seconds. The default is 60 seconds.

- **vlan-nas-port-stacked-format**—The format that turns off RADIUS attribute 5 (NAS-Port) to include the S-VLAN ID, in addition to the VLAN ID, for subscribers on Ethernet interfaces.

**Related
Documentation**

- [Configuring RADIUS Server Options for Subscriber Access on page 102](#)

Global RADIUS Options for Subscriber Access

You can specify options that the router uses when communicating with all configured RADIUS servers for subscriber access.

The following list describes the global RADIUS options you can configure:

- **revert-interval**—The number of seconds that the router waits after a server has become unreachable. The router rechecks the connection to the server when the **revert-interval** expires. If the server is then reachable, it is used in accordance with the order of the server list. You can configure from 0 (off) through 604800 seconds. The default is 60 seconds.
- **request-rate**—The number of requests per second that the router can send to all configured RADIUS servers collectively. By limiting the flow of requests from the router to the RADIUS servers, you can prevent the RADIUS servers from being flooded with requests. You can configure from 500 through 4000 requests per second. The default is 500 requests per second.

**Related
Documentation**

- [Configuring RADIUS Options for Subscriber Access Globally on page 105](#)
- [request-rate on page 908](#)
- [revert-interval on page 911](#)

Subscriber Access Interface Description Storage and Reporting Through RADIUS Overview

You can configure Junos OS to store subscriber access interface descriptions and report the interface description through RADIUS. This capability enables you to uniquely identify subscribers on a particular logical or physical interface. When you enable storing of the interface descriptions, RADIUS requests include the interface description in VSA 26-63, if the subscriber's access interface has been configured with an interface description. All interface descriptions must be statically configured using the Junos OS CLI. Storing and reporting of interface descriptions is supported for DHCP, PPP, and authenticated dynamic VLANs, and applies to any client session that either authenticates or uses the RADIUS accounting service. The description can contain letters, numbers, and hyphens (-), and can be up to 64 characters long.

You can enable or disable storage and reporting of interface descriptions as follows:

- To enable storing and reporting of interface descriptions, include the **report-interface-descriptions** statement at the **[edit access]** hierarchy level.
- To disable storing and reporting of interface descriptions, include the **radius attributes exclude** statement at the **[edit access profile *profile-name*]** hierarchy level.

Interface Description Precedence

The interface description sent in the VSA depends on the configured interface. Two configuration models apply across topologies and protocols for subscriber management.

- Subscriber logical interface directly over a physical interface (non-underlying logical interfaces).
- Subscriber logical interface over an underlying logical interface and physical interface.

In both models, Junos OS selects the interface description to report based on order of precedence. Interfaces not configured with interface descriptions are excluded when selecting an interface by precedence. If no interface description is configured on any of the static interfaces in the subscriber interface hierarchy, VSA 26-63 is not sent in any of the RADIUS messages.

Example: Reporting Interface Descriptions on Non-Underlying Logical Interfaces

This topic shows an example of subscriber access with non-underlying logical interfaces. In this case, the logical interface can be a VLAN or a VLAN demux interface. This example shows a DHCP subscriber logical interface over a VLAN without a demux interface. For non-underlying interfaces, Junos OS selects which interface description to report based on the following order of precedence:

1. Logical interface description
2. Physical interface description

Based on the order of precedence that Junos OS uses to select the interface description for non-underlying interfaces, Junos OS reports `subscriber_ifl_descr` as the interface description.

```
system {
  services {
    dhcp-local-server {
      group LSG1 {
        authentication {
          password radius;
          username-include {
            user-prefix rich;
          }
        }
      }
      interface ge-1/0/0.100;
    }
  }
}
```

```

interfaces {
  ge-1/0/0 {
    description subscriber_ifd_descr;
    vlan-tagging;
    unit 100 {
      description subscriber_ifl_descr;
      vlan-id 100;
      family inet {
        unnumbered-address lo0.0 preferred-source-address 100.20.0.1;
      }
    }
  }
}

```

Reporting Interface Descriptions on Underlying Logical Interfaces

Underlying logical interfaces can apply to both DHCP and PPP.

For DHCP, Junos OS selects which interface description to report based on the following order of precedence:

1. Underlying logical interface description
2. Underlying physical interface description



NOTE: For DHCP, Junos OS does not report the IP demux logical interface description.

For PPP over an underlying VLAN or VLAN demux interface, Junos OS selects which interface description to report based on the following order of precedence:

1. PPP interface description
2. Underlying VLAN without a demux interface or VLAN demux logical interface description
3. Underlying physical interface description

Example: PPP over an Underlying VLAN Demux Interface

The following example shows a PPP subscriber over an underlying VLAN demux interface. This configuration includes three possible interface descriptions. Based on the order of precedence that Junos OS uses to select the interface description for PPP, the interface description is reported as subscriber_ppp_ifl_descr_0.

```

interfaces {
  ge-1/0/0 {
    description subscriber_ifd_descr;
    hierarchical-scheduler maximum-hierarchy-levels 2;
    flexible-vlan-tagging;
  }
  demux0 {
    unit 0 {
      vlan-tags outer 1 inner 1;
      description subscriber_under_ifl_descr_1_1;
      demux-options {

```

```
        underlying-interface ge-1/0/0;
    }
    family pppoe {
        duplicate-protection;
    }
}
unit 1 {
    vlan-tags outer 1 inner 2;
    description subscriber_under_ifl_descr_1_2;
    demux-options {
        underlying-interface ge-1/0/0;
    }
    family pppoe {
        duplicate-protection;
    }
}
}
pp0 {
    unit 0 {
        description subscriber_ppp_ifl_descr_0;
        ppp-options {
            chap;
            pap;
        }
        pppoe-options {
            underlying-interface demux0.0;
            server;
        }
    }
    unit 1 {
        description subscriber_ppp_ifl_descr_1;
        ppp-options {
            chap;
            pap;
        }
        pppoe-options {
            underlying-interface demux0.1;
            server;
        }
    }
}
}
```

Interface Descriptions on Aggregated Ethernet Physical Interfaces

For aggregated Ethernet interfaces, the interface description on the aggregated Ethernet interface, for example AEO or AE1, serves as the physical interface description.

Interface Descriptions on a Combination of Dynamic and Static Interfaces

If the subscriber's access is a combination of dynamic and static interfaces, Junos OS uses the description on the static interface.

Example: Reporting Interface Descriptions on Dynamic VLANs

If you create dynamic VLANs with authentication, Junos OS reports the interface description on the physical interface. In the following example, dynamic VLANs created

over the ge-1/2/0 interface are authenticated with an interface description of ge-1/2/0-bos-mktg-group.

```
ge-1/2/0 {
  description ge-1/2/0-bos-mktg-group;
  flexible-vlan-tagging;
  auto-configure {
    vlan-ranges {
      dynamic-profile vlan-prof {
        accept inet;
        ranges {
          any;
        }
      }
    }
    authentication {
      password radius;
      username-include {
        user-prefix rich;
      }
    }
  }
}
```

**Related
Documentation**

- [report-interface-descriptions \(Edit Access\) on page 901](#)
- [exclude on page 724](#)
- [Configuring RADIUS Server Options for Subscriber Access on page 102](#)
- [Configuring Authentication and Accounting Parameters for Subscriber Access on page 80](#)

CHAPTER 2

Configuring RADIUS Attributes and Juniper Networks VSAs

- [RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework on page 13](#)
- [RADIUS IETF Attributes Supported by the AAA Service Framework on page 14](#)
- [Juniper Networks VSAs Supported by the AAA Service Framework on page 21](#)
- [AAA Access Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS on page 31](#)
- [AAA Accounting Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS on page 37](#)
- [Configuring How RADIUS Attributes Are Used for Subscriber Access on page 40](#)
- [Junos OS Predefined Variables That Correspond to RADIUS Attributes and VSAs on page 46](#)
- [DSL Forum Vendor-Specific Attributes on page 51](#)
- [DSL Forum VSAs Support in AAA Access and Accounting Messages for Junos OS on page 53](#)

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

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

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

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

Related Documentation

- [RADIUS IETF Attributes Supported by the AAA Service Framework on page 14](#)
- [Juniper Networks VSAs Supported by the AAA Service Framework on page 21](#)
- [DSL Forum Vendor-Specific Attributes on page 51](#)
- [AAA Access Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS on page 31](#)
- [AAA Accounting Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS on page 37](#)
- [Junos OS Predefined Variables That Correspond to RADIUS Attributes and VSAs on page 46](#)

RADIUS IETF Attributes Supported by the AAA Service Framework

Table 3 on page 14 describes the RADIUS IETF attributes that the Junos OS AAA Service Framework supports.



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

Table 3: Supported RADIUS IETF Attributes

Attribute Number	Attribute Name	Description	Dynamic CoA Support
1	User-Name	<ul style="list-style-type: none"> • Name of user to be authenticated. • Configurable username override. • Non-standard use for LLID preauthentication feature. 	No
2	User-Password	<ul style="list-style-type: none"> • Password of user to be authenticated by Password Authentication Protocol (PAP). • Configurable password override. • Non-standard use for LLID preauthentication feature. 	No
4	NAS-IP-Address	IP address of the network access server (NAS) that is requesting authentication of the user.	No
5	NAS-Port	<p>Physical port number of the NAS that is authenticating the user.</p> <p>For a tunneled PPP user in an L2TP LNS session, there is no physical port. In this case, the port value is reported as 4194303.</p>	No

Table 3: Supported RADIUS IETF Attributes (*continued*)

Attribute Number	Attribute Name	Description	Dynamic CoA Support
6	Service-Type	Type of service the user has requested or the type of service to be provided.	No
8	Framed-IP-Address	<ul style="list-style-type: none"> IP address to be configured for the user. 0.0.0.0 or absence is interpreted as 255.255.255.254. 	No
9	Framed-IP-Netmask	<ul style="list-style-type: none"> IP network to be configured for the user when the user is a router or switch to a network. Absence implies 255.255.255.255. 	No
11	Filter-Id	<p>Name of a subscriber firewall filter, formatted as follows:</p> <ul style="list-style-type: none"> For an IPv4 input filter—IPv4-ingress:<i>ingress-filter-name</i> For an IPv4 output filter—IPv4-egress:<i>egress-filter-name</i> For an IPv6 input filter—IPv6-ingress:<i>ingress-filter-name</i> For an IPv6 output filter—IPv6-egress:<i>egress-filter-name</i> <p>RADIUS accounting request messages, Acct-Start and Acct-Stop, can include more than one Filter-Id attribute, one of each of the listed types.</p> <p>However, RADIUS Access-Accept messages can include only one attribute instance. The value is always treated as an IPv4 input filter name.</p>	Yes
18	Reply-Message	<ul style="list-style-type: none"> Text that may be displayed to the user. Only the first instance of this attribute is used. 	No
22	Framed-Route	<p>String that provides routing information to be configured for the user on the NAS in the format:</p> <pre><addr>[/<maskLen>] [<nexthop> [<cost>]] [tag <tagValue>] [distance <distValue>]</pre>	Yes
25	Class	Arbitrary value that the NAS includes in all accounting packets for the user if supplied by the RADIUS server.	No

Table 3: Supported RADIUS IETF Attributes (*continued*)

Attribute Number	Attribute Name	Description	Dynamic CoA Support
27	Session-Timeout	Maximum number of consecutive seconds of service to be provided to the user before termination of the session.	No
31	Calling-Station-ID	Phone number from which the call originated.	No
32	NAS-Identifier	NAS originating the request.	No
40	Acct-Status-Type	Whether this Accounting-Request marks the beginning of the user service (Start), the end (Stop), or the interim (Interim-Update).	No
41	Acct-Delay-Time	Number of seconds the client has been trying to send a particular record.	No
42	Acct-Input-Octets	Number of octets that have been received from the port during the time this service has been provided.	No
43	Acct-Output-Octets	Number of octets that have been sent to the port during the time this service has been provided.	No
44	Acct-Session-ID	<p>Unique accounting identifier that makes it easy to match start and stop records in a log file. The identifier can be in one of the following formats:</p> <ul style="list-style-type: none"> decimal—For example, 435264 description—In the generic format, <i>jnpr interface-specifier:subscriber-session-id</i>; For example, <i>jnpr fastEthernet 3/2.6:1010101010101</i> 	No
45	Acct-Authentic	Method by which user was authentication: whether by RADIUS, the NAS itself, or another remote authentication protocol.	No
46	Acct-Session-Time	Number of seconds that the user has received service	No
47	Acct-Input-Packets	Number of packets that have been received from the port during the time this service has been provided to a framed user.	No

Table 3: Supported RADIUS IETF Attributes (*continued*)

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

Table 3: Supported RADIUS IETF Attributes (*continued*)

Attribute Number	Attribute Name	Description	Dynamic CoA Support
61	NAS-Port-Type	Type of physical port the NAS is using to authenticate the user. For a tunneled PPP user in an L2TP LNS session, there is no physical port. In this case, the port type is Virtual .	No
64	Tunnel-Type	<ul style="list-style-type: none"> Tunneling protocol to use (in the case of a tunnel initiator) or the tunneling protocol already in use (in the case of a tunnel terminator). Only L2TP tunnels are currently supported. 	No
65	Tunnel-Medium-Type	<ul style="list-style-type: none"> Transport medium to use when creating a tunnel for protocols that can operate over multiple transports. Only IPv4 is currently supported. 	No
66	Tunnel-Client-Endpoint	Address of the initiator end of the tunnel (LAC).	No
67	Tunnel-Server-Endpoint	Address of the server end of the tunnel (LNS).	No
69	Tunnel-Password	Encrypted password used to authenticate to a remote server. Recommended over using VSA Tunnel-Password [26-9] because of the encryption. Do not use both this attribute and the VSA.	No
77	Connect-Info	<ul style="list-style-type: none"> Information sent from the NAS that describes the subscriber's connection, such as transmit speed. Non-standard use for LLID preauthentication feature. 	No
82	Tunnel-Assignment -Id	Tunnel to which a session is assigned. When user profiles share the same values for Tunnel-Assignment-Id, Tunnel-Server-Endpoint, and Tunnel-Type, the LAC can group these users into the same tunnel. This grouping enables fewer tunnels to be created. (LAC)	No

Table 3: Supported RADIUS IETF Attributes (*continued*)

Attribute Number	Attribute Name	Description	Dynamic CoA Support
83	Tunnel-Preference	<ul style="list-style-type: none"> Included in each set of tunneling attributes to indicate the relative preference assigned to each tunnel when more than one set of tunneling attributes is returned by the RADIUS server to the tunnel initiator. Included in the Tunnel-Link-Start, the Tunnel-Link-Reject, and the Tunnel-Link-Stop packets (LAC only). 	No
85	Acct-Interim-Interval	<p>Number of seconds between each interim accounting update for this session.</p> <p>The router uses the following guidelines for interim accounting:</p> <ul style="list-style-type: none"> Attribute value is within the acceptable range (from 600 through 86,400 seconds)—Accounting is updated at the specified interval. Attribute value of 0—No RADIUS accounting is performed. Attribute value is less than the minimum acceptable value—Accounting is updated at the minimum interval (600 seconds). Attribute value is greater than the maximum acceptable value—Accounting is updated at the maximum interval (86,400 seconds). <p>NOTE: Values are rounded up to the next higher multiple of 10 minutes. For example, a setting of 900 seconds (15 minutes) is rounded up to 20 minutes (1200 seconds).</p>	No

Table 3: Supported RADIUS IETF Attributes (*continued*)

Attribute Number	Attribute Name	Description	Dynamic CoA Support
87	NAS-Port-Id	Text string that identifies the physical interface of the NAS that is authenticating the user. For a tunneled PPP user in an L2TP LNS session, there is no physical port, and the NAS-Port-Id value has the following format: <i>media:local address:peer address:local tunnel id:peer tunnel id:local session id:peer session id:call serial number</i> . For example, Ip:172.20.0.1:192.168.0.2:3341:21031:16138:11846:2431. The local information refers to the LNS and the peer information refers to the LAC.	No
88	Framed-Pool	Name of an assigned address pool to use to assign an address for the user.	No
90	Tunnel-Client-Auth-Id	Name of the tunnel initiator (LAC) used during the authentication phase of tunnel establishment.	No
91	Tunnel-Server-Auth-Id	Name of the tunnel terminator (LNS) used during the authentication phase of tunnel establishment.	No
95	NAS-IPv6-Address	Address of the NAS that is requesting authentication of the user.	No
96	Framed-Interface-ID	Interface identifier that is configured for the user.	No
97	Framed-IPv6-Prefix	IPv6 prefix and address that are configured for the user. Prefix lengths of 128 are associated with host addresses. Prefix lengths less than 128 are associated with NDRA prefixes.	No
98	Login-IPv6-Host	System the user connects to when the Login-Service attribute is included.	No
99	Framed-IPv6-Route	IPv6 routing information that is configured for the user.	Yes
100	Framed-IPv6-Pool	Name of the assigned pool used to assign the address and IPv6 prefix for the user.	No
123	Delegated-IPv6-Prefix	IPv6 prefix that is delegated to the user.	No

Table 3: Supported RADIUS IETF Attributes (*continued*)

Attribute Number	Attribute Name	Description	Dynamic CoA Support
242	Ascend-Data-Filter	Binary data that specifies RADIUS policy definitions.	Yes

Related Documentation

- [AAA Access Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS on page 31](#)
- [AAA Accounting Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS on page 37](#)

Juniper Networks VSAs Supported by the AAA Service Framework

Table 4 on page 22 describes Juniper Networks VSAs supported by the Junos OS AAA Service Framework. The AAA Service Framework uses vendor ID 4874, which is assigned to Juniper Networks by the Internet Assigned Numbers Authority (IANA).



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

Table 4: Supported Juniper Networks VSAs

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-1	Virtual-Router	<p>Client logical system:routing instance name. Allowed only from AAA server for “default” logical system:routing instance.</p> <p>When this VSA is not included in the subscriber profile, the routing instance assigned to the subscriber—the one in which the subscriber session comes up—varies by subscriber type.</p> <p>For DHCP and PPPoE subscribers, it is the default routing instance.</p> <p>For L2TP tunnel subscribers, it is the routing instance in which the tunnel resides, whether default or non-default. If the tunnel routing instance is not default and you want the L2TP session to be in the default routing instance, you must use the Virtual-Router VSA to set the desired routing instance.</p>	string: <i>logical system:routing instance</i>	No
26-4	Primary-DNS	Client DNS address negotiated during IPCP.	integer: 4-byte <i>primary-dns-address</i>	No
26-5	Secondary-DNS	Client DNS address negotiated during IPCP	integer: 4-byte <i>secondary-dns-address</i>	No
26-6	Primary-WINS	Client WINS (NBNS) address negotiated during IPCP.	integer: 4-byte <i>primary-wins-address</i>	No
26-7	Secondary-WINS	Client WINS (NBNS) address negotiated during IPCP.	integer: 4-byte <i>secondary-wins-address</i>	No
26-8	Tunnel-Virtual-Router	Virtual router name for tunnel connection.	string: <i>tunnel-virtual-router</i>	No
26-9	Tunnel-Password	<p>Tunnel password in cleartext.</p> <p>Do not use both this VSA and the standard RADIUS attribute Tunnel-Password [69]. The standard attribute is recommended because the password is encrypted when that attribute is used.</p>	string: <i>tunnel-password</i>	No
26-10	Ingress-Policy-Name	Input policy name to apply to client interface.	string: <i>input-policy-name</i>	Yes

Table 4: Supported Juniper Networks VSAs (*continued*)

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-11	Egress-Policy-Name	Output policy name to apply to client interface.	string: <i>output-policy-name</i>	Yes
26-23	IGMP-Enable	Whether IGMP is enabled or disabled on a client interface.	integer: <ul style="list-style-type: none"> • 0=disable • 1=enable 	Yes
26-25	Redirect-VRouter-Name	Client logical system:routing instance name indicating to which logical system:routing instance the request is redirected for user authentication.	string: <i>logical-system:routing-instance</i>	No
26-30	Tunnel-Nas-Port-Method	Method that determines whether the RADIUS server conveys to the LNS the physical NAS port number identifier and the type of the physical port, such as Ethernet or ATM. This information is conveyed only when the VSA value is 1. The VSA is formatted such that the first octet indicates the tunnel and the remaining three bytes are the attribute value.	4-octet integer: <ul style="list-style-type: none"> • 0 = none • 1 = Cisco CLID 	Yes
26-31	Service-Bundle	The SSC service bundle.	string <i>bundle-name</i>	No
26-33	Tunnel-Max-Sessions	Maximum number of sessions allowed in a tunnel.	integer: 4-octet	No
26-34	Framed-IP-Route-Tag	Route tag to apply to returned framed-ip-address.	integer: 4-octet	No
26-42	Input-Gigapackets	Number of times the input-packets attribute rolls over its 4-octet field.	Integer	No
26-43	Output-Gigapackets	Number of times the output-packets attribute rolls over its 4-octet field.	Integer	No
26-47	Ipv6-Primary-DNS	Client primary IPv6 DNS address negotiated by DHCP.	hexadecimal string: <i>ipv6-primary-dns-address</i>	No
26-48	Ipv6-Secondary-DNS	Client secondary IPv6 DNS address negotiated by DHCP.	hexadecimal string: <i>ipv6-secondary-dns-address</i>	No

Table 4: Supported Juniper Networks VSAs (*continued*)

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-51	Tunnel-Disconnect-Cause-Info	Disconnect cause when a tunneled subscriber is disconnected, and the termination is initiated by the L2TP layer of the LNS. The PPP Disconnect Cause Code (L2TP AVP 46) is included in VSA 26-51 in the Accounting-Stop message that the router sends to the RADIUS server.	hexadecimal string: <i>tunnel-disconnect-cause-info</i>	No
26-55	DHCP-Options	Client DHCP options.	string: <i>dhcp-options</i>	No
26-56	DHCP-MAC-Address	Client MAC address.	string: <i>mac-address</i>	No
26-57	DHCP-GI-Address	DHCP relay agent IP address.	integer: 4-octet	No
26-58	LI-Action	<p>Traffic mirroring action.</p> <p>For dynamic CoA, VSA 26-58 changes the action on the mirrored traffic identified by VSA 26-59.</p> <p>CoA-Request messages that include any of the RADIUS-based mirroring attributes (VSAs 26-58, 26-59, 26-60, or 26-61) must always include all four VSAs.</p> <p>If the CoA action is to stop mirroring (VSA 26-58 value is 0), then the values of the other three attributes in the CoA message must match the existing attribute values, or the action fails.</p>	<p>Salt-encrypted integer</p> <p>0=stop mirroring 1=start mirroring 2=no action</p>	Yes
26-59	Med-Dev-Handle	<p>Identifier that associates mirrored traffic to a specific subscriber.</p> <p>For dynamic CoA, VSA 26-58 changes the action on the mirrored traffic identified by VSA 26-59.</p> <p>CoA-Request messages that include any of the RADIUS-based mirroring attributes (VSAs 26-58, 26-59, 26-60, or 26-61) must always include all four VSAs.</p>	Salt-encrypted string	No

Table 4: Supported Juniper Networks VSAs (*continued*)

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-60	Med-Ip-Address	IP address of content destination device to which mirrored traffic is forwarded. CoA-Request messages that include any of the RADIUS-based mirroring attributes (VSAs 26–58, 26–59, 26–60, or 26–61) must always include all four VSAs.	Salt-encrypted IP address	No
26-61	Med-Port-Number	UDP port in the content destination device to which mirrored traffic is forwarded. CoA-Request messages that include any of the RADIUS-based mirroring attributes (VSAs 26–58, 26–59, 26–60, or 26–61) must always include all four VSAs.	Salt-encrypted integer	No
26-63	Interface-Desc	Text string that identifies the subscriber's access interface.	string: <i>interface-description</i>	No
26-64	Tunnel-Group	Name of the tunnel group (profile) assigned to a domain map.	string: <i>tunnel-group-name</i>	No
26-65	Activate-Service	Service to activate for the subscriber. Tagged VSA, which supports 8 tags (1-8).	string: <i>service-name</i>	Yes
26-66	Deactivate-Service	Service to deactivate for the subscriber.	string: <i>service-name</i>	No
26-67	Service-Volume	Amount of traffic, in MB, that can use the service; service is deactivated when the volume is exceeded. Tagged VSA, which supports 8 tags (1-8).	<ul style="list-style-type: none"> range = 0 through 16777215 MB 0 = no limit 	Yes
26-68	Service-Timeout	Number of seconds that the service can be active; service is deactivated when the timeout expires. Tagged VSA, which supports 8 tags (1-8).	<ul style="list-style-type: none"> range = 0 through 16777215 seconds 0 = no timeout 	Yes
26-69	Service-Statistics	Whether statistics for the service is enabled or disabled. Tagged VSA, which supports 8 tags (1-8).	<ul style="list-style-type: none"> 0 = disable 1 = enable time statistics 2 = enable time and volume statistics 	Yes
26-71	IGMP-Access-Name	Access list to use for the group (G) filter.	string: 32-octet	Yes

Table 4: Supported Juniper Networks VSAs (*continued*)

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-72	IGMP-Access-Src-Name	Access list to use for the source-group (S,G) filter.	string: 32-octet	Yes
26-74	MLD-Access-Name	Access list to use for the group (G) filter.	string: 32-octet	Yes
26-75	MLD-Access-Src-Name	Access list to use for the source-group (S,G) filter.	string: 32-octet	Yes
26-77	MLD-Version	MLD protocol version.	integer: 1-octet <ul style="list-style-type: none"> 1=MLD version 1 2=MLD version 2 	Yes
26-78	IGMP-Version	IGMP protocol version.	integer: 1-octet <ul style="list-style-type: none"> 1=IGMP version 1 2=IGMP version 2 3=IGMP version 3 	Yes
26-83	Service-Session	Name of the service.	string: <i>service-name</i>	No
26-84	Mobile-IP-Algorithm	Authentication algorithm used for Mobile IP registration.	integer: 4-octet	No
26-85	Mobile-IP-SPI	Security parameter index number for Mobile IP registration.	integer: 4-octet	No
26-86	Mobile-IP-Key	Security association MD5 key for Mobile IP registration.	string: key	No
26-87	Mobile-IP-Replay	Replay timestamp for Mobile IP registration.	integer: 4-octet	No
26-89	Mobile-IP-Lifetime	Registration lifetime for Mobile IP registration.	integer: 4-octet	No
26-91	Tunnel-Switch-Profile	Tunnel switch profile that determines whether a subscriber session is switched to a second session to a remote LNS. Takes precedence over tunnel switch profiles applied in any other manner,	string: <i>profile-name</i>	No
26-92	L2C-Up-Stream-Data	Actual upstream rate access loop parameter (ASCII encoded) as defined in GSMP extensions for layer2 control (L2C) Topology Discovery and Line Configuration.	string: actual upstream rate access loop parameter (ASCII encoded)	

Table 4: Supported Juniper Networks VSAs (*continued*)

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-93	L2C-Down-Stream-Data	Actual downstream rate access loop parameter (ASCII encoded) as defined in GSMP extensions for layer2 control (L2C) Topology Discovery and Line Configuration.	string: actual downstream rate access loop parameter (ASCII encoded)	
26-97	IGMP-Immediate-Leave	IGMP Immediate Leave.	integer: 4-octet <ul style="list-style-type: none"> 0=disable 1=enable 	Yes
26-100	MLD-Immediate-Leave	MLD Immediate Leave.	integer: 4-octet <ul style="list-style-type: none"> 0=disable 1=enable 	Yes
26-106	IPv6-Ingress-Policy-Name	Input policy name to apply to a user IPv6 interface.	string: <i>policy-name</i>	Yes
26-107	IPv6-Egress-Policy-Name	Output policy name to apply to a user IPv6 interface.	string: <i>policy-name</i>	Yes
26-108	CoS-Traffic-Control-Profile-Parameter-Type	CoS traffic-shaping parameter type and description: <ul style="list-style-type: none"> T01: Scheduler-map name T02: Shaping rate T03: Guaranteed rate T04: Delay-buffer rate T05: Excess rate T06: Traffic-control profile T07: Shaping mode T08: Byte adjust T09: Adjust minimum T10: Excess-rate high T11: Excess-rate low T12: Shaping rate burst T13: Guaranteed rate burst 	Two parts, delimited by white space: <ul style="list-style-type: none"> Parameter type Parameter value Examples: <ul style="list-style-type: none"> T01 smap_basic T02 50m T03 1m T04 2000 T05 200 T06 tcp-gold T07 frame-mode T08 50 	Yes
26-109	DHCP-Guided-Relay-Server	IP address of DHCP server that DHCP relay agent uses to forward the discover PDUs.	integer: 4-byte <i>ip-address</i>	No
26-110	Acc-Loop-Cir-Id	Identification of the subscriber node connection to the access node.	string: up to 63 ASCII characters	
26-111	Acc-Aggr-Cir-Id-Bin	Unique identification of the DSL line.	integer: 8-octet	

Table 4: Supported Juniper Networks VSAs (*continued*)

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-112	Acc-Aggr-Cir-Id-Asc	<p>Identification of the uplink on the access node, as in the following examples:</p> <ul style="list-style-type: none"> Ethernet access aggregation—ethernet slot/port [:inner-vlan-id] [:outer-vlan-id] ATM aggregation—atm slot/port:vpi.vci 	string: up to 63 ASCII characters	
26-113	Act-Data-Rate-Up	Actual upstream data rate of the subscriber's synchronized DSL link.	integer: 4-octet	
26-114	Act-Data-Rate-Dn	Actual downstream data rate of the subscriber's synchronized DSL link.	integer: 4-octet	
26-115	Min-Data-Rate-Up	Minimum upstream data rate configured for the subscriber.	integer: 4-octet	
26-116	Min-Data-Rate-Dn	Minimum downstream data rate configured for the subscriber.	integer: 4-octet	
26-117	Att-Data-Rate-Up	Maximum upstream data rate that the subscriber can attain.	integer: 4-octet	
26-118	Att-Data-Rate-Dn	Maximum downstream data rate that the subscriber can attain.	integer: 4-octet	
26-119	Max-Data-Rate-Up	Maximum upstream data rate configured for the subscriber.	integer: 4-octet	
26-120	Max-Data-Rate-Dn	Maximum downstream data rate configured for the subscriber.	integer: 4-octet	
26-121	Min-LP-Data-Rate-Up	Minimum upstream data rate in low power state configured for the subscriber.	integer: 4-octet	
26-122	Min-LP-Data-Rate-Dn	Minimum downstream data rate in low power state configured for the subscriber.	integer: 4-octet	
26-123	Max-Interlv-Delay-Up	Maximum one-way upstream interleaving delay configured for the subscriber.	integer: 4-octet	
26-124	Act-Interlv-Delay-Up	Subscriber's actual one-way upstream interleaving delay..	integer: 4-octet	

Table 4: Supported Juniper Networks VSAs (*continued*)

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-125	Max-Interlv-Delay-Dn	Maximum one-way downstream interleaving delay configured for the subscriber.	integer: 4-octet	
26-126	Act-Interlv-Delay-Dn	Subscriber's actual one-way downstream interleaving delay.	integer: 4-octet	
26-127	DSL-Line-State	State of the DSL line.	integer: 4-octet <ul style="list-style-type: none"> • 1 = Show uptime • 2 = Idle • 3 = Silent 	
26-128	DSL-Type	Encapsulation used by the subscriber associated with the DSLAM interface from which requests are initiated.		
26-130	Qos-Set-Name	Interface set to apply to the dynamic profile.	string: <i>interface-set-name</i>	No
26-140	Service-Interim-Acct-Interval	Amount of time between interim accounting updates for this service. Tagged VSA, which supports 8 tags (1-8).	<ul style="list-style-type: none"> • range = 600 through 86400 seconds • 0 = disabled <p>NOTE: Values are rounded up to the next higher multiple of 10 minutes. For example, a setting of 900 seconds (15 minutes) is rounded up to 20 minutes (1200 seconds).</p>	Yes
26-141	Downstream-Calculated-QoS-Rate	Calculated (adjusted) downstream QoS rate in Kbps as set by the ANCP configuration.	range = 1000 through 4,294,967,295	
26-142	Upstream-Calculated-QoS-Rate	Calculated (adjusted) upstream QoS rate in Kbps as set by the ANCP configuration.	range = 1000 through 4,294,967,295	
26-143	Max-Clients-Per-Interface	Maximum allowable client sessions per interface. For DHCP clients, this value is the maximum sessions per logical interface. For PPPoE clients, this value is the maximum sessions (PPPoE interfaces) per PPPoE underlying interface.	integer: 4-octet	No

Table 4: Supported Juniper Networks VSAs (continued)

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-146	CoS-Scheduler-Pmt-Type	CoS scheduler parameter type and description: <ul style="list-style-type: none"> • Null: CoS scheduler name • T01: CoS scheduler transmit rate • T02: CoS scheduler buffer size • T03: CoS scheduler priority • T04: CoS scheduler drop-profile low • T05: CoS scheduler drop-profile medium-low • T06: CoS scheduler drop-profile medium-high • T07: CoS scheduler drop-profile high • T08: CoS scheduler drop-profile any 	Three parts, delimited by white space: <ul style="list-style-type: none"> • Scheduler name • Parameter type • Parameter value Examples: <ul style="list-style-type: none"> • be_sched • be_sched T01 12m • be_sched T02 26 	Yes
26-151	IPv6-Acct-Input-Octets	IPv6 receive octets.	integer	No
26-152	IPv6-Acct-Output-Octets	IPv6 transmit octets.	integer	No
26-153	IPv6-Acct-Input-Packets	IPv6 receive packets.	integer	No
26-154	IPv6-Acct-Output-Packets	IPv6 transmit packets.	integer	No
26-155	IPv6-Acct-Input-Gigawords	IPv6 receive gigawords.	integer	No
26-156	IPv6-Acct-Output-Gigawords	IPv6 transmit gigawords.	integer	No
26-158	PPPoE-Padn	Route add for PPPoE sessions	string	No
26-161	IPv6-Delegated-Pool-Name	Address pool used to locally allocate a delegated prefix (IA_PD).	string	No
26-162	Tx-Connect-Speed	Indication of user's connection.	string	No
26-163	Rx-Connect-Speed	Indication of user's connection.	string	No
26-173	Service-Activate-Type	Indication of service activation type. This is a tagged attribute.	integer: 4-octet <ul style="list-style-type: none"> • 1 = dynamic-profile • 2 = op-script 	No
26-174	Client-Profile-Name	Enables RADIUS to override an assigned client dynamic profile with the included profile.	string	No

Table 4: Supported Juniper Networks VSAs (*continued*)

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-177	Cos-Shaping-Rate	Effective downstream shaping rate for subscriber.	string	No
26-179	Service-Volume-Gigawords	Amount of traffic, in 4GB units, that can use the service; service is deactivated when the volume is exceeded. Tagged VSA, which supports 8 tags (1-8).	<ul style="list-style-type: none"> range = 0 through 16777215 4GB units 0 = no limit 	Yes
26-180	Update-Service	New values of service and time quotas for existing service. Tagged VSA, which supports 8 tags (1-8).	string: <i>service-name</i>	Yes

Related Documentation

- [AAA Access Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS on page 31](#)
- [AAA Accounting Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS on page 37](#)

AAA Access Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS

Table 5 on page 31 shows the RADIUS attributes and Juniper Networks VSAs support in AAA access messages. A checkmark in a column indicates that the message type supports that attribute.

Table 5: AAA Access Messages—Supported RADIUS Attributes and Juniper Networks VSAs

Attribute Number	Attribute Name	Access Request	Access Accept	Access Reject	Access Challenge	CoA Request	Disconnect Request
1	User-Name	✓	✓	—	—	✓	✓
2	User-Password	✓	—	—	—	—	—
3	CHAP-Password	✓	—	—	—	—	—
4	NAS-IP-Address	✓	—	—	—	—	—
5	NAS-Port	✓	—	—	—	—	—
6	Service-Type	✓	✓	—	—	—	—
7	Framed-Protocol	✓	✓	—	—	—	—
8	Framed-IP-Address	✓	✓	—	—	✓	—

Table 5: AAA Access Messages—Supported RADIUS Attributes and Juniper Networks VSAs (*continued*)

Attribute Number	Attribute Name	Access Request	Access Accept	Access Reject	Access Challenge	CoA Request	Disconnect Request
9	Framed-IP-Netmask	–	✓	–	–	–	–
11	Filter-Id	–	✓	–	–	–	–
12	Framed-MTU	✓	–	–	–	–	–
18	Reply-Message	–	✓	✓	✓	–	–
22	Framed-Route	–	✓	–	–	–	–
25	Class	–	✓	–	–	–	–
26-1	Virtual-Router	–	✓	–	–	✓	–
26-4	Primary-DNS	–	✓	–	–	–	–
26-5	Secondary-DNS	–	✓	–	–	–	–
26-6	Primary-WINS	–	✓	–	–	–	–
26-7	Secondary-WINS	–	✓	–	–	–	–
26-8	Tunnel-Virtual-Router	–	✓	–	–	–	–
26-9	Tunnel-Password	–	✓	–	–	–	–
26-10	Ingress-Policy-Name	–	✓	–	–	–	–
26-11	Egress-Policy-Name	–	✓	–	–	–	–
26-23	IGMP-Enable	–	✓	–	–	–	–
26-25	Redirect-VR-Name	–	✓	–	–	–	–
26-31	Service-Bundle	–	✓	–	–	–	–
26-33	Tunnel-Maximum-Sessions	–	✓	–	–	–	–
26-34	Framed-IP-Route-Tag	–	✓	–	–	–	–
26-47	Ipv6-Primary-DNS	–	✓	–	–	–	–
26-48	Ipv6-Secondary-DNS	–	✓	–	–	–	–
26-55	DHCP-Options	✓	–	–	–	–	–

Table 5: AAA Access Messages—Supported RADIUS Attributes and Juniper Networks VSAs (continued)

Attribute Number	Attribute Name	Access Request	Access Accept	Access Reject	Access Challenge	CoA Request	Disconnect Request
26-56	DHCP-MAC-Address	✓	✓	–	–	–	–
26-57	DHCP-GI-Address	✓	–	–	–	–	–
26-58	LI-Action	–	✓	–	–	✓	–
26-59	Med-Dev-Handle	–	✓	–	–	✓	–
26-60	Med-Ip-Address	–	✓	–	–	✓	–
26-61	Med-Port-Number	–	✓	–	–	✓	–
26-63	Interface-Desc	✓	–	–	–	–	–
26-64	Tunnel-Group	–	✓	–	–	–	–
26-65	Activate-Service	–	✓	–	–	✓	–
26-66	Deactivate-Service	–	✓	–	–	✓	–
26-67	Service-Volume	–	✓	–	–	✓	–
26-68	Service-Timeout	–	✓	–	–	✓	–
26-69	Service-Statistics	–	✓	–	–	✓	–
26-71	IGMP-Access-Name	–	✓	–	–	–	–
26-72	IGMP-Access-Src-Name	–	✓	–	–	–	–
26-74	MLD-Access-Name	–	✓	–	–	–	–
26-75	MLD-Access-Src-Name	–	✓	–	–	–	–
26-77	MLD-Version	–	✓	–	–	–	–
26-78	IGMP-Version	–	✓	–	–	–	–
26–91	Tunnel-Switch-Profile	–	✓	–	–	–	–
26-97	IGMP-Immediate-Leave	–	✓	–	–	–	–
26-100	MLD-Immediate-Leave	–	✓	–	–	–	–
26-106	IPv6-Ingress-Policy-Name	–	✓	–	–	–	–

Table 5: AAA Access Messages—Supported RADIUS Attributes and Juniper Networks VSAs (*continued*)

Attribute Number	Attribute Name	Access Request	Access Accept	Access Reject	Access Challenge	CoA Request	Disconnect Request
26-107	IPv6-Egress-Policy-Name	–	✓	–	–	–	–
26-108	CoS-Parameter-Type	–	✓	–	–	✓	–
26-109	DHCP-Guided-Relay-Server	–	✓	–	–	–	–
26-110	Acc-Loop-Cir-Id	✓	–	–	–	–	–
26-111	Acc-Aggr-Cir-Id-Bin	✓	–	–	–	–	–
26-112	Acc-Aggr-Cir-Id-Asc	✓	–	–	–	–	–
26-113	Act-Data-Rate-Up	✓	–	–	–	–	–
26-114	Act-Data-Rate-Dn	✓	–	–	–	–	–
26-115	Min-Data-Rate-Up	✓	–	–	–	–	–
26-116	Min-Data-Rate-Dn	✓	–	–	–	–	–
26-117	Att-Data-Rate-Up	✓	–	–	–	–	–
26-118	Att-Data-Rate-Dn	✓	–	–	–	–	–
26-119	Max-Data-Rate-Up	✓	–	–	–	–	–
26-120	Max-Data-Rate-Dn	✓	–	–	–	–	–
26-121	Min-LP-Data-Rate-Up	✓	–	–	–	–	–
26-122	Min-LP-Data-Rate-Dn	✓	–	–	–	–	–
26-123	Max-Interlv-Delay-Up	✓	–	–	–	–	–
26-124	Act-Interlv-Delay-Up	✓	–	–	–	–	–
26-125	Max-Interlv-Delay-Dn	✓	–	–	–	–	–
26-126	Act-Interlv-Delay-Dn	✓	–	–	–	–	–
26-127	DSL-Line-State	✓	–	–	–	–	–
26-128	DSL-Type	✓	–	–	–	–	–
26-130	QoS-Set-Name	–	✓	–	–	–	–

Table 5: AAA Access Messages—Supported RADIUS Attributes and Juniper Networks VSAs (continued)

Attribute Number	Attribute Name	Access Request	Access Accept	Access Reject	Access Challenge	CoA Request	Disconnect Request
26-140	Service-Interim-Account-Interval	–	✓	–	–	✓	–
26-141	Downstream-Calculated-QoS-Rate	✓	–	–	–	–	–
26-142	Upstream-Calculated-QoS-Rate	✓	–	–	–	–	–
26-143	Max-Clients-Per-Interface	–	✓	–	–	–	–
26-146	Cos-Scheduler-Pmt-Type	–	✓	–	–	✓	–
26-158	PPPoE-Padn	–	✓	–	–	–	–
26-160	Vlan-Map-ID	–	✓	–	–	–	–
26-161	IPv6-Delegated-Pool-Name	–	✓	–	–	–	–
26-162	Tx-Connect-Speed	✓	–	–	–	–	–
26-163	Rx-Connect-Speed	✓	–	–	–	–	–
26-173	Service-Activate-Type	–	✓	–	–	✓	–
26-174	Client-Profile-Name	–	✓	–	–	–	–
26-179	Service-Volume-Gigawords	–	✓	–	–	✓	–
26-180	Update-Service	–	–	–	–	✓	–
27	Session-Timeout	–	✓	–	✓	–	–
31	Calling-Station-ID	✓	–	–	–	✓	–
32	NAS-Identifier	✓	–	–	–	–	–
44	Acct-Session-ID	✓	–	–	–	✓	✓
61	NAS-Port-Type	✓	–	–	–	–	–
64	Tunnel-Type	–	✓	–	–	–	–
65	Tunnel-Medium-Type	–	✓	–	–	–	–
66	Tunnel-Client-Endpoint	–	✓	–	–	–	–
67	Tunnel-Server-Endpoint	–	✓	–	–	–	–

Table 5: AAA Access Messages—Supported RADIUS Attributes and Juniper Networks VSAs (continued)

Attribute Number	Attribute Name	Access Request	Access Accept	Access Reject	Access Challenge	CoA Request	Disconnect Request
69	Tunnel-Password	–	✓	–	–	–	–
82	Tunnel-Assignment-Id	–	✓	–	–	–	–
83	Tunnel-Preference	–	✓	–	–	–	–
85	Acct-Interim-Interval	–	✓	–	–	–	–
87	NAS-Port-Id	✓	–	–	–	✓	–
88	Framed-Pool	–	✓	–	–	–	–
90	Tunnel-Client-Auth-Id	–	✓	–	–	–	–
91	Tunnel-Server-Auth-Id	–	✓	–	–	–	–
96	Framed-Interface-ID	–	✓	–	–	–	–
97	Framed-IPv6-Prefix	–	✓	–	–	–	–
99	Framed-IPv6-Route	–	✓	–	–	–	–
100	Framed-IPv6-Pool	–	✓	–	–	–	–
101	Error-Cause	–	–	–	–	✓	✓
123	Delegated-IPv6-Prefix	–	✓	–	–	–	–
242	Ascend-Data-Filter	–	✓	–	–	✓	–

Related Documentation

- [AAA Accounting Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS on page 37](#)
- [RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework on page 13](#)
- [RADIUS IETF Attributes Supported by the AAA Service Framework on page 14](#)
- [Juniper Networks VSAs Supported by the AAA Service Framework on page 21](#)

AAA Accounting Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS

Table 6 on page 37 shows the RADIUS attributes and Juniper Networks VSAs support in AAA accounting messages. A checkmark in a column indicates that the message type supports that attribute.

Table 6: AAA Accounting Messages—Supported RADIUS Attributes and Juniper Networks VSAs

Attribute Number	Attribute Name	Acct Start	Acct Stop	Interim Acct	Acct On	Acct Off
1	User-Name	✓	✓	✓	–	–
3	CHAP-Password	✓	–	–	–	–
4	NAS-IP-Address	✓	✓	✓	✓	✓
5	NAS-Port	✓	✓	✓	–	–
6	Service-Type	✓	✓	✓	–	–
7	Framed-Protocol	✓	✓	✓	–	–
8	Framed-IP-Address	✓	✓	✓	–	–
9	Framed-IP-Netmask	✓	✓	✓	–	–
11	Filter-Id	–	✓	✓	–	–
22	Framed-Route	✓	✓	✓	–	–
25	Class	✓	✓	✓	–	–
26-10	Ingress-Policy-Name	✓	✓	✓	–	–
26-11	Egress-Policy-Name	✓	✓	✓	–	–
26-42	Input-Gigapackets	–	✓	✓	–	–
26-43	Output-Gigapackets	–	✓	✓	–	–
26-47	Ipv6-Primary-DNS	✓	✓	✓	–	–
26-48	Ipv6-Secondary-DNS	✓	✓	✓	–	–
26-51	Tunnel-Disconnect-Cause-Info	–	✓	–	–	–
26-55	DHCP-Options	✓	✓	✓	–	–

Table 6: AAA Accounting Messages—Supported RADIUS Attributes and Juniper Networks VSAs (continued)

Attribute Number	Attribute Name	Acct Start	Acct Stop	Interim Acct	Acct On	Acct Off
26-56	DHCP-MAC-Address	✓	✓	✓	–	–
26-57	DHCP-GI-Address	✓	✓	✓	–	–
26-63	Interface-Desc	✓	✓	✓	–	–
26-83	Service-Session	–	✓	✓	–	–
26-110	Acc-Loop-Cir-Id	✓	✓	✓	–	–
26-111	Acc-Aggr-Cir-Id-Bin	✓	✓	✓	–	–
26-112	Acc-Aggr-Cir-Id-Asc	✓	✓	✓	–	–
26-113	Act-Data-Rate-Up	✓	✓	✓	–	–
26-114	Act-Data-Rate-Dn	✓	✓	✓	–	–
26-115	Min-Data-Rate-Up	✓	✓	✓	–	–
26-116	Min-Data-Rate-Dn	✓	✓	✓	–	–
26-117	Att-Data-Rate-Up	✓	✓	✓	–	–
26-118	Att-Data-Rate-Dn	✓	✓	✓	–	–
26-119	Max-Data-Rate-Up	✓	✓	✓	–	–
26-120	Max-Data-Rate-Dn	✓	✓	✓	–	–
26-121	Min-LP-Data-Rate-Up	✓	✓	✓	–	–
26-122	Min-LP-Data-Rate-Dn	✓	✓	✓	–	–
26-123	Max-Interlv-Delay-Up	✓	✓	✓	–	–
26-124	Act-Interlv-Delay-Up	✓	✓	✓	–	–
26-125	Max-Interlv-Delay-Dn	✓	✓	✓	–	–
26-126	Act-Interlv-Delay-Dn	✓	✓	✓	–	–
26-127	DSL-Line-State	✓	✓	✓	–	–
26-128	DSL-Type	✓	✓	✓	–	–

Table 6: AAA Accounting Messages—Supported RADIUS Attributes and Juniper Networks VSAs (*continued*)

Attribute Number	Attribute Name	Acct Start	Acct Stop	Interim Acct	Acct On	Acct Off
26-141	Downstream-Calculated-QoS-Rate	✓	✓	✓	–	–
26-142	Upstream-Calculated-QoS-Rate	✓	✓	✓	–	–
26-151	IPv6-Acct-Input-Octets	–	✓	✓	–	–
26-152	IPv6-Acct-Output-Octets	–	✓	✓	–	–
26-153	IPv6-Acct-Input-Packets	–	✓	✓	–	–
26-154	IPv6-Acct-Output-Packets	–	✓	✓	–	–
26-155	IPv6-Acct-Input-Gigawords	–	✓	✓	–	–
26-156	IPv6-Acct-Output-Gigawords	–	✓	✓	–	–
26-162	Tx-Connect-Speed	✓	✓	✓	–	–
26-163	Rx-Connect-Speed	✓	✓	✓	–	–
26-177	Cos-Shaping-Rate	✓	✓	✓	–	–
31	Calling-Station-ID	✓	✓	✓	–	–
32	NAS-Identifier	✓	✓	✓	–	–
40	Acct-Status-Type	✓	✓	✓	✓	✓
41	Acct-Delay-Time	✓	✓	✓	✓	✓
42	Acct-Input-Octets	–	✓	✓	–	–
43	Acct-Output-Octets	–	✓	✓	–	–
44	Acct-Session-ID	✓	✓	✓	✓	✓
45	Acct-Authentic	✓	✓	✓	✓	✓
46	Acct-Session-Time	–	✓	✓	–	–
47	Acct-Input-Packets	–	✓	✓	–	–
48	Acct-Output-Packets	–	✓	✓	–	–
49	Acct-Terminate-Cause	–	✓	✓	–	–

Table 6: AAA Accounting Messages—Supported RADIUS Attributes and Juniper Networks VSAs (continued)

Attribute Number	Attribute Name	Acct Start	Acct Stop	Interim Acct	Acct On	Acct Off
52	Acct-Input-Gigawords	–	✓	✓	–	–
53	Acct-Output-Gigawords	–	✓	✓	–	–
55	Event-Timestamp	✓	✓	✓	✓	✓
61	NAS-Port-Type	✓	✓	✓	–	–
64	Tunnel-Type	✓	✓	✓	–	–
65	Tunnel-Medium-Type	✓	✓	✓	–	–
66	Tunnel-Client-Endpoint	✓	✓	✓	–	–
67	Tunnel-Server-Endpoint	✓	✓	✓	–	–
82	Tunnel-Assignment-Id	✓	✓	✓	–	–
87	NAS-Port-Id	✓	✓	✓	–	–
90	Tunnel-Client-Auth-Id	✓	✓	✓	–	–
91	Tunnel-Server-Auth-Id	✓	✓	✓	–	–
99	Framed-IPv6-Route	✓	✓	✓	–	–
100	Framed-IPv6-Pool	✓	✓	✓	–	–
123	Delegated-IPv6-Prefix	✓	✓	✓	–	–

Related Documentation

- [AAA Access Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS on page 31](#)
- [RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework on page 13](#)
- [RADIUS IETF Attributes Supported by the AAA Service Framework on page 14](#)
- [Juniper Networks VSAs Supported by the AAA Service Framework on page 21](#)

Configuring How RADIUS Attributes Are Used for Subscriber Access

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

To configure the attributes RADIUS ignores or excludes:

1. Specify that you want to configure RADIUS.

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

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

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

3. Specify the attributes you want RADIUS to ignore when the attributes are in Access-Accept messages. See [Table 7 on page 41](#) for the attributes you can configure.

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

4. Configure RADIUS to exclude the specified attribute from the specified RADIUS message type. See [Table 8 on page 42](#) for the attributes and message type combinations you can configure.

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

You use the **ignore** statement to configure the router or switch to ignore a particular attribute in RADIUS Access-Accept messages. By default, the router or switch processes the attributes received from the external AAA server. [Table 7 on page 41](#) lists the attributes supported in the **ignore** statement.

Table 7: Attributes That Can Be Ignored in RADIUS Access-Accept Messages

CLI Entry	Attribute Name	Attribute Number
dynamic-iflset-name	Interface-Set-Name	Juniper Networks VSA 26-130
framed-ip-netmask	Framed-Ip-Netmask	RADIUS attribute 9
input-filter	Ingress-Policy-Name	Juniper Networks VSA 26-10
logical-system:routing-instance	Virtual-Router	Juniper Networks VSA 26-1
output-filter	Egress-Policy-Name	Juniper Networks VSA 26-11

You use the **exclude** statement to configure the router or switch to exclude the specified attributes from the specified type of RADIUS message. Not all attributes appear in all types of RADIUS messages—the CLI indicates the RADIUS message type. By default, the router or switch includes the specified attributes in RADIUS Access-Request, Acct-On, Acct-Off, Acct-Start, and Acct-Stop messages. [Table 8 on page 42](#) lists the attributes and message types supported in the **exclude** statement.

Table 8: Attributes That Can Be Excluded from RADIUS Messages

CLI Entry	Attribute Name	Attribute Number	Supported Message Type
accounting-authentic	Acct-Authentic	RADIUS attribute 45	Accounting-On Accounting-Off
accounting-delay-time	Acct-Delay-Time	RADIUS attribute 41	Accounting-On Accounting-Off
accounting-session-id	Acct-Session-Id	RADIUS attribute 44	Access-Request Accounting-On Accounting-Off Accounting-Stop
accounting-terminate-cause	Acct-Terminate-Cause	RADIUS attribute 49	Accounting-Off
called-station-id	Called-Station-Id	RADIUS attribute 30	Access-Request Accounting-Start Accounting-Stop
calling-station-id	Calling-Station-Id	RADIUS attribute 31	Access-Request Accounting-Start Accounting-Stop
class	Class	RADIUS attribute 25	Accounting-Start Accounting-Stop
cos-shaping-rate	Cos-Shaping-Rate	Juniper Networks VSA 26-177	Accounting-Start Accounting-Stop
delegated-ipv6-prefix	Delegated-IPv6-Prefix	RADIUS attribute 123	Accounting-Start Accounting-Stop
dhcp-gi-address	DHCP-GI-Address	Juniper Networks VSA 26-57	Access-Request Accounting-Start Accounting-Stop
dhcp-mac-address	DHCP-MAC-Address	Juniper Networks VSA 26-56	Access-Request Accounting-Start Accounting-Stop

Table 8: Attributes That Can Be Excluded from RADIUS Messages (*continued*)

CLI Entry	Attribute Name	Attribute Number	Supported Message Type
dhcp-options	DHCP-Options	Juniper Networks VSA 26–55	Access-Request Accounting-Start Accounting-Stop
downstream-calculated-qos-rate	Downstream-Calculated-QoS-Rate	Juniper Networks VSA 26-141	Access-Request Accounting-Start Accounting-Stop Interim-accounting
dsl-forum-attributes	Not applicable	Excludes the DSL Forum VSA (IANA vendor ID 3561)	Access-Request Accounting-Start Accounting-Stop Interim-accounting
dynamic-iflset-name	Qos-Set-Name	Juniper Networks VSA 26–130	Accounting-Start Accounting-Stop
event-timestamp	Event-Timestamp	RADIUS attribute 55	Accounting-On Accounting-Off Accounting-Start Accounting-Stop
filter-id	Filter-Id	RADIUS attribute 11	Accounting-Start Accounting-Stop
framed-ip-address	Framed-IP-Address	RADIUS attribute 8	Accounting-Start Accounting-Stop
framed-ip-netmask	Framed-IP-Netmask	RADIUS attribute 9	Accounting-Start Accounting-Stop
framed-ip-route	Framed-Route	RADIUS attribute 22	Accounting-Start Accounting-Stop

Table 8: Attributes That Can Be Excluded from RADIUS Messages (*continued*)

CLI Entry	Attribute Name	Attribute Number	Supported Message Type
framed-ipv6-pool	Framed-IPv6-Pool	RADIUS attribute 100	Accounting-Start Accounting-Stop
framed-ipv6-prefix	Framed-IPv6-Prefix	RADIUS attribute 97	Accounting-Start Accounting-Stop
framed-ipv6-route	Framed-IPv6-Route	RADIUS attribute 99	Accounting-Start Accounting-Stop
framed-pool	Framed-Pool	RADIUS attribute 88	Accounting-Start Accounting-Stop
input-filter	Ingress-Policy-Name	Juniper Networks VSA 26–10	Accounting-Start Accounting-Stop
input-gigapackets	Acct-Input-Gigapackets	Juniper Networks VSA 26–42	Accounting-Stop
input-gigawords	Acct-Input-Gigawords	RADIUS attribute 52	Accounting-Stop
input-ipv6-gigawords	IPv6-Acct-Input-Gigawords	Juniper Networks VSA 26–155	Accounting-Stop
input-ipv6-octets	IPv6-Acct-Input-Octets	Juniper Networks VSA 26–151	Accounting-Stop
input-ipv6-packets	IPv6-Acct-Input-Packets	Juniper Networks VSA 26–153	Accounting-Stop
interface-description	Interface-Desc	Juniper Networks VSA 26–53	Access-Request Accounting-Start Accounting-Stop
nas-identifier	NAS-Identifier	RADIUS attribute 32	Access-Request Accounting-on Accounting-off Accounting-Start Accounting-Stop

Table 8: Attributes That Can Be Excluded from RADIUS Messages (*continued*)

CLI Entry	Attribute Name	Attribute Number	Supported Message Type
nas-port	NAS-Port	RADIUS attribute 5	Access-Request Accounting-Start Accounting-Stop
nas-port-id	NAS-Port-Id	RADIUS attribute 87	Access-Request Accounting-Start Accounting-Stop
nas-port-type	NAS-Port-Type	RADIUS attribute 61	Access-Request Accounting-Start Accounting-Stop
output-filter	Egress-Policy-Name	Juniper Networks VSA 26–11	Accounting-Start Accounting-Stop
output-gigapackets	Acct-Output-Gigapackets	Juniper Networks VSA 26–43	Accounting-Stop
output-gigawords	Acct-Output-Gigawords	RADIUS attribute 53	Accounting-Stop
output-ipv6-gigawords	IPv6-Acct-Output-Gigawords	Juniper Networks VSA 26–156	Accounting-Stop
output-ipv6-octets	IPv6-Acct-Output-Octets	Juniper Networks VSA 26–152	Accounting-Stop
output-ipv6-packets	IPv6-Acct-Output-Packets	Juniper Networks VSA 26–154	Accounting-Stop
upstream-calculated-qos-rate	Upstream-Calculated-QoS-Rate	Juniper Networks VSA 26–142	Access-Request Accounting-Start Accounting-Stop Interim-accounting

Related Documentation

- [Configuring Router or Switch Interaction with RADIUS Servers on page 99](#)
- [Configuring Authentication and Accounting Parameters for Subscriber Access on page 80](#)

- [Specifying RADIUS Authentication and Accounting Servers for Subscriber Access on page 81](#)
- [Configuring RADIUS Server Options for Subscriber Access on page 102](#)
- [Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 82](#)

Junos OS Predefined Variables That Correspond to RADIUS Attributes and VSAs

Table 9 on page 46 lists the RADIUS attributes and Juniper Networks VSAs and their corresponding Junos OS predefined variables that are used in dynamic profiles. When the router instantiates a dynamic profile following subscriber access, the Junos OS uses the predefined variable to specify the RADIUS attribute or VSA for the information obtained from the RADIUS server.

Table 9: RADIUS Attributes and Corresponding Junos OS Predefined Variables

RADIUS Attribute or VSA	Junos OS Predefined Variable	Description	Default Value Support for Junos OS Predefined Variable
RADIUS Attribute			
Framed-IP-Address (8)	<code>\$junos-framed-route-ip-address</code>	Address for the client	No
Filter-ID (11)	<code>\$junos-input-filter</code> NOTE: Variable is also used for VSA 26–10.	Input filter to apply to client IPv4 interface	Yes
Framed-Route (22)	<code>\$junos-framed-route-ip-address-prefix</code>	(Subattribute 1): Route prefix for access route	No
	<code>\$junos-framed-route-nexthop</code>	(Subattribute 2): Next hop address for access route	No
	<code>\$junos-framed-route-cost</code>	(Subattribute 3): Metric for access route	No
	<code>\$junos-framed-route-distance</code>	(Subattribute 5): Preference for access route	No
	<code>\$junos-framed-route-tag</code>	(Subattribute 6): Tag for access route	No
Framed-IPv6-Prefix (97)	<code>\$junos-ipv6-ndra-prefix</code>	Prefix value in IPv6 Neighbor Discovery route advertisements	No

Table 9: RADIUS Attributes and Corresponding Junos OS Predefined Variables (*continued*)

RADIUS Attribute or VSA	Junos OS Predefined Variable	Description	Default Value Support for Junos OS Predefined Variable
Framed-IPv6-Route (99)	\$junos-framed-route-ipv6-address-prefix	(Subattribute 1): Framed IPv6 route prefix configured for the client	No
	\$junos-framed-route-ipv6-cost	(Subattribute 3): Metric for access route	No
	\$junos-framed-route-ipv6-distance	(Subattribute 5): Preference for access route	No
	\$junos-framed-route-ipv6-nexthop	(Subattribute 2): IPv6 routing information configured for the client	No
	\$junos-framed-route-ipv6-tag	(Subattribute 6): Tag for access route	No
Juniper Networks VSA			
Virtual-Router (26–1)	\$junos-routing-instance	Routing instance to which subscriber is assigned	No
Ingress-Policy-Name (26–10)	\$junos-input-filter NOTE: Variable is also used for RADIUS attribute 11.	Input filter to apply to client IPv4 interface	Yes
Egress-Policy-Name (26–11)	\$junos-output-filter	Output filter to apply to client IPv4 interface	Yes
IGMP-Enable (26–23)	\$junos-igmp-enable	Enable or disable IGMP on client interface	Yes
IGMP-Access-Name (26–71)	\$junos-igmp-access-group-name	Access list to use for the group (G) filter	Yes
IGMP-Access-Src-Name (26–72)	\$junos-igmp-access-source-group-name	Access List to use for the source group (S,G) filter	Yes
MLD-Access-Name (26–74)	\$junos-mld-access-group-name	Access list to use for the group (G) filter	Yes
MLD-Access-Src-Name (26–75)	\$junos-mld-access-source-group-name	Access List to use for the source group (S,G) filter	Yes

Table 9: RADIUS Attributes and Corresponding Junos OS Predefined Variables (*continued*)

RADIUS Attribute or VSA	Junos OS Predefined Variable	Description	Default Value Support for Junos OS Predefined Variable
MLD-Version (26–77)	\$junos-mld-version	MLD protocol version	Yes
IGMP-Version (26–78)	\$junos-igmp-version	IGMP protocol version	Yes
IGMP-Immediate-Leave (26–97)	\$junos-igmp-immediate-leave	IGMP immediate leave	Yes
MLD-Immediate-Leave (26–100)	\$junos-mld-immediate-leave	MLD immediate leave	Yes
IPv6-Ingress-Policy-Name (26–106)	\$junos-input-ipv6-filter	Input filter to apply to client IPv6 interface	Yes
IPv6-Egress-Policy-Name (26–107)	\$junos-output-ipv6-filter	Output filter to apply to client IPv6 interface	Yes
CoS-Traffic-Control-Profile-Parameter-Type (26–108)	\$junos-cos-scheduler-map	(T01: Scheduler-map name) Name of scheduler map configured in traffic-control profile	Yes
	\$junos-cos-shaping-rate	(T02: Shaping rate) Shaping rate configured in traffic-control profile	Yes
	\$junos-cos-guaranteed-rate	(T03: Guaranteed rate) Guaranteed rate configured in traffic-control profile	Yes
	\$junos-cos-delay-buffer-rate	(T04: Delay-buffer rate) Delay-buffer rate configured in traffic-control profile	Yes
	\$junos-cos-excess-rate	(T05: Excess rate) Excess rate configured in traffic-control profile	Yes
	\$junos-cos-traffic-control-profile	(T06: Traffic-control profile) Name of the traffic-control profile configured in a dynamic profile	Yes
	\$junos-cos-shaping-mode	(T07: Shaping mode) CoS shaping mode configured in a dynamic profile	Yes

Table 9: RADIUS Attributes and Corresponding Junos OS Predefined Variables (*continued*)

RADIUS Attribute or VSA	Junos OS Predefined Variable	Description	Default Value Support for Junos OS Predefined Variable
	\$junos-cos-byte-adjust	(T08; Byte adjust) Byte adjustments configured for the shaping mode in a dynamic profile	Yes
	\$junos-cos-adjust-minimum	(T09; Adjust minimum) Minimum adjusted value allowed for the shaping rate in a dynamic profile	Yes
	\$junos-cos-excess-rate-high	(T10; Excess rate high) Excess rate configured for high-priority traffic in a dynamic profile	Yes
	\$junos-cos-excess-rate-low	(T11; Excess rate low) Excess rate configured for low-priority traffic in a dynamic profile	Yes
	\$junos-cos-shaping-rate-burst	(T12; Shaping rate burst) Burst size configured for the shaping rate in a dynamic profile	Yes
	\$junos-cos-guaranteed-rate-burst	(T13; Guaranteed rate burst) Burst size configured for the guaranteed rate in a dynamic profile	Yes
Qos-Set-Name (26–130)	\$junos-interface-set-name	Name of an interface set configured in a dynamic profile	Yes
CoS-Scheduler-Pmt-Type (26–146)	\$junos-cos-scheduler	(Null: Scheduler name) Name of scheduler configured in a dynamic profile	Yes
	\$junos-cos-scheduler-tx	(T01: CoS scheduler transmit rate) Transmit rate for scheduler configured in a dynamic profile	Yes Available for multiple parameters: <ul style="list-style-type: none"> • Percent • Rate

Table 9: RADIUS Attributes and Corresponding Junos OS Predefined Variables (*continued*)

RADIUS Attribute or VSA	Junos OS Predefined Variable	Description	Default Value Support for Junos OS Predefined Variable
	\$junos-cos-scheduler-bs	(T02: CoS scheduler buffer size) Buffer size for scheduler configured in a dynamic profile	Yes Available for multiple parameters: <ul style="list-style-type: none"> • Percent • Temporal
	\$junos-cos-scheduler-pri	(T03: CoS scheduler priority) Packet-scheduling priority for scheduler configured in a dynamic profile	Yes
	\$junos-cos-scheduler-dropfile-low	(T04: CoS scheduler drop-profile low) Name of drop profile for RED loss-priority level low for scheduler configured in a dynamic profile	Yes
	\$junos-cos-scheduler-dropfile-medium-low	(T05: CoS scheduler drop-profile medium-low) Name of drop profile for RED loss-priority level medium-low for scheduler configured in a dynamic profile	Yes
	\$junos-cos-scheduler-dropfile-medium-high	(T06: CoS scheduler drop-profile medium-high) Name of drop profile for RED loss-priority level medium-high for scheduler configured in a dynamic profile	Yes
	\$junos-cos-scheduler-dropfile-high	(T07: CoS scheduler drop-profile high) Name of drop profile for RED loss-priority level high for scheduler configured in a dynamic profile	Yes

Table 9: RADIUS Attributes and Corresponding Junos OS Predefined Variables (*continued*)

RADIUS Attribute or VSA	Junos OS Predefined Variable	Description	Default Value Support for Junos OS Predefined Variable
	\$junos-cos-scheduler-dropfile-any	(T08: CoS scheduler drop-profile any) Name of drop profile for RED loss-priority level any for scheduler configured in a dynamic profile	Yes
	\$junos-cos-scheduler-excess-rate	(T09: CoS scheduler excess rate) Excess rate configured for a scheduler in a dynamic profile	Yes Available for multiple parameters: <ul style="list-style-type: none"> • Percent • Proportion
	\$junos-cos-scheduler-shaping-rate	(T10: CoS scheduler shaping rate) Shaping rate configured for a scheduler in a dynamic profile	Yes Available for multiple parameters: <ul style="list-style-type: none"> • Percent • Rate
	\$junos-cos-scheduler-excess-priority	(T11: CoS scheduler excess priority) Excess priority configured for a scheduler in a dynamic profile	Yes

- Related Documentation**
- *Dynamic Variables Overview*
 - *Configuring Predefined Dynamic Variables in Dynamic Profiles*
 - *Junos OS Predefined Variables*

DSL Forum Vendor-Specific Attributes

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



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

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

Table 10 on page 52 describes the DSL Forum VSAs.

Table 10: DSL Forum VSAs

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

Table 10: DSL Forum VSAs (*continued*)

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

Related Documentation • [DSL Forum VSAs Support in AAA Access and Accounting Messages for Junos OS on page 53](#)

DSL Forum VSAs Support in AAA Access and Accounting Messages for Junos OS

Table 11 on page 53 lists the DSL Forum VSAs supported by Junos OS in RADIUS Access-Request, Acct-Start, Acct-Stop, Interim-Acct, and CoA-Request messages. A checkmark in a column indicates that the message type supports that attribute. The DSL Forum vendor ID is 3561 (hexadecimal DE9), which is assigned by the IANA.

Table 11: DSL Forum VSAs—Supported RADIUS Messages

Attribute Number	Attribute Name	Access Request	Acct Start	Acct Stop	Interim Acct	CoA Request
[26-1]	Agent-Circuit-Id	✓	✓	✓	✓	✓
[26-2]	Agent-Remote-Id	✓	✓	✓	✓	✓
[26-129]	Actual-Data-Rate-Upstream	✓	✓	✓	✓	–
[26-130]	Actual-Data-Rate-Downstream	✓	✓	✓	✓	–
[26-131]	Minimum-Data-Rate-Upstream	✓	✓	✓	✓	–
[26-132]	Minimum-Data-Rate-Downstream	✓	✓	✓	✓	–
[26-133]	Attainable-Data-Rate-Upstream	✓	✓	✓	✓	–

Table 11: DSL Forum VSAs—Supported RADIUS Messages (*continued*)

Attribute Number	Attribute Name	Access Request	Acct Start	Acct Stop	Interim Acct	CoA Request
[26-134]	Attainable-Data-Rate-Downstream	✓	✓	✓	✓	–
[26-135]	Maximum-Data-Rate-Upstream	✓	✓	✓	✓	–
[26-136]	Maximum-Data-Rate-Downstream	✓	✓	✓	✓	–
[26-137]	Minimum-Data-Rate-Upstream-Low-Power	✓	✓	✓	✓	–
[26-138]	Minimum-Data-Rate-Downstream-Low-Power	✓	✓	✓	✓	–
[26-139]	Maximum-Interleaving-Delay-Upstream	✓	✓	✓	✓	–
[26-140]	Actual-Interleaving-Delay-Upstream	✓	✓	✓	✓	–
[26-141]	Maximum-Interleaving-Delay-Downstream	✓	✓	✓	✓	–
[26-142]	Actual-Interleaving-Delay-Downstream	✓	✓	✓	✓	–
[26-144]	Access-Loop-Encapsulation	✓	✓	✓	✓	–
[26-254]	IWF-Session	✓	✓	✓	✓	–

Related Documentation • [DSL Forum Vendor-Specific Attributes on page 51](#)

CHAPTER 3

Configuring RADIUS NAS-Port Attributes and Options

- [Manual Configuration of the NAS-Port-ID RADIUS Attribute on page 55](#)
- [Configuring a NAS-Port-ID with Additional Options on page 56](#)
- [Configuring a Calling-Station-ID with Additional Attributes on page 58](#)
- [RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN Overview on page 60](#)
- [Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 62](#)
- [Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 63](#)
- [Manual Configuration of the NAS-Port-Type RADIUS Attribute on page 64](#)
- [Configuring the RADIUS NAS-Port-Type per Physical Interface on page 66](#)
- [Configuring the RADIUS NAS-Port-Type per VLAN on page 68](#)
- [Configuring the RADIUS NAS-Port-Type per Stacked VLAN on page 69](#)
- [Configuring the RADIUS NAS-Port Extended Format per Physical Interface on page 71](#)
- [Configuring the RADIUS NAS-Port Extended Format per VLAN on page 72](#)
- [Configuring the RADIUS NAS-Port Extended Format per Stacked VLAN on page 74](#)
- [Configuring the RADIUS NAS-Port Extended Format for ATM Interfaces on page 76](#)

Manual Configuration of the NAS-Port-ID RADIUS Attribute

Subscriber management uses the NAS-Port-ID (RADIUS attribute 87) to provide an interface description that identifies the physical interface that is used to authenticate subscribers. The NAS-Port-ID is included in RADIUS Access-Request, Acct-Start, Acct-Stop, Acct-On, and Acct-Off messages.

You can configure access profiles to specify additional information in the NAS-Port-ID. The additional information can be any combination of the interface description (the default value), the Agent Circuit ID, the Agent Remote ID, and the NAS identifier. You can also specify an optional delimiter character, which separates the values in a NAS-Port-ID. The default delimiter character is the hash character (#).

A default NAS-Port-ID consists of the following **interface-description** string:

```
[physical-interface].<interface-type>-<slot>/<adapter>/<port><subinterface>[:<svlan>-<vlan>]
```

For example: **ge-1/2/0.100:100**

You might optionally configure an access profile that specifies that the NAS-Port-ID includes the NAS identifier, the Agent Circuit ID, and the Agent Remote ID, in addition to the default interface description. For this configuration, the NAS-Port-ID consists of the following string:

```
nas-identifier#interface-description#agent-circuit-id#agent-remote-id
```

For example:

```
retailer25#ge-1/2/0.100:100#ACI 12/1/22/1230:1.1.23#ARI 55/2/23.9999:10.11.1923
```



NOTE: The NAS-Port-ID displays the configured values in the following order (where # is the delimiter):

```
nas-identifier#interface-description#agent-circuit-id#agent-remote-id
```

**Related
Documentation**

- [Configuring a NAS-Port-ID with Additional Options on page 56](#)
- [RADIUS Server Options for Subscriber Access on page 4](#)

Configuring a NAS-Port-ID with Additional Options

You can include optional values in the NAS-Port-ID (RADIUS attribute 87), which identifies the physical interface subscriber management uses to authenticate subscribers. By default, the NAS-Port-ID includes the **interface-description** value that describes the physical interface. You can include the following values in the NAS-Port-ID:

- **agent-circuit-id**
- **agent-remote-id**
- **interface-description**
- **nas-identifier**

To configure an access profile to provide additional options in the NAS-Port-ID:

1. Specify the access profile you want to configure.

```
[edit]
```

```
user@host# edit access profile retailer25
```

2. Specify that you want to configure RADIUS options.

```
[edit access profile retailer25]
```

```
user@host# edit radius options
```

3. Specify the character to use as the delimiter between the different attribute values in the NAS-Port-ID. By default, subscriber management uses the hash character (#).

```
[edit access profile retailer25 radius options]  
user@host# set nas-port-delimiter %
```

4. Specify that you want to configure the format of the NAS-Port-ID.

```
[edit access profile retailer25 radius options]  
user@host# edit nas-port-id-format
```

5. Include the interface description in the NAS-Port-ID. (The interface description is not included by default when you configure the **nas-port-id-format** statement.)

```
[edit access profile retailer25 radius options nas-port-id-format]  
user@host# set interface-description
```

6. Include the Agent Circuit ID in the NAS-Port-ID.

```
[edit access profile retailer25 radius options nas-port-id-format]  
user@host# set agent-circuit-id
```

7. Include the Agent Remote ID in the NAS-Port-ID.

```
[edit access profile retailer25 radius options nas-port-id-format]  
user@host# set agent-remote-id
```

8. Include the NAS identifier value in the NAS-Port-ID.

```
[edit access profile retailer25 radius options nas-port-id-format]  
user@host# set nas-identifier
```

Configuring a Calling-Station-ID with Additional Attributes

You can configure an alternative value for the Calling-Station-ID (RADIUS IETF attribute 31) in an access profile on the MX Series router.

By default, the Calling-Station-ID includes the **agent-circuit-id** string. Optionally, you can configure the Calling-Station-ID to include one or more of the following attributes, in any combination:

- Agent circuit identifier (**agent-circuit-id**)—Identifier of the subscriber's access node and the digital subscriber line (DSL) on the access node. The agent circuit identifier (ACI) string is stored in either the DHCP option 82 field of DHCP messages for DHCP traffic, or in the DSL Forum Agent-Circuit-ID VSA [26-1] of PPPoE Active Discovery Initiation (PADI) and PPPoE Active Discovery Request (PADR) control packets for PPPoE traffic.
- Agent remote identifier (**agent-remote-id**)—Identifier of the subscriber on the digital subscriber line access multiplexer (DSLAM) interface that initiated the service request. The agent remote identifier (ARI) string is stored in either the DHCP option 82 field for DHCP traffic, or in the DSL Forum Agent-Remote-ID VSA [26-2] for PPPoE traffic.
- Interface description (**interface-description**)—Value of the interface.
- NAS identifier (**nas-identifier**)—Name of the NAS that originated the authentication or accounting request. NAS-Identifier is RADIUS IETF attribute 32.

If you configure the format of the Calling-Station-ID with more than one optional value, a hash character (#) is the default delimiter that the router uses as a separator between the concatenated values in the resulting Calling-Station-ID string. Optionally, you can configure an alternative delimiter character for the Calling-Station-ID to use. The following example shows the order of output when you configure multiple optional values:

nas-identifier#interface-description#agent-circuit-id#agent-remote-id#stacked-vlan#vlan

To configure an access profile to provide additional attributes in the Calling-Station-ID:

1. Specify the access profile you want to configure.

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

2. Specify that you want to configure RADIUS options.

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

3. Specify the nondefault character to use as the delimiter between the different attribute values in the Calling-Station-ID.

By default, subscriber management uses the hash character (#) as the delimiter in Calling-Station-ID strings that contain more than one optional value.

```
[edit access profile profile-name radius options]
user@host# set calling-station-id-delimiter delimiter-character
```

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

```
[edit access profile profile-name radius options]
user@host# set nas-identifier identifier-value
```

5. Specify that you want to configure the format of the Calling-Station-ID.

```
[edit access profile profile-name radius options]
user@host# edit calling-station-id-format
```

6. (Optional) Include the interface description value in the Calling-Station-ID.

```
[edit access profile profile-name radius options calling-station-id-format]
user@host# set interface-description
```

7. (Optional) Include the agent circuit identifier in the Calling-Station-ID.

```
[edit access profile profile-name radius options calling-station-id-format]
user@host# set agent-circuit-id
```

8. (Optional) Include the agent remote identifier in the Calling-Station-ID.

```
[edit access profile profile-name radius options calling-station-id-format]
user@host# set agent-remote-id
```

9. (Optional) Include the configured NAS identifier value in the Calling-Station-ID.

```
[edit access profile profile-name radius options calling-station-id-format]
user@host# set nas-identifier
```

Example:
Calling-Station-ID with
Additional Attributes
in an Access Profile

The following example creates an access profile named `retailer01` that configures a Calling-Station-ID string that includes the NAS-Identifier (**fox**), interface description, agent circuit identifier, and agent remote identifier optional attributes.

```
[edit access profile retailer01 radius options]
nas-identifier "fox";
calling-station-id-delimiter "*";
calling-station-id format {
  nas-identifier;
  interface-description;
  agent-circuit-id;
  agent-remote-id;
}
```

The resulting Calling-Station-ID string is formatted as follows:

```
fox*ge-1/2/0.100:100*as007*ar921
```

where:

- The NAS-Identifier value is **fox**.
- The Calling-Station-ID delimiter character is ***** (asterisk).
- The interface description value is **ge-1/2/0.100:100**.

- The agent circuit identifier value is **as007**.
- The agent remote identifier value is **ar921**.

**Related
Documentation**

- [Configuring RADIUS Server Options for Subscriber Access on page 102](#)
- [RADIUS Server Options for Subscriber Access on page 4](#)

RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN Overview

On MX Series routers with Modular Port Concentrator/Modular Interface Card (MPC/MIC) interfaces, you can configure the NAS-Port-Type (61) RADIUS IETF attribute, and an extended format for the NAS-Port (5) RADIUS IETF attribute, on a per-interface, per-VLAN, or per-stacked VLAN basis. The router passes the NAS-Port and NAS-Port-Type attributes to the RADIUS server during the authentication, authorization, and accounting (AAA) process.

This overview covers the following topics:

- [NAS-Port-Type RADIUS Attribute on page 60](#)
- [NAS-Port RADIUS Attribute on page 60](#)
- [NAS-Port Options Configuration and Subscriber Network Access Models on page 61](#)
- [NAS-Port Options Definition on page 61](#)

NAS-Port-Type RADIUS Attribute

The NAS-Port-Type attribute specifies the type of physical port that the network access server (NAS) uses to authenticate the subscriber. When you use the **nas-port-type** statement to configure the NAS-Port-Type, you can specify one of several predefined port types, or a user-defined port type value in the range 0 through 65535.

NAS-Port RADIUS Attribute

The NAS-Port attribute specifies the physical port number of the NAS that is authenticating the user, and is formed by a combination of the physical port's slot number, port number, adapter number, VLAN ID, and S-VLAN ID. The NAS-Port extended format, which you configure with the **nas-port-extended-format** statement, specifies the number of bits (bit width) for each field in the NAS-Port attribute: slot, adapter, port, VLAN, and S-VLAN.

To include stacked VLAN IDs, in addition to VLAN IDs, in the NAS-Port extended format, use the **stacked** option as part of the **nas-port-extended-format** statement. If you do not configure the **stacked** option, stacked VLAN IDs are not included in the extended format.

NAS-Port Options Configuration and Subscriber Network Access Models

Configuring the NAS-Port-Type and the extended format for NAS-Port on a per-VLAN, per-stacked VLAN, or per-physical interface basis is useful in network configurations that use the following subscriber access models:

- 1:1 access model (per-VLAN basis)—In a 1:1 access model, dedicated customer VLANs (C-VLANs) provide a one-to-one correspondence between an individual subscriber and the VLAN encapsulation.
- N:1 access model (per-S-VLAN basis)—In an N:1 access model, service VLANs are dedicated to a particular service, such as video, voice, or data, instead of to a particular subscriber. Because a service VLAN is typically shared by many subscribers within the same household or in different households, the N:1 access model provides a many-to-one correspondence between individual subscribers and the VLAN encapsulation.
- 1:1 or N:1 access model (per-physical interface basis)—You can configure the NAS-Port-Type and NAS-Port format on a per-physical interface basis for both the 1:1 access model and the N:1 access model.

NAS-Port Options Definition

As an alternative to globally configuring the NAS-Port-Type and NAS-Port extended format in an access profile, you can configure these attributes on a per-interface, per-VLAN, or per-stacked VLAN basis. To do so, you must create a *NAS-Port options definition*, which includes some or all of the following components:

- NAS-Port-Type value—Specifies the type of physical port that the network access server (NAS) uses to authenticate the subscriber.
- NAS-Port extended format—Configures the number of bits (bit width) for each field in the NAS-Port attribute, including: slot, adapter, port, VLAN, and S-VLAN. Optionally, you can also use the **stacked** option as part of the **nas-port-extended-format** statement to include S-VLAN IDs, in addition to VLAN IDs, in the extended format. If you do not configure the **stacked** option, stacked VLAN IDs are not included in the extended format.
- VLAN ranges or S-VLAN ranges—Defines the VLAN range of subscribers or stacked VLAN range of subscribers to which each NAS-Port options definition applies.

Related Documentation

- [Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 62](#)
- [Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 63](#)

Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN

The following guidelines apply when you configure the NAS-Port-Type attribute and the extended format for the NAS-Port attribute on a per-VLAN, per-stacked VLAN, or per-physical interface basis:

- You can create a maximum of 16 NAS-Port options definitions per physical interface. Each definition can include either a maximum of 32 VLAN ranges or a maximum of 32 stacked VLAN ranges, but cannot include a combination of VLAN ranges and stacked VLAN ranges.
- Configuring the NAS-Port-Type attribute and NAS-Port extended format on a per-VLAN, per-stacked VLAN, or per-physical interface basis overrides the global settings for these attributes configured in an access profile.
- If the NAS-Port-Type attribute and the NAS-Port extended format are not configured on a per-VLAN basis (in a 1:1 access model) or on a per-stacked VLAN basis (in an N:1 access model), the router uses the global settings configured for these attributes in an access profile for all RADIUS request messages.

Related Documentation

- [RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN Overview on page 60](#)
- [Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 63](#)

Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN

On MX Series routers with MPC/MIC interfaces, you can configure the NAS-Port-Type (61) RADIUS IETF attribute, and an extended format for the NAS-Port (5) RADIUS IETF attribute, on a per-physical interface, per-VLAN, or per-stacked VLAN (S-VLAN) basis. The router passes the NAS-Port-Type and NAS-Port attributes to the RADIUS server during the authentication, authorization, and accounting (AAA) process.

To configure the NAS-Port-Type and NAS-Port extended format on a per-physical interface, per-VLAN, or per-stacked VLAN basis, you must create a NAS-Port options definition, which includes the following components:

- NAS-Port-Type value—Specifies the type of physical port that the network access server (NAS) uses to authenticate the subscriber.
- NAS-Port extended format—Configures the number of bits (bit width) for each field in the NAS-Port attribute, which specifies the physical port number of the NAS that is authenticating the subscriber. Fields in the NAS-Port attribute include: slot, adapter, port, VLAN, and S-VLAN. Optionally, you can also use the **stacked** option as part of the **nas-port-extended-format** statement to include S-VLAN IDs, in addition to VLAN IDs, in the extended format. If you do not configure the **stacked** option, stacked VLAN IDs are not included in the extended format.
- VLAN ranges or S-VLAN ranges—Defines the VLAN range of subscribers or stacked VLAN range of subscribers to which each NAS-Port options definition applies.



NOTE: You can create a maximum of 16 NAS-Port options definitions per physical interface. Each definition can include a maximum of 32 VLAN ranges or 32 stacked VLAN ranges, but *cannot* include a combination of VLAN ranges and stacked VLAN ranges.

To configure the NAS-Port-Type and NAS-Port extended format on a per-physical interface, per-VLAN, or per-stacked VLAN basis:

1. Specify the physical interface you want to configure.
2. Enable VLAN tagging, stacked VLAN tagging, or flexible VLAN tagging on the interface.
 - For VLAN tagging, see *Enabling VLAN Tagging*.
 - For stacked VLAN tagging, see *Configuring Stacked VLAN Tagging*
 - For flexible VLAN tagging, also referred to as mixed tagging, see *Enabling VLAN Tagging*.
3. Specify that you want to configure RADIUS options for a physical interface, VLAN, or S-VLAN.

```
[edit interfaces interface-name]
user@host> edit radius-options
```

4. Create a named NAS-Port options definition.

```
[edit interfaces interface-name radius-options]  
user@host# edit nas-port-options nas-port-options-name
```

5. Configure the NAS-Port-Type, and the VLAN ranges or stacked VLAN ranges to which the named NAS-Port options definition applies.
 - For per-physical interface configurations, see [“Configuring the RADIUS NAS-Port-Type per Physical Interface” on page 66](#).
 - For per-VLAN configurations, see [“Configuring the RADIUS NAS-Port-Type per VLAN” on page 68](#).
 - For per-stacked VLAN configurations, see [“Configuring the RADIUS NAS-Port-Type per Stacked VLAN” on page 69](#).
6. Configure the NAS-Port extended format, and the VLAN ranges or stacked VLAN ranges to which the named NAS-Port options definition applies.
 - For per-physical interface configurations, see [“Configuring the RADIUS NAS-Port Extended Format per Physical Interface” on page 71](#).
 - For per-VLAN configurations, see [“Configuring the RADIUS NAS-Port Extended Format per VLAN” on page 72](#).
 - For per-stacked VLAN configurations, see [“Configuring the RADIUS NAS-Port Extended Format per Stacked VLAN” on page 74](#).

**Related
Documentation**

- [RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN Overview on page 60](#)
- [Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 62](#)
- [Configuring the RADIUS NAS-Port-Type per Physical Interface on page 66](#)
- [Configuring the RADIUS NAS-Port-Type per VLAN on page 68](#)
- [Configuring the RADIUS NAS-Port-Type per Stacked VLAN on page 69](#)
- [Configuring the RADIUS NAS-Port Extended Format per Physical Interface on page 71](#)
- [Configuring the RADIUS NAS-Port Extended Format per VLAN on page 72](#)
- [Configuring the RADIUS NAS-Port Extended Format per Stacked VLAN on page 74](#)

Manual Configuration of the NAS-Port-Type RADIUS Attribute

Subscriber management uses the NAS-Port-Type (RADIUS attribute 61) to identify the type of physical port that is used to authenticate subscribers. By default, subscriber management uses a NAS-Port-Type of **ethernet**.

You can optionally configure access profiles to provide the value for the NAS-Port-Type attribute, which enables you to explicitly specify the NAS port type that is used for a given connection. For example, you might configure an access profile that specifies that a NAS

port type of **wireless** is used for all Ethernet connections that are managed by that access profile.



NOTE: The **ethernet-port-type-virtual** configuration statement takes precedence over the **nas-port-type** statement when you include both statements in the same access profile. When you include the **ethernet-port-type-virtual** statement, subscriber management uses the RADIUS attribute value of 5, which specifies a NAS port type of **virtual**.

Table 12 on page 65 shows the supported port type values for RADIUS attribute 61 (NAS-Port-Type) that you can include in an access profile.

Table 12: RADIUS NAS-Port-Type Values

Statement Option	NAS-Port-Type Value	Description
<i>value</i>	0–65535	Number that indicates either the IANA-assigned value for the RADIUS port type or a custom number-to-port type defined by the user
adsl-cap	12	Asymmetric DSL, carrierless amplitude phase (CAP) modulation
adsl-dmt	13	Asymmetric DSL, discrete multitone (DMT)
async	0	Asynchronous
cable	17	Cable
ethernet	15	Ethernet
fddi	21	Fiber Distributed Data Interface
g3-fax	10	G.3 Fax
hdlc-clear-channel	7	HDLC Clear Channel
iapp	25	Inter-Access Point Protocol (IAPP)
idsl	14	ISDN DSL
isdn-sync	2	ISDN Synchronous
isdn-v110	4	ISDN Async V.110
isdn-v120	3	ISDN Async V.120
piafs	6	Personal Handyphone System (PHS) Internet Access Forum Standard

Table 12: RADIUS NAS-Port-Type Values (*continued*)

Statement Option	NAS-Port-Type Value	Description
sdsl	11	Symmetric DSL
sync	1	Synchronous
token-ring	20	Token Ring
virtual	5	Virtual
wireless	18	Other wireless
wireless-1x-ev	24	Wireless 1xEV
wireless-cdma2000	22	Wireless code division multiple access (CDMA) 2000
wireless-ieee80211	19	Wireless 802.11
wireless-umts	23	Wireless universal mobile telecommunications system (UMTS)
x25	8	X.25
x75	9	X.75
xdsl	16	DSL of unknown type

Related Documentation

- [Configuring RADIUS Server Options for Subscriber Access on page 102](#)

Configuring the RADIUS NAS-Port-Type per Physical Interface

As an alternative to globally configuring the NAS-Port-Type (61) RADIUS attribute in an access profile, you can configure the NAS-Port-Type on a per-physical interface basis as part of a NAS-Port options definition. The NAS-Port-Type specifies the type of physical port that the network access server (NAS) uses to authenticate the subscriber.

Configuring NAS-Port options definitions on a per-physical interface basis is useful in network configurations that use a 1:1 access model or an N:1 access model.

To configure the NAS-Port-Type RADIUS attribute per physical interface:

1. Specify the interface you want to configure.

```
[edit]
user@host# edit interfaces interface-name
```

2. Enable VLAN tagging on the interface.

```
[edit interfaces interface-name]
user@host# set vlan-tagging
```

Setting VLAN tagging enables the reception and transmission of 802.1Q VLAN-tagged frames on the interface. You must enable VLAN tagging before you can configure the VLAN ranges to which the NAS-Port options definition applies.

3. Specify that you want to configure RADIUS options for a physical interface.

```
[edit interfaces interface-name]
user@host# edit radius-options
```

4. Create a named NAS-Port options definition.

```
[edit interfaces interface-name radius-options]
user@host# edit nas-port-options nas-port-options-name
```

5. Configure the NAS-Port-Type.

```
[edit interfaces interface-name radius-options nas-port-options nas-port-options-name]
user@host# set nas-port-type port-type
```

6. Configure the VLAN range or ranges to which the NAS-Port options definition applies.

```
[edit interfaces interface-name radius-options nas-port-options nas-port-options-name]
user@host# set vlan-ranges (any | low-tag-high-tag)
```

Per-physical interface configurations typically require you to create a VLAN range that consists of all VLAN IDs on the physical interface. To do so, use the **any** option with the **vlan-ranges** statement.

The following example shows a per-interface NAS-Port options definition named **subscribers-east** that configures the **wireless-umts** NAS-Port-Type for a VLAN range consisting of all VLAN IDs on Gigabit Ethernet physical interface **ge-1/0/0**.

```
[edit interfaces ge-1/0/0 radius-options]
nas-port-options subscribers-east {
  nas-port-type wireless-umts;
  vlan-ranges {
    any;
  }
}
```

Related Documentation

- [Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 63](#)
- [Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 62](#)
- [Configuring the RADIUS NAS-Port-Type per VLAN on page 68](#)
- [Configuring the RADIUS NAS-Port-Type per Stacked VLAN on page 69](#)
- [Configuring the RADIUS NAS-Port Extended Format per Physical Interface on page 71](#)
- [Configuring the RADIUS NAS-Port Extended Format per VLAN on page 72](#)
- [Configuring the RADIUS NAS-Port Extended Format per Stacked VLAN on page 74](#)

Configuring the RADIUS NAS-Port-Type per VLAN

As an alternative to globally configuring the NAS-Port-Type (61) RADIUS attribute in an access profile, you can configure the NAS-Port-Type on a per-VLAN basis as part of a NAS-Port options definition. The NAS-Port-Type specifies the type of physical port that the network access server (NAS) uses to authenticate the subscriber.

Configuring NAS-Port options definitions on a per-VLAN basis is useful in network configurations that use a 1:1 access model.

To configure the NAS-Port-Type RADIUS attribute per VLAN:

1. Specify the interface you want to configure.

```
[edit]
user@host# edit interfaces interface-name
```

2. Enable VLAN tagging on the interface.

```
[edit interfaces interface-name]
user@host# set vlan-tagging
```

Setting VLAN tagging enables the reception and transmission of 802.1Q VLAN-tagged frames on the interface. You must enable VLAN tagging before you can configure the VLAN ranges to which the NAS-Port options definition applies.

3. Specify that you want to configure RADIUS options for a VLAN interface.

```
[edit interfaces interface-name]
user@host# edit radius-options
```

4. Create a named NAS-Port options definition.

```
[edit interfaces interface-name radius-options]
user@host# edit nas-port-options nas-port-options-name
```

5. Configure the NAS-Port-Type.

```
[edit interfaces interface-name radius-options nas-port-options nas-port-options-name]
user@host# set nas-port-type port-type
```

6. Configure the VLAN range or ranges to which the NAS-Port options definition applies.

```
[edit interfaces interface-name radius-options nas-port-options nas-port-options-name]
user@host# set vlan-ranges (any | low-tag-high-tag)
```

Per-VLAN configurations typically require you to create a VLAN range that consists of a single VLAN ID on the physical interface. To do so, set the **low-tag** and **high-tag** options in the **vlan-ranges** statement to the same value, as shown in the following example.

The following example shows a per-VLAN NAS-Port options definition named **subscribers-west** that configures the **ethernet** NAS-Port-Type for VLAN ID 3 on Gigabit Ethernet physical interface **ge-1/1/0**.

```
[edit interfaces ge-1/1/0 radius-options]
nas-port-options subscribers-west {
  nas-port-type ethernet;
```



```

vlan-ranges {
  3-3;
}

```

Related Documentation

- [Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 63](#)
- [Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 62](#)
- [Configuring the RADIUS NAS-Port-Type per Physical Interface on page 66](#)
- [Configuring the RADIUS NAS-Port-Type per Stacked VLAN on page 69](#)
- [Configuring the RADIUS NAS-Port Extended Format per Physical Interface on page 71](#)
- [Configuring the RADIUS NAS-Port Extended Format per VLAN on page 72](#)
- [Configuring the RADIUS NAS-Port Extended Format per Stacked VLAN on page 74](#)

Configuring the RADIUS NAS-Port-Type per Stacked VLAN

As an alternative to globally configuring the NAS-Port-Type (61) RADIUS attribute in an access profile, you can configure the NAS-Port-Type on a per-stacked VLAN basis as part of a NAS-Port options definition. The NAS-Port-Type specifies the type of physical port that the network access server (NAS) uses to authenticate the subscriber.

Configuring NAS-Port options definitions on a per-stacked VLAN basis is useful in network configurations that use an N:1 access model.

To configure the NAS-Port-Type RADIUS attribute per stacked VLAN:

1. Specify the interface you want to configure.

```

[edit]
user@host# edit interfaces interface-name

```

2. Enable stacked VLAN tagging on the interface.

```

[edit interfaces interface-name]
user@host# set stacked-vlan-tagging

```

Setting stacked VLAN tagging enables you to configure dual VLAN tags for all logical interfaces on the physical interface. You must enable stacked VLAN tagging before you can configure the stacked VLAN ranges to which the NAS-Port options definition applies.

3. Specify that you want to configure RADIUS options for a stacked VLAN interface.

```

[edit interfaces interface-name]
user@host# edit radius-options

```

4. Create a named NAS-Port options definition.

```

[edit interfaces interface-name radius-options]
user@host# edit nas-port-options nas-port-options-name

```

5. Configure the NAS-Port-Type.

```
[edit interfaces interface-name radius-options nas-port-options nas-port-options-name]
user@host# set nas-port-type port-type
```

6. Configure the stacked VLAN range or ranges to which the NAS-Port options definition applies.

```
[edit interfaces interface-name radius-options nas-port-options nas-port-options-name]
user@host# set stacked-vlan-ranges (any | low-outer-tag-high-outer-tag),any
```

Per-stacked VLAN configurations require you to create a stacked VLAN range of subscribers to which the NAS-Port options definition applies. You must configure the low and high outer tags (VLAN IDs) in the range 1 through 4094, and the inner tag (S-VLAN ID) as **any** to represent all S-VLAN ID tags.

7. Repeat Steps 3 through 6 to configure additional NAS-Port options definitions on this interface.

The following example creates two NAS-Port options definitions, subscribers-north and subscribers-south, configured on a per-stacked VLAN basis on Gigabit Ethernet physical interface ge-1/1/0.

The subscribers-north definition configures a NAS-Port-Type user-defined value (4711) for a stacked VLAN range with outer VLAN ID 1 and all inner S-VLAN IDs. The subscribers-south definition configures a NAS-Port-Type user-defined value (4722) for a stacked VLAN range with outer VLAN IDs in the range 2 through 10, and all inner S-VLAN IDs.

```
[edit interfaces ge-2/0/1 radius-options]
nas-port-options subscribers-north {
  nas-port-type 4711;
  stacked-vlan-ranges {
    1-1,any;
  }
}
nas-port-options subscribers-south {
  nas-port-type 4722;
  stacked-vlan-ranges {
    2-10,any;
  }
}
```

Related Documentation

- [Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 63](#)
- [Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 62](#)
- [Configuring the RADIUS NAS-Port-Type per Physical Interface on page 66](#)
- [Configuring the RADIUS NAS-Port-Type per VLAN on page 68](#)
- [Configuring the RADIUS NAS-Port Extended Format per Physical Interface on page 71](#)
- [Configuring the RADIUS NAS-Port Extended Format per VLAN on page 72](#)
- [Configuring the RADIUS NAS-Port Extended Format per Stacked VLAN on page 74](#)

Configuring the RADIUS NAS-Port Extended Format per Physical Interface

As an alternative to globally configuring the extended format for the NAS-Port (5) RADIUS attribute in an access profile, you can configure the NAS-Port extended format on a per-physical interface basis as part of a NAS-Port options definition. The NAS-Port extended format configures the number of bits (bit width) in each field in the NAS-Port attribute, including: slot, adapter, port, VLAN, and S-VLAN.

Configuring NAS-Port options definitions on a per-physical interface basis is useful in network configurations that use a 1:1 access model or an N:1 access model.

To configure an extended format for the NAS-Port RADIUS attribute per physical interface:

1. Specify the interface you want to configure.

```
[edit]
user@host# edit interfaces interface-name
```

2. Enable VLAN tagging on the interface.

```
[edit interfaces interface-name]
user@host# set vlan-tagging
```

Setting VLAN tagging enables the reception and transmission of 802.1Q VLAN-tagged frames on the interface. You must enable VLAN tagging before you can configure the VLAN ranges to which the NAS-Port options definition applies.

3. Specify that you want to configure RADIUS options for a physical interface.

```
[edit interfaces interface-name]
user@host# edit radius-options
```

4. Create a named NAS-Port options definition.

```
[edit interfaces interface-name radius-options]
user@host# edit nas-port-options nas-port-options-name
```

5. Configure the NAS-Port extended format.

```
[edit interfaces interface-name radius-options nas-port-options nas-port-options-name]
user@host# set nas-port-extended-format slot-width width adapter-width width
port-width width vlan-width width
```

6. Configure the VLAN range or ranges to which the NAS-Port options definition applies.

```
[edit interfaces interface-name radius-options nas-port-options nas-port-options-name]
user@host# set vlan-ranges (any | low-tag-high-tag)
```

Per-physical interface configurations typically require you to create a VLAN range that consists of all VLAN IDs on the physical interface. To do so, use the **any** option with the **vlan-ranges** statement.

The following example shows a per-interface NAS-Port options definition named *boston-subscribers* that configures a NAS-Port extended format consisting of an 8-bit slot field, 8-bit adapter field, 8-bit port field, and 4-bit VLAN field. The *boston-subscribers* definition applies to a VLAN range consisting of all VLAN IDs on Gigabit Ethernet physical interface *ge-2/0/1*.

```
[edit interfaces ge-2/0/1 radius-options]
nas-port-options boston-subscribers {
  nas-port-extended-format {
    slot-width 8;
    adapter-width 8;
    port-width 8;
    vlan-width 4;
  }
  vlan-ranges {
    any;
  }
}
```

Related Documentation

- [Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 63](#)
- [Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 62](#)
- [Configuring the RADIUS NAS-Port-Type per Physical Interface on page 66](#)
- [Configuring the RADIUS NAS-Port-Type per VLAN on page 68](#)
- [Configuring the RADIUS NAS-Port-Type per Stacked VLAN on page 69](#)
- [Configuring the RADIUS NAS-Port Extended Format per VLAN on page 72](#)
- [Configuring the RADIUS NAS-Port Extended Format per Stacked VLAN on page 74](#)

Configuring the RADIUS NAS-Port Extended Format per VLAN

As an alternative to globally configuring the extended format for the NAS-Port (5) RADIUS attribute in an access profile, you can configure the NAS-Port extended format on a per-VLAN basis as part of a NAS-Port options definition. The NAS-Port extended format configures the number of bits (bit width) in each field in the NAS-Port attribute, including: slot, adapter, port, VLAN, and S-VLAN.

Configuring NAS-Port options definitions on a per-VLAN basis is useful in network configurations that use a 1:1 access model.

To configure an extended format for the NAS-Port RADIUS attribute per VLAN:

1. Specify the interface you want to configure.

```
[edit]
user@host# edit interfaces interface-name
```

2. Enable VLAN tagging on the interface.

```
[edit interfaces interface-name]
user@host# set vlan-tagging
```

Setting VLAN tagging enables the reception and transmission of 802.1Q VLAN-tagged frames on the interface. You must enable VLAN tagging before you can configure the VLAN ranges to which the NAS-Port options definition applies.

3. Specify that you want to configure RADIUS options for a VLAN interface.

```
[edit interfaces interface-name]
user@host# edit radius-options
```

4. Create a named NAS-Port options definition.

```
[edit interfaces interface-name radius-options]
user@host# edit nas-port-options nas-port-options-name
```

5. Configure the NAS-Port extended format.

```
[edit interfaces interface-name radius-options nas-port-options nas-port-options-name]
user@host# set nas-port-extended-format slot-width width adapter-width width
port-width width vlan-width width
```

6. Configure the VLAN range or ranges to which the NAS-Port options definition applies.

```
[edit interfaces interface-name radius-options nas-port-options nas-port-options-name]
user@host# set vlan-ranges (any | low-tag-high-tag)
```

Per-VLAN configurations typically require you to create a VLAN range that consists of a single VLAN ID on the physical interface. To do so, set the **low-tag** and **high-tag** options in the **vlan-ranges** statement to the same value, as shown in the following example.

The following example shows a per-VLAN NAS-Port options definition named *paris-subscribers* that configures a NAS-Port extended format consisting of a 4-bit slot field, 2-bit adapter field, 4-bit port field, and 2-bit VLAN field. The *paris-subscribers* definition applies to VLAN ID 1 on Gigabit Ethernet physical interface *ge-1/0/1*.

```
[edit interfaces ge-1/0/1 radius-options]
nas-port-options paris-subscribers {
  nas-port-extended-format {
    slot-width 4;
    adapter-width 2;
    port-width 4;
    vlan-width 2;
  }
  vlan-ranges {
    1-1;
  }
}
```

Related Documentation

- [Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 63](#)
- [Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 62](#)
- [Configuring the RADIUS NAS-Port-Type per Physical Interface on page 66](#)
- [Configuring the RADIUS NAS-Port-Type per VLAN on page 68](#)
- [Configuring the RADIUS NAS-Port-Type per Stacked VLAN on page 69](#)
- [Configuring the RADIUS NAS-Port Extended Format per Physical Interface on page 71](#)
- [Configuring the RADIUS NAS-Port Extended Format per Stacked VLAN on page 74](#)

Configuring the RADIUS NAS-Port Extended Format per Stacked VLAN

As an alternative to globally configuring the extended format for the NAS-Port (5) RADIUS attribute in an access profile, you can configure the NAS-Port extended format on a per-stacked VLAN basis as part of a NAS-Port options definition. The NAS-Port extended format configures the number of bits (bit width) in each field in the NAS-Port attribute, including: slot, adapter, port, VLAN, and S-VLAN.

Configuring NAS-Port options definitions on a per-stacked VLAN basis is useful in network configurations that use an N:1 access model.

To configure an extended format for the NAS-Port RADIUS attribute per stacked VLAN:

1. Specify the interface you want to configure.

```
[edit]
user@host# edit interfaces interface-name
```

2. Enable stacked VLAN tagging on the interface.

```
[edit interfaces interface-name]
user@host# set stacked-vlan-tagging
```

Setting stacked VLAN tagging enables you to configure dual VLAN tags for all logical interfaces on the physical interface. You must enable stacked VLAN tagging before you can configure the stacked VLAN ranges to which the NAS-Port options definition applies.

3. Specify that you want to configure RADIUS options for a stacked VLAN interface.

```
[edit interfaces interface-name]
user@host# edit radius-options
```

4. Create a named NAS-Port options definition.

```
[edit interfaces interface-name radius-options]
user@host# edit nas-port-options nas-port-options-name
```

5. Configure the NAS-Port extended format.

```
[edit interfaces interface-name radius-options nas-port-options nas-port-options-name]
user@host# set nas-port-extended-format slot-width width adapter-width width
port-width width vlan-width width stacked
```

To include S-VLAN IDs, in addition to VLAN IDs, in the NAS-Port extended format, include the **stacked** option in the **nas-port-extended-format** statement.

6. Configure the stacked VLAN range or ranges to which the NAS-Port options definition applies.

```
[edit interfaces interface-name radius-options nas-port-options nas-port-options-name]
user@host# set stacked-vlan-ranges (any | low-outer-tag-high-outer-tag),any
```

Per-stacked VLAN configurations require you to create a stacked VLAN range of subscribers to which the NAS-Port options definition applies. You must configure the

low and high outer tags (VLAN IDs) in the range 1 through 4094, and the inner tag (S-VLAN ID) as **any** to represent all S-VLAN ID tags.

7. Repeat Steps 3 through 6 to configure additional NAS-Port options definitions on this interface.

The following example creates two NAS-Port options definitions, `chicago-subscribers` and `barcelona-subscribers`, configured on a per-stacked VLAN basis on Gigabit Ethernet physical interface `ge-3/2/1`.

The `chicago-subscribers` definition configures a NAS-Port extended format consisting of a 8-bit slot field, 8-bit adapter field, 8-bit port field, 4-bit stacked VLAN field, and 4-bit VLAN field. Because the **stacked** option is configured in this definition, S-VLAN IDs, in addition to VLAN IDs, are included in the extended format. The `chicago-subscribers` definition applies to a stacked VLAN range with outer VLAN ID 1, and all inner S-VLAN IDs.

The `barcelona-subscribers` definition configures a NAS-Port extended format consisting of a 8-bit slot field, 8-bit adapter field, 8-bit port field, 4-bit stacked VLAN field, and 4-bit VLAN field. Because the **stacked** option is *not* configured in this definition, S-VLAN IDs are not included in the extended format. The `barcelona-subscribers` definition applies to a stacked VLAN range with outer VLAN IDs in the range 2 through 10, and all inner S-VLAN IDs.

```
[edit interfaces ge-3/2/1 radius-options]
nas-port-options chicago-subscribers {
  nas-port-extended-format {
    slot-width 8;
    adapter-width 8;
    port-width 8;
    stacked-vlan-width 4;
    vlan-width 4;
    stacked;
  }
  stacked-vlan-ranges {
    1-1,any;
  }
}
nas-port-options barcelona-subscribers {
  nas-port-extended-format {
    slot-width 8;
    adapter-width 8;
    port-width 8;
    stacked-vlan-width 4;
    vlan-width 4;
  }
  stacked-vlan-ranges {
    2-10,any;
  }
}
```

Related Documentation

- [Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 63](#)

- [Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 62](#)
- [Configuring the RADIUS NAS-Port-Type per Physical Interface on page 66](#)
- [Configuring the RADIUS NAS-Port-Type per VLAN on page 68](#)
- [Configuring the RADIUS NAS-Port-Type per Stacked VLAN on page 69](#)
- [Configuring the RADIUS NAS-Port Extended Format per Physical Interface on page 71](#)
- [Configuring the RADIUS NAS-Port Extended Format per VLAN on page 72](#)

Configuring the RADIUS NAS-Port Extended Format for ATM Interfaces

As an alternative to globally configuring an extended format for the NAS-Port (5) RADIUS attribute in an access profile, you can configure the NAS-Port extended format on a per-physical interface basis for both Ethernet subscribers and ATM subscribers as part of a NAS-Port options definition. The NAS-Port extended format configures the number of bits (bit width) in each field of the NAS-Port attribute, including: slot, adapter, port, ATM virtual path identifier (VPI), and ATM virtual circuit identifier (VCI).

To configure the NAS-Port extended format for an ATM interface, include one or both of the following options in the **nas-port-extended-format** statement along with the other options as appropriate for your needs:

- **vpi-width**—Number of bits in the ATM VPI field, in the range 1 through 32
- **vci-width**—Number of bits in the ATM VCI field, in the range 1 through 32



NOTE: For ATM subscribers, the combined total of the widths of all fields must not exceed 32 bits, or the configuration fails. The router may truncate the values of individual fields depending on the bit width you specify.

To configure an extended format for the NAS-Port RADIUS attribute for an ATM interface:

1. Specify the ATM interface you want to configure.

```
[edit]  
user@host# edit interfaces interface-name
```

2. Specify that you want to configure RADIUS options for a physical interface.

```
[edit interfaces interface-name]  
user@host# edit radius-options
```

3. Create a named NAS-Port options definition.

```
[edit interfaces interface-name radius-options]  
user@host# edit nas-port-options nas-port-options-name
```

4. Configure the NAS-Port extended format.

```
[edit interfaces interface-name radius-options nas-port-options nas-port-options-name]
```



```
user@host# set nas-port-extended-format slot-width width adapter-width width  
port-width width vpi-width width vci-width width
```

The following example shows a NAS-Port options definition named boston-subscribers for ATM interface at-1/0/4 that configures a NAS-Port extended format with an ATM slot width of 6 bits, ATM adapter width of 3 bits, ATM port width of 4 bits, ATM VPI width of 12 bits, and ATM VCI width of 24 bits.

```
[edit interfaces at-1/0/4 radius-options]  
nas-port-options boston-subscribers {  
  nas-port-extended-format {  
    slot-width 6;  
    adapter-width 3;  
    port-width 4;  
    vpi-width 12;  
    vci-width 24;  
  }  
}
```

**Related
Documentation**

- [Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 63](#)
- [RADIUS Server Options for Subscriber Access on page 4](#)
- [Configuring RADIUS Server Options for Subscriber Access on page 102](#)

CHAPTER 4

Configuring RADIUS Authentication for Subscriber Access

- [Retaining Authentication and Accounting Information During Session Startup on page 79](#)
- [Configuring Authentication and Accounting Parameters for Subscriber Access on page 80](#)
- [Specifying the Authentication and Accounting Methods for Subscriber Access on page 80](#)
- [Specifying RADIUS Authentication and Accounting Servers for Subscriber Access on page 81](#)
- [Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 82](#)

Retaining Authentication and Accounting Information During Session Startup

At subscriber session startup, the Junos OS **authd** process sends an Acct-On message to the RADIUS server and the new session starts authentication and accounting operations. However, in some service provider environments, upon receipt of the Acct-On message, the RADIUS server cleans up the previous session state and removes accounting statistics. In this scenario, the RADIUS server's cleanup operation can inadvertently delete the new session's authentication and accounting information, which might include customer billing information.

To ensure that the new session's authentication and accounting information is not deleted, you can optionally use the **wait-for-acct-on-ack** statement to configure the **authd** process to wait for an Acct-On-Ack response message from the RADIUS accounting server, so the RADIUS cleanup can finish before **authd** sends any new authentication and accounting updates.

You configure this feature for an access profile for a logical system and routing instance context. All authentication requests fail until the router receives an Acct-On-Ack response from a RADIUS accounting server that is configured in the access profile. If multiple RADIUS accounting servers are configured for the access profile, **authd** waits until the first response is received.

You can also configure the **authd** process to send accounting messages when the RADIUS server status changes for an access profile. This configuration enables you to monitor

whether the access profile has an active RADIUS server. You use the **send-acct-status-on-config-change** statement to specify that **authd** send an Acct-On message when the first RADIUS server is added to an access profile, and to send an Acct-Off message when the last RADIUS server is deleted from the access profile.

- Related Documentation**
- [Configuring Per-Subscriber Session Accounting on page 92](#)

Configuring Authentication and Accounting Parameters for Subscriber Access

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

To configure authentication and accounting for subscriber access:

1. Specify the authentication and accounting methods to use.
[See “Specifying the Authentication and Accounting Methods for Subscriber Access” on page 80.](#)
2. Specify how accounting statistics are collected.
[See “Configuring Per-Subscriber Session Accounting” on page 92.](#)

- Related Documentation**
- [AAA Service Framework Overview on page 3](#)
 - [Configuring Router or Switch Interaction with RADIUS Servers on page 99](#)
 - [Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 82](#)

Specifying the Authentication and Accounting Methods for Subscriber Access

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

You can configure multiple authentication and accounting methods—the **authentication-order** and **accounting order** statements specify the order in which the subscriber access management feature uses the methods. For example, an authentication entry of **radius password** specifies that RADIUS authentication is performed first and, if it fails, local authentication (**password**) is done.

You can specify the following authentication methods:



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

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

You can specify the following accounting methods:

- **radius**—RADIUS-based accounting

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

1. Specify the authentication methods and the order in which they are used. Only **radius** is supported.

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

2. Specify the accounting method.

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

Related Documentation

- [Configuring Router or Switch Interaction with RADIUS Servers on page 99](#)
- [Configuring Authentication and Accounting Parameters for Subscriber Access on page 80](#)
- [Configuring Per-Subscriber Session Accounting on page 92](#)
- [Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 82](#)

Specifying RADIUS Authentication and Accounting Servers for Subscriber Access

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

To configure RADIUS authentication and accounting support:

1. Specify that you want to configure RADIUS support.

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

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

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

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

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

To configure multiple RADIUS authentication or accounting servers:

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

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

**Related
Documentation**

- [Configuring Router or Switch Interaction with RADIUS Servers on page 99](#)
- [Configuring Authentication and Accounting Parameters for Subscriber Access on page 80](#)
- [Configuring RADIUS Server Options for Subscriber Access on page 102](#)
- [Configuring How RADIUS Attributes Are Used for Subscriber Access on page 40](#)
- [Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 82](#)

Example: Configuring RADIUS-Based Subscriber Authentication and Accounting

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

```
[edit access]
radius-server {
  192.168.1.250 {
    port 1812;
    accounting-port 1813;
    accounting-retry 6;
    accounting-timeout 20;
    retry 3;
    secret &tIUeI*7688+;
    source-address 192.168.1.100;
    timeout 45;
  }
  192.168.1.251 {
    port 1812;
    accounting-port 1813;
    accounting-retry 6;
    accounting-timeout 20;
    retry 3;
    secret $Dyu*UY(877-;
    source-address 192.168.1.100;
    timeout 30;
  }
  192.168.1.252 {
    port 1812;
    secret $Dyu*UY(877-;
  }
}
```

```

profile isp-bos-metro-fiber-basic {
  authentication-order radius;
  accounting {
    order radius;
    accounting-stop-on-access-deny;
    accounting-stop-on-failure;
    immediate-update;
    statistics time;
    update-interval 12;
    wait-for-acct-on-ack;
    send-acct-status-on-config-change;
  }
  radius {
    authentication-server 192.168.1.251 192.168.1.252;
    accounting-server 192.168.1.250 192.168.1.251;
    options {
      accounting-session-id-format decimal;
      client-accounting-algorithm round-robin;
      client-authentication-algorithm round-robin;
      nas-identifier 56;
      nas-port-id-delimiter %;
      nas-port-id-format {
        nas-identifier;
        interface-description;
      }
      nas-port-type {
        ethernet {
          wireless-80211;
        }
      }
    }
  }
  attributes {
    ignore {
      framed-ip-netmask;
    }
    exclude {
      accounting-delay-time [accounting-start accounting-stop];
      accounting-session-id [access-request accounting-on accounting-off
        accounting-start accounting-stop];
      dhcp-gi-address [access-request accounting-start accounting-stop];
      dhcp-mac-address [access-request accounting-start accounting-stop];
      nas-identifier [access-request accounting-start accounting-stop];
      nas-port [accounting-start accounting-stop];
      nas-port-id [accounting-start accounting-stop];
      nas-port-type [access-request accounting-start accounting-stop];
    }
  }
}
[edit logical-systems isp-bos-metro-12 routing-instances isp-cmbrg-12-32]
interfaces {
  lo0 {
    unit 0 {
      family inet {
        address 192.168.1.100/24;
      }
    }
  }
}

```

```
    }  
  }  
  ge-0/0/0 {  
    vlan-tagging;  
    unit 0 {  
      vlan-id 200;  
      family inet {  
        unnumbered-address lo0.0;  
      }  
    }  
  }  
}
```

Related Documentation

- [Configuring Router or Switch Interaction with RADIUS Servers on page 99](#)

CHAPTER 5

Configuring RADIUS Accounting for Subscriber Access

- [RADIUS Accounting Statistics for Subscriber Access Overview on page 85](#)
- [Understanding RADIUS Accounting Duplicate Reporting on page 87](#)
- [Preservation of RADIUS Accounting Information During an Accounting Server Outage on page 88](#)
- [RADIUS Acct-On and Acct-Off Messages on page 91](#)
- [Configuring Per-Subscriber Session Accounting on page 92](#)
- [Configuring Per-Service Session Accounting on page 94](#)
- [Configuring Service Packet Counting on page 95](#)
- [Configuring Back-up Options for RADIUS Accounting on page 97](#)

RADIUS Accounting Statistics for Subscriber Access Overview

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

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

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



NOTE: Subscriber management counts forwarded packets only. Dropped traffic (for example, as a result of a filter action) and control traffic are not included in the accounting statistics.

The router uses the RADIUS attributes and Juniper Networks VSAs listed in [Table 13 on page 86](#) to provide the accounting statistics for subscriber and service sessions.

If the session has both IPv4 and IPv6 families enabled, the router reports statistics for both families.



NOTE:

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

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

Table 13: RADIUS Attributes and VSAs Used for Per-Subscriber Session Accounting

Attribute Number	Attribute Name	Type of Statistics
26–151	IPv6-Acct-Input-Octets	IPv6
26–152	IPv6-Acct-Output-Octets	IPv6
26–153	IPv6-Acct-Input-Packets	IPv6
26–154	IPv6-Acct-Output-Packets	IPv6
26–155	IPv6-Acct-Input-Gigawords	IPv6
26–156	IPv6-Acct-Output-Gigawords	IPv6
47	Acct-Input-Packets	IPv4 and IPv6 aggregation
48	Acct-Output-Packets	IPv4 and IPv6 aggregation
52	Acct-Input-Gigawords	IPv4 and IPv6 aggregation
53	Acct-Output-Gigawords	IPv4 and IPv6 aggregation

Related Documentation

- [Configuring Per-Subscriber Session Accounting on page 92](#)
- [Configuring Per-Service Session Accounting on page 94](#)
- [Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 82](#)

Understanding RADIUS Accounting Duplicate Reporting

When you configure RADIUS accounting, by default the router sends the accounting reports to the accounting servers in the context in which the subscriber was last authenticated. You can configure RADIUS accounting to send duplicate accounting reports to other servers in the same context or in other contexts.

Layer 3 Wholesale Scenarios

In a Layer 3 wholesale network environment, the wholesaler and retailer might use different RADIUS accounting servers, and both might want to receive accounting reports. In this situation, you can configure RADIUS accounting duplicate reporting, which sends reports to both the wholesaler and the retailer accounting servers. The target to which the duplicate accounting records are sent must be in the default:default logical system:routing instance combination (LS:RI) , also called the *default VRF*.

Table 14 on page 87 shows where subscriber management sends the accounting reports when you enable duplicate reporting. Subscriber management sends duplicate reports based on the access profile in which you configure the **duplication** statement at the **[edit access profile *profile-name* accounting]** hierarchy level, where the subscriber resides, and how the subscriber is authenticated.



NOTE: You can also enable accounting duplicate reporting based on the domain map configuration—you configure subscribers to authenticate with a nondefault routing instance and a target logical system:routing instance of default:default. The accounting reports are then sent to both the authentication context and the default:default context.

Table 14: Duplicate RADIUS Accounting Reporting

Access Profile in Which Duplication Is Configured	Where Subscriber Is Authenticated	Subscriber's Target Logical System/Routing Instance	Accounting Servers Where Accounting Reports Are Sent
retailer A	wholesaler	retailer A	wholesaler and retailer A
retailer A	retailer A	retailer A	wholesaler (default/default context) NOTE: This is the domain map configuration described in the Note preceding this table.
wholesaler	wholesaler and retailer A	retailer A	wholesaler and retailer A

Table 14: Duplicate RADIUS Accounting Reporting (*continued*)

Access Profile in Which Duplication Is Configured	Where Subscriber Is Authenticated	Subscriber's Target Logical System/Routing Instance	Accounting Servers Where Accounting Reports Are Sent
wholesaler and retailer B	wholesaler and retailer A	retailer B	wholesaler, retailer A, and retailer B
not configured (default)	any	any	single report sent to accounting servers in the context in which subscriber was last authenticated

Other Scenarios

For scenarios that are not in a Layer 3 wholesale network environment, you might want to send duplicate accounting records to a different set of RADIUS servers that reside in either the same or a different routing context. Unlike the Layer 3 wholesale scenario, the target for the duplicate RADIUS accounting records does not have to be the default VRF. You can specify a single nondefault VRF—that is, other than the default:default LS:RI combination—as the target. Additionally, you can specify up to five access profiles in the target VRF that list the RADIUS accounting servers that receive the duplicate reports.

For example, you might have a lawful intercept scenario where the subscriber is authenticated in the default domain. An authorized law enforcement organization needs duplicate accounting records for the subscriber to be sent to a mediation device that resides in the organization's networking domain, which lies in a nondefault VRF.

Subscriber management sends duplicate reports to the VRF that you specify with the **vrf-name** statement at the **[edit access profile *profile-name* accounting duplication-vrf]** hierarchy level. Include the **access-profile-name** statement at the same level to designate the access profiles that in turn specify the RADIUS servers that receive the duplicate reports.

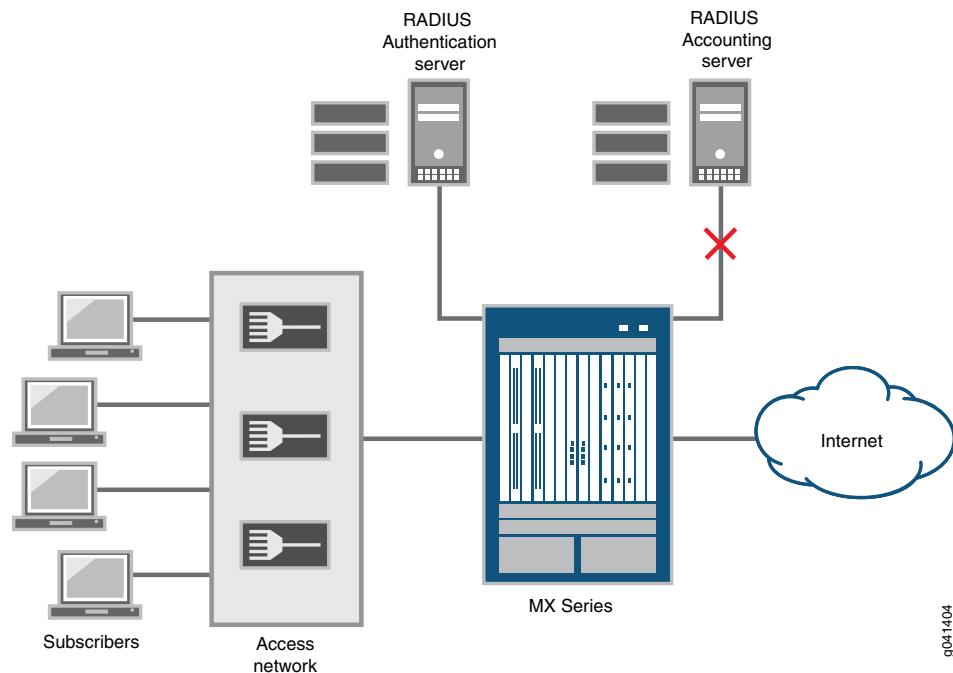
Related Documentation

- [Configuring Per-Subscriber Session Accounting on page 92](#)

Preservation of RADIUS Accounting Information During an Accounting Server Outage

If the router loses contact with the RADIUS accounting server, as represented in [Figure 1 on page 89](#), whether due to a server outage or a problem in the network connecting to the server, you can lose all the billing information that would have been received by the server. RADIUS accounting backup preserves the accounting data that accumulates during the outage. If you have not configured RADIUS accounting backup, the accounting data is lost for the duration of the outage from the time when the router has exhausted its attempts to resume contact with the RADIUS server. The configurable retry value determines the number of times the router attempts to contact the server.

Figure 1: Topology with Loss of Access to Accounting Server



By default, the router must wait until the revert timer expires before it can attempt to contact the non-responsive server again. However, when you configure accounting backup, the revert timer is disabled and the router immediately retries its accounting requests as soon as the router fails to receive accounting acknowledgments. Accounting backup follows this sequence:

1. The router fails to receive accounting acknowledgments from the server.
2. The router immediately attempts to contact the accounting server and marks the server as offline if the router does not receive an acknowledgment before exhausting the number of retries.
3. The router next attempts to contact in turn each additional accounting server configured in the RADIUS profile.

If a server is reached, then the router resumes sending accounting requests to this server.

4. If none of the servers responds or if no other servers are in the profile, the router declares a timeout and begins backing up the accounting data. It withholds all accounting stop messages and does not forward new accounting requests to the server.
5. During the outage, the router sends a single pending accounting stop message to the servers at periodic intervals.
6. If one of the servers acknowledges receipt, then the router sends all the pending stop messages to that server in batches at the same interval until all the stored stop messages have been sent. However, any new accounting requests are sent immediately rather being held and sent periodically.

The router replays accounting stop messages to the server in the correct order because it preserves both the temporal order among subscribers and the causal order between service and session stop requests for each subscriber. Only accounting stop messages are backed up, because they include the start time and duration of sessions and all the accounting statistics. This makes it unnecessary to withhold the accounting start messages, which eventually time out. Interim updates are not backed up and time out as well; if the session remains active, then the next interim update after the server connection is restored provides the interim accounting information.

You can configure the number of accounting stop messages that the router can queue pending restoration of contact with the accounting server. To preserve current accounting data in preference to collecting new accounting data, subscriber logins fail as soon as the maximum number of messages has been withheld. Subscriber logins resume immediately when the pending queue drops below the queue limit.



NOTE: Service accounting stop messages are withheld for a maximum of ten services per subscriber. If a subscriber attempts to activate an eleventh service while that accounting server is offline, the activation fails.

The router can hold the pending accounting messages for up to 24 hours. When the configurable maximum holding period passes, all accounting stop messages still in the pending queue are flushed, even if the accounting server has come back online. A consequence of this is that subscriber logins resume immediately if they were failing because the maximum pending limit had been reached.

All pending messages are also flushed in either of the following circumstances:

- If you remove the last accounting server from the access profile, because then there is no place to send the messages.
- If you remove the accounting backup configuration.

While the router is withholding accounting stop messages, you can force the router to attempt contact with the accounting server immediately, rather than allowing it to wait until the periodic interval has expired. When you do so, the router first replays a batch of stop messages to the server, with one of the following outcomes:

- If the router receives an acknowledgment of receipt, then it marks the server as online and begins replaying all remaining pending stop messages in batches.
- If the router does not receive the acknowledgment, then it resumes sending a single pending accounting stop message at the periodic interval.

When a subscriber logs out while the accounting server is offline, the accounting stop requests for the subscriber and the session are queued and replayed to the server when it comes online. In this case, the subscriber session and service session information is retained, so that the router can send a correct accounting request when the server comes back online.

In the event of a graceful Routing Engine switchover while the accounting server is offline, the pending stop messages can be replayed from the active Routing Engine when the server is online again.



NOTE: When RADIUS accounting backup is configured, you must use different servers for RADIUS authentication and accounting. Subscriber authentication fails when the same server is configured for both authentication and accounting.

If the RADIUS server acts on behalf of other back-end RADIUS accounting or authentication servers and forwards requests to them, subscribers can be authenticated but accounting requests are not sent out.

**Related
Documentation**

- [Configuring Back-up Options for RADIUS Accounting on page 97](#)
- [Forcing the Router to Contact the Accounting Server Immediately on page 101](#)

RADIUS Acct-On and Acct-Off Messages

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

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

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

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

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

**Related
Documentation**

- [AAA Service Framework Overview on page 3](#)
- [Configuring Per-Subscriber Session Accounting on page 92](#)

- [AAA Accounting Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS on page 37](#)

Configuring Per-Subscriber Session Accounting

To configure accounting for a subscriber session, you use an access profile, and specify how the subscriber access management feature collects and uses the accounting statistics. The router uses the RADIUS attributes and Juniper Networks VSAs discussed in [“RADIUS Accounting Statistics for Subscriber Access Overview” on page 85](#) to provide the accounting statistics for the subscriber session.

To configure accounting for a subscriber session:

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

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

2. (Optional) Configure AAA to issue an Acct-Stop message if the AAA server denies access to the subscriber.

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

3. (Optional) Configure AAA to send an Acct-Stop message if the subscriber fails AAA but is granted access by the AAA server.

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

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

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

5. (Optional) Configure subscriber management to send the RADIUS accounting report to both the wholesaler and the retailer accounting servers.

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

6. (Optional) Configure the router to send the RADIUS accounting report to multiple accounting servers listed in access profiles in a nondefault VRF (LS:RI).

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

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

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


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

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

9. (Optional) Configure the types of statistics to gather. You can specify that the router or switch collect both volume and time statistics or only time statistics for subscriber sessions. When you change the type of statistics being collected, current subscribers continue to use the previous collection specification. Subscribers who log in after the change use the new specification.

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

10. (Optional) Override the default behavior and specify that, after a CoA action that changes the RADIUS Class attribute, accounting reports for the subscriber's service sessions continue to use the original Class attribute that was assigned when the service sessions were created. The new Class attribute value is used in accounting reports for the subscriber session only. By default, the accounting reports for both the subscriber session and the subscriber's service sessions use the new Class attribute value.

```
[edit access profile profile-name accounting]
user@host# set coa-no-override service-class-attribute
```

11. (Optional) Configure the number of minutes between accounting updates. You can configure an interval from 10 through 1440 minutes. All values are rounded up to the next higher multiple of 10. For example, the values 811 through 819 are all accepted by the CLI, but are all rounded up to 820.

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

12. (Optional) Configure AAA to send an immediate interim accounting update to the RADIUS server when AAA receives a rate change notification from the ANCP agent on the router.

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

13. (Optional) Configure the authd process to wait for an Acct-On-Ack response message from RADIUS before sending any new authentication and accounting updates to the RADIUS server. This configuration ensures that when a new subscriber session starts, the authentication and accounting information for the new session does not get deleted when RADIUS clears previously existing session state information.

```
[edit access profile profile-name accounting]
user@host# set wait-for-acct-on-ack
```

14. (Optional) Configure the authd process to send an Acct-On message when the first RADIUS server is added to the access profile, and to send an Acct-Off message when the last RADIUS server is removed from the access profile. This configuration enables you to monitor whether the access profile has an active RADIUS server.

```
[edit access profile profile-name accounting]
user@host# set send-acct-status-on-config-change
```

Related Documentation

- [RADIUS Accounting Statistics for Subscriber Access Overview on page 85](#)
- [Understanding RADIUS Accounting Duplicate Reporting on page 87](#)
- [Configuring Per-Service Session Accounting on page 94](#)
- [Retaining Authentication and Accounting Information During Session Startup on page 79](#)
- [Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 82](#)
- [Configuring Immediate Interim Accounting Updates to RADIUS in Response to ANCP Notifications on page 408](#)

Configuring Per-Service Session Accounting

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

The router uses the RADIUS attributes and Juniper Networks VSAs discussed in “[RADIUS Accounting Statistics for Subscriber Access Overview](#)” on page 85 to provide the accounting statistics for the subscriber session.



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

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

1. Ensure that the required RADIUS VSAs are configured.
See [Table 15 on page 94](#) for the VSAs that the router uses for per-service accounting.
2. Configure the classic firewall filter or fast update filter to count the service packets.
See “[Configuring Service Packet Counting](#)” on page 95.

Table 15: Juniper Networks VSAs Used for Per-Service Session Accounting

Attribute Number	Attribute Name	Description	Value
26-69	Service-Statistics	Enable or disable statistics for the service	<ul style="list-style-type: none"> • 0 = disable • 1 = enable time statistics • 2 = enable time and volume statistics

Table 15: Juniper Networks VSAs Used for Per-Service Session Accounting (*continued*)

Attribute Number	Attribute Name	Description	Value
26-83	Service-Session	Service string sent in accounting stop and start messages from the router to the RADIUS server	string: service-name, with parameter values that are sent from RADIUS server in attribute 26-65.
26-140	Service-Interim-Acct-Interval	Amount of time between interim accounting updates for this service	<ul style="list-style-type: none"> • range = 600–86400 seconds • 0 = disabled <p>NOTE: Values are rounded up to the next higher multiple of 10 minutes. For example, a setting of 900 seconds (15 minutes) is rounded up to 20 minutes (1200 seconds).</p>

- Related Documentation**
- [Configuring Service Packet Counting on page 95](#)
 - [RADIUS Accounting Statistics for Subscriber Access Overview on page 85](#)
 - [Configuring Per-Subscriber Session Accounting on page 92](#)
 - [Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 82](#)

Configuring Service Packet Counting

Subscriber management uses service packet counting to report volume statistics for subscribers on a per-service session basis. To configure service packet counting, you specify the accounting action, and subscriber management then applies the results to a specific named counter (`_junos-dyn-service-counter`) for use by RADIUS.

The accounting action you configure specifies the counting mechanism that subscriber management uses when capturing statistics—either inline counters or deferred counters. Inline counters are captured when the event occurs, and do not include any additional packet processing that might occur after the event. Deferred counters (also called accurate accounting) are not incremented until the packet is queued for transmission, and therefore include the entire packet processing. Deferred counters provide a more accurate count of the packets than inline counters, and are more useful for subscriber accounting and billing.

You configure the accounting mechanism by specifying either the **service-accounting-deferred** action (for deferred counters) or the **service-accounting** action (for inline counters) at the `[edit firewall family family-name filter filter-name term term-name then]` hierarchy level.

The two accounting mechanisms are mutually exclusive, both on a per-term basis and a per-filter basis. Also, both accounting actions are mutually exclusive with the count action on a per-term basis.



NOTE: You can define deferred counters for the inet and inet6 families for classic filters only. Fast update filters do not support deferred counters.

To enable service packet counting:

1. Configure any match conditions that you want to count using the service accounting action. For example:

```
[edit firewall family inet filter filtername term term-name]  
user@host# set from source-address address
```

2. Specify the accounting action for the filter.

To use deferred counters:

```
[edit firewall family inet filter filtername term term-name]  
user@host# set then service-accounting-deferred
```

To use inline counters:

```
[edit firewall family inet filter filtername term term-name]  
user@host# set then service-accounting
```

When the match conditions for the filter are met, the packet is counted and applied to the well-known service counter (`_junos-dyn-service-counter`) for use by the RADIUS server. This counter provides the volume statistics for per-service accounting.



TIP: You cannot use the `service-accounting` action or the `service-accounting-deferred` action in the same term as a count action.

Related Documentation

- [Classic Filters Overview](#)
- [Defining Dynamic Filter Processing Order](#)
- [RADIUS Accounting Statistics for Subscriber Access Overview on page 85](#)
- [Configuring Per-Service Session Accounting on page 94](#)
- [Configuring Per-Subscriber Session Accounting on page 92](#)
- [Guidelines for Configuring Firewall Filters](#)
- [Guidelines for Applying Firewall Filters](#)
- [Firewall Filter Terminating Actions](#)
- [Firewall Filter Nonterminating Actions](#)

Configuring Back-up Options for RADIUS Accounting

You can configure RADIUS accounting backup to preserve accounting data when the accounting server is unavailable because of a server or network outage. When backup is configured, RADIUS accounting stop messages are withheld and queued to be sent when connectivity is restored. You can specify the maximum number of stop messages that can be queued. When this maximum is reached, subsequent new subscriber logins fail because there is no remaining capacity to preserve accounting data for new sessions.

You can also configure how long the queued messages can be held. When this period expires, all pending accounting stops are flushed from the queue, even if the accounting server has come back online.



NOTE: Configuring accounting backup disables the revert timer. An error message is generated if you attempt to configure the `revert-interval` statement at the [edit access profile *profile-name* options] or [edit access radius-options] hierarchy levels.



CAUTION: Before you configure RADIUS accounting backup, ensure that RADIUS accounting and RADIUS authentication are configured on different servers. Subscriber authentication fails when the same server is configured for both authentication and accounting.

1. Enable accounting backup to use the default values.

```
[edit access ]
user@host# set accounting-backup-options
```

2. (Optional) Configure the number of accounting stops that the router can preserve while the accounting server is offline.

```
[edit access accounting-backup-options]
user@host# set max-pending-accounting-stops number
```

3. (Optional) Configure how long the router holds pending accounting stops before flushing them.

```
[edit access accounting-backup-options]
user@host# set max-withhold-time hold-time
```

For example, the following statements configure the backup options for all subscriber accounting; these statements specify that the router holds no more than 32,000 pending accounting stops—at which point all subsequent subscriber logins fail—and holds them no longer than 6 hours—at which point all pending messages are flushed and subscriber logins resume if they were failing:

```
[edit access accounting-backup-options]
user@host# set max-pending-accounting-stops 32000
user@host# set max-withhold-time 360
```

- Related Documentation**
- [Preservation of RADIUS Accounting Information During an Accounting Server Outage on page 88](#)
 - [Forcing the Router to Contact the Accounting Server Immediately on page 101](#)

CHAPTER 6

Configuring Routers and RADIUS Servers for Subscriber Access

- [Configuring Router or Switch Interaction with RADIUS Servers on page 99](#)
- [Forcing the Router to Contact the Accounting Server Immediately on page 101](#)
- [Configuring RADIUS Server Parameters for Subscriber Access on page 102](#)
- [Configuring RADIUS Server Options for Subscriber Access on page 102](#)
- [Configuring RADIUS Options for Subscriber Access Globally on page 105](#)

Configuring Router or Switch Interaction with RADIUS Servers

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

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

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

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

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

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

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

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

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

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

5. (Optional) Configure the maximum number of outstanding requests that a RADIUS server can maintain. An outstanding request is a request to which the RADIUS server has not yet responded. You can limit the number from 0 through 2000 outstanding requests per RADIUS server. The default setting is 1000 outstanding requests per server.

```
[edit access radius-server 192.168.1.250]
user@host# set max-outstanding-requests 500
```

6. Configure the source address for the RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address. The source address is a valid IPv4 address configured on one of the router or switch interfaces.

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

7. (Optional) Configure retry and timeout values for authentication and accounting messages.
 - a. Configure how many times the router attempts to contact a RADIUS server when it has received no response. You can configure the router or switch to retry from 1 through 30 times. The default setting is 3 retry attempts.

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

- b. Configure how long the router or switch waits to receive a response from a RADIUS server before retrying the contact. By default, the router or switch waits 3 seconds. You can configure the timeout to be from 1 through 90 seconds.

```
[edit access radius-server 192.168.1.250]
user@host# set accounting-timeout 20
```



NOTE: We recommend that you do not configure the maximum retry duration: 30 retries times 90 seconds. Configure either fewer retries, a shorter timeout, or both.



NOTE: The retry and timeout settings apply to both authentication and accounting messages unless you configure both the `accounting-retry` statements and the `accounting-timeout` statement. In that case, the retry and timeout settings apply only to authentication messages.

8. (Optional) Configure retry and timeout values for accounting messages separate from the settings for authentication messages.



NOTE: You must configure both of these options. If you do not, then the value you configure is ignored in favor of the values configured with the **retry** and **timeout** statements.

- a. Configure how many times the router attempts to send accounting messages to the RADIUS accounting server when it has received no response. You can configure the router to retry from 0 through 30 times. The default setting is 0, meaning that this option is disabled.

```
[edit access radius-server 192.168.1.250]
user@host# set accounting-retry 6
```

- b. Configure how long the router waits to receive a response from a RADIUS accounting server before retrying the request. You can configure the timeout to be from 0 through 900 seconds. The default setting is 0, meaning that this option is disabled.

```
[edit access radius-server 192.168.1.250]
user@host# set accounting-timeout 20
```

Related Documentation

- [AAA Service Framework Overview on page 3](#)
- [Configuring Authentication and Accounting Parameters for Subscriber Access on page 80](#)
- [Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 82](#)

Forcing the Router to Contact the Accounting Server Immediately

In the event of an accounting server outage while RADIUS accounting backup is enabled, by default the router waits for a time interval to expire before contacting the offline server. Rather than waiting for that interval to pass, you can force the router to immediately contact the server by issuing the **request network-access aaa replay pending-accounting-stops** command. The router sends a batch of pending accounting stop requests to the server. If the router receives an acknowledgment from the server, then the router continues to replay the pending messages to the server in batches at the periodic interval. If the router does not get that acknowledgment, then it resumes sending a single pending accounting stop message at the periodic interval.

To force the router to immediately contact the offline accounting server:

- Request the messages to be replayed.

```
user@host> request network-access aaa replay pending-accounting-stops
```

Related Documentation

- [Preservation of RADIUS Accounting Information During an Accounting Server Outage on page 88](#)

Configuring RADIUS Server Parameters for Subscriber Access

Include the **radius** statement at the **[edit access profile *profile-name*]** hierarchy level to specify the RADIUS parameters for the subscriber access manager feature. The following list provides an overview of the parameters you can configure:

- The IP addresses of one or more RADIUS authentication and accounting servers.
- Options for the RADIUS servers, such as the following:
 - Format (decimal or description) used for the accounting session
 - Method (round-robin or direct) the router or switch uses to communicate with the servers
 - NAS identifier to use for RADIUS requests
 - Revert time setting that specifies when the router or switch reverts to using the primary RADIUS server
 - Delimiter character and format for the NAS-Port-ID (RADIUS attribute 87) and Calling-Station-ID (RADIUS attribute 31)
- The RADIUS attributes to be ignored or excluded from RADIUS messages.

To configure RADIUS server parameters:

1. Specify that you want to configure RADIUS support.

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

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

See [“Specifying RADIUS Authentication and Accounting Servers for Subscriber Access” on page 81](#).

3. Configure the RADIUS server options.

See [“Configuring RADIUS Server Options for Subscriber Access” on page 102](#).

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

See [“Configuring How RADIUS Attributes Are Used for Subscriber Access” on page 40](#).

Related Documentation

- [Specifying RADIUS Authentication and Accounting Servers for Subscriber Access on page 81](#)
- [Configuring RADIUS Server Options for Subscriber Access on page 102](#)
- [Configuring How RADIUS Attributes Are Used for Subscriber Access on page 40](#)

Configuring RADIUS Server Options for Subscriber Access

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

To configure RADIUS authentication and accounting server options:

1. Specify that you want to configure RADIUS.

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

2. Specify that you want to configure RADIUS options.

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

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

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

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

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

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

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

6. (Optional) Specify that the Agent-Remote-Id and Agent-Circuit-Id are generated locally when these values are not present in the client database.

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

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

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

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

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

9. (Optional) Configure the RADIUS client to use the extended format for RADIUS attribute 5 (NAS-Port) and specify the width of the fields in the NAS-Port attribute. The total of the widths must not exceed 32 bits, or the configuration fails.

- For Ethernet subscribers:

```
[edit access profile isp-bos-metro-fiber-basic radius options]
user@host# set nas-port-extended-format ae-width 10 slot-width 4 adapter-width
2 port-width 4 stacked-vlan-width 10 vlan-width 2
```

- For ATM subscribers:

```
[edit access profile retailer01 radius options]
```

```
user@host# set nas-port-extended-format atm slot-width 3 adapter-width 2
port-width 3 vpi-width 8 vci-width 16
```

10. (Optional) Configure the delimiter character that the router inserts between values in RADIUS attribute 87 (NAS-Port-ID).

```
[edit access profile isp-bos-metro-fiber-basic radius options]
user@host# set nas-port-id-delimiter %
```

11. (Optional) Configure the information that the router includes in RADIUS attribute 87 (NAS-Port-ID).

```
[edit access profile isp-bos-metro-fiber-basic radius options]
user@host# set nas-port-id-format agent-circuit-id agent-remote-id
```

12. (Optional) Configure the delimiter character that the router inserts between values in RADIUS attribute 31 (Calling-Station-ID).

```
[edit access profile isp-bos-metro-fiber-basic radius options]
user@host# set calling-station-id-delimiter "%"
```

13. (Optional) Configure the information that the router includes in RADIUS attribute 31 (Calling-Station-ID).

```
[edit access profile isp-bos-metro-fiber-basic radius options]
user@host# set calling-station-id-format agent-circuit-id agent-remote-id
```

14. (Optional) Configure the port type that is included in RADIUS attribute 61 (NAS-Port-Type). This specifies the port type the router uses to authenticate subscribers.

```
[edit access profile isp-bos-metro-fiber-basic radius options]
user@host# set nas-port-type ethernet wireless-ieee80211
```



NOTE: This statement is ignored if you configure the `ethernet-port-type-virtual` in the same access profile.

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

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



NOTE: This statement takes precedence over the `nas-port-type` statement if you include both in the same access profile.

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

```
[edit access profile isp-bos-metro-fiber-basic radius options]
user@host# set revert-interval 259200
```

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

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

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

18. (Optional) Configure the router to use the optional behavior when processing CoA requests that include changes to client profile dynamic variables.

```
[edit access profile isp-bos-metro-fiber-basic radius options]  
user@host# set coa-dynamic-variable-validation
```

**Related
Documentation**

- [RADIUS Server Options for Subscriber Access on page 4](#)
- [Configuring Router or Switch Interaction with RADIUS Servers on page 99](#)
- [Manual Configuration of the NAS-Port-Type RADIUS Attribute on page 64](#)
- [Configuring a NAS-Port-ID with Additional Options on page 56](#)
- [Configuring a Calling-Station-ID with Additional Attributes on page 58](#)
- [Example: Configuring RADIUS-Based Subscriber Authentication and Accounting on page 82](#)

Configuring RADIUS Options for Subscriber Access Globally

You can configure RADIUS options that apply to all RADIUS servers globally.

To configure RADIUS options globally:

1. Specify that you want to configure RADIUS options.

```
[edit access ]  
user@host# edit radius-options
```

2. (Optional) Configure the number of requests per second that the router can send to all the RADIUS servers collectively.

```
[edit access radius-options]  
user@host# set request-rate 1000
```

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

```
[edit access radius-options]  
user@host# set revert-interval 86400
```

**Related
Documentation**

- [Global RADIUS Options for Subscriber Access on page 7](#)
- [request-rate on page 908](#)
- [revert-interval on page 911](#)

CHAPTER 7

Configuring Access Profiles for Subscriber Access

- [Configuring an Access Profile for Subscriber Management on page 107](#)
- [Attaching Access Profiles on page 108](#)

Configuring an Access Profile for Subscriber Management

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

To configure an access profile:

1. Edit the access stanza.

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

2. Specify an existing or new access profile name.

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

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

Related Documentation

- [Attaching Access Profiles on page 108](#)
- [Configuring Dynamic Authentication for VLAN Interfaces profile on page 858](#)

Attaching Access Profiles

After you have created the access profile that specifies the subscriber authentication and accounting parameters, you must specify where the profile is used. Authentication and accounting will not run unless you specify the profile. Subscriber management supports attaching access profiles at the following hierarchy levels:

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

To attach an access profile:

1. Edit the desired hierarchy level.

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

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

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

Related Documentation

- [AAA Service Framework Overview on page 3](#)

CHAPTER 8

Configuring Session Options for Subscriber Access

- [Understanding Session Options for Subscriber Access on page 109](#)
- [Configuring Subscriber Session Options on page 111](#)
- [Removing Inactive Dynamic Subscriber VLANs on page 112](#)

Understanding Session Options for Subscriber Access

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



NOTE: For all subscriber types other than DHCP (such as L2TP-tunneled and PPP-terminated subscribers), the session timeout value limits the subscriber session. For DHCP subscribers, the session timeout value is used to limit the lease. The lease expires when the timeout value expires. If this value is not supplied by either the CLI or RADIUS, the DHCP lease does not expire.

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

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

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

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

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

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

- A value of zero is treated as no timeout.
- A value in the range 1 through 59 is raised to 60 seconds.
- A value that exceeds 31,622,400 is reduced to 31,622,400 seconds.

For Idle-Timeout [28]:

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

In configurations using dynamically created subscriber VLANs, the idle timeout also deletes the inactive subscriber VLANs when the inactivity threshold has been reached. In addition to deleting inactive dynamic subscriber VLANs, the idle timeout also removes dynamic VLANs when no client sessions were ever created (for example, in the event no client sessions are created on the dynamic VLAN or following the occurrence of an error during session creation or client authentication where no client sessions are created on the dynamic VLAN).

When using the idle timeout for dynamic VLAN removal, keep the following in mind:

- The idle timeout period begins after a dynamic subscriber VLAN interface is created or traffic activity stops on a dynamic subscriber VLAN interface.
- If a new client session is created or a client session is reactivated successfully, the client idle timeout resets.
- The removal of inactive subscriber VLANs functions only with VLANs that have been authenticated.

**Related
Documentation**

- [RADIUS IETF Attributes Supported by the AAA Service Framework on page 14](#)
- [Configuring Subscriber Session Options on page 111](#)
- [Removing Inactive Dynamic Subscriber VLANs on page 112](#)

Configuring Subscriber Session Options

Subscriber session timeouts enable you to place limits on subscriber access based on how long the session has been up, how long the user has been inactive, or both. The subscriber session timeouts apply to both L2TP-tunneled and PPP-terminated subscriber sessions.



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

To configure limitations on subscriber sessions:

1. Edit session options for the router access profile.

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

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

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

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

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

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

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

Related Documentation

- [Understanding Session Options for Subscriber Access on page 109](#)
- [client-idle-timeout on page 666](#)
- [client-session-timeout on page 667](#)

Removing Inactive Dynamic Subscriber VLANs

Subscriber session timeouts enable you to place limits on subscriber access based on how long the session has been up, how long the user has been inactive, or both. In configurations using dynamically created subscriber VLANs, the idle timeout also:

- Deletes the inactive subscriber VLANs when the inactivity threshold has been reached.
- Removes dynamic VLANs when no client sessions were ever created (for example, in the event no client sessions are created on the dynamic VLAN or following the occurrence of an error during session creation or client authentication where no client sessions are created on the dynamic VLAN).



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

To remove inactive dynamic subscriber VLANs:

1. Edit session options for the router access profile.

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

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

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

Related Documentation

- [Understanding Session Options for Subscriber Access on page 109](#)
- [Configuring Subscriber Session Options on page 111](#)
- [client-idle-timeout on page 666](#)

CHAPTER 9

Receiving DHCP Options From a RADIUS Server

- [Centrally Configured Opaque DHCP Options on page 114](#)
- [Monitoring DHCP Options Configured on RADIUS Servers on page 118](#)

Centrally Configured Opaque DHCP Options

Subscriber management (on the routers) or DHCP management (on the switches) enables you to centrally configure DHCP options on a RADIUS server and then distribute the options on a per-subscriber or per DHCP-client basis. This method results in RADIUS-sourced DHCP options—the DHCP options originate at the RADIUS server and are sent to the subscriber (or DHCP client). This differs from the traditional client-sourced method (also called DHCP-sourced) of configuring DHCP options, in which the options originate at the client and are sent to the RADIUS server. The subscriber management (DHCP management) RADIUS-sourced DHCP options are also considered to be *opaque*, because DHCP local server performs minimal processing and error checking for the DHCP options string before passing the options to the subscriber (DHCP client).

Subscriber management (or DHCP management) uses Juniper Networks VSA 26-55 (DHCP-Options) to distribute the RADIUS-sourced DHCP options. The RADIUS server includes VSA 26-55 in the Access-Accept message that the server returns during subscriber authentication or DHCP client authentication. The RADIUS server sends the Access-Accept message to the RADIUS client, and then on to DHCP local server for return to the DHCP subscriber. The RADIUS server can include multiple instances of VSA 26-55 in a single Access-Accept message. The RADIUS client concatenates the multiple instances and uses the result as a single instance.

There is no CLI configuration required to enable subscriber management (DHCP management) to use the centrally configured DHCP options—the procedure is triggered by the presence of VSA 26-55 in the RADIUS Access-Accept message.

When building the offer packet for the DHCP client, DHCP local server uses the following sequence:

1. Processes any RADIUS-configured parameters that are passed as separate RADIUS attributes; for example, RADIUS attribute 27 (Session Timeout).
2. Processes any client-sourced parameters; for example, RADIUS attributes 53 (DHCP Message Type) and 54 (Server Identifier).
3. Appends (without performing any processing) the opaque DHCP options string contained in the VSA 26-55 received from the RADIUS server.

In addition to supporting central configuration of DHCP options directly on the RADIUS server (RADIUS-sourced options), subscriber management (DHCP management) also supports the traditional client-sourced options configuration, in which the router's (switch's) DHCP component sends the options to the RADIUS server. The client-sourced DHCP options method is supported for both DHCP local server and DHCP relay agent; however, the RADIUS-sourced central configuration method is supported on DHCP local server only. Both the RADIUS-sourced and client-sourced methods support DHCPv4 and DHCPv6 subscribers (clients).



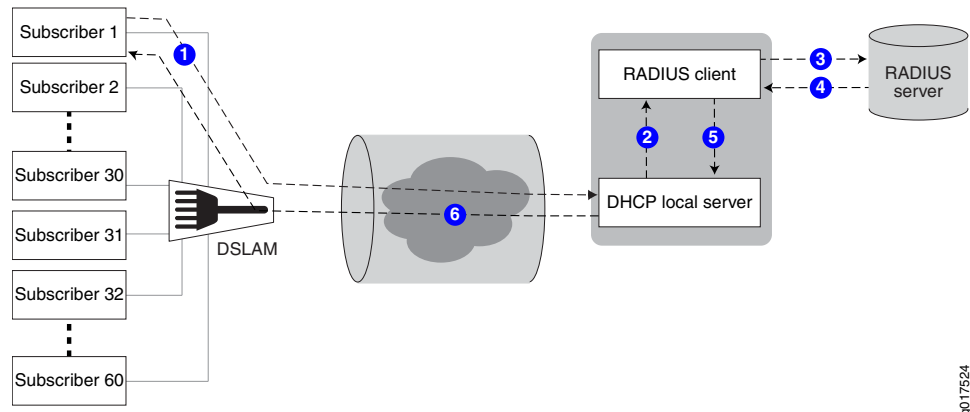
NOTE: You can use the RADIUS-sourced and client-sourced methods simultaneously on DHCP local server. However, you must ensure that the central configuration method does not include options that override client-sourced DHCP options, because this can create unpredictable results.

- [Data Flow for RADIUS-Sourced DHCP Options on page 116](#)
- [Multiple VSA 26-55 Instances Configuration on page 117](#)
- [DHCP Options That Cannot Be Centrally Configured on page 117](#)

Data Flow for RADIUS-Sourced DHCP Options

Figure 2 on page 116 shows the procedure subscriber management (DHCP management) uses when configuring DHCP options for subscribers (DHCP clients).

Figure 2: DHCP Options Data Flow



The following general sequence describes the data flow when subscriber management (DHCP management) uses RADIUS-sourced DHCP options and VSA 26-55 to configure a DHCP subscriber (client):

1. The subscriber (DHCP client) sends a DHCP discover message (or DHCPv6 solicit message) to the DHCP local server. The message includes client-sourced DHCP options.
2. The DHCP local server initiates authentication with the Junos OS RADIUS client.
3. The RADIUS client sends an Access-Request message on behalf of the subscriber (DHCP client) to the external RADIUS server. The message includes the subscriber's (DHCP client's) client-sourced DHCP options.
4. The external RADIUS server responds by sending an Access-Accept message to the RADIUS client. The Access-Accept message includes the RADIUS-sourced opaque DHCP options in VSA 26-55.
5. The RADIUS client sends the DHCP options string to DHCP local server. If there are multiple VSA 26-55 instances, the RADIUS client first assembles them into a single options string.
6. DHCP local server processes all options into the DHCP offer (or DHCPv6 reply) message, except for the RADIUS-sourced VSA 26-55 DHCP options. After processing all other options, DHCP local server then appends the unmodified VSA 26-55 DHCP options to the message and sends the message to the subscriber (DHCP client).

7. The subscriber (DHCP client) is configured with the DHCP options.
8. The following operations occur after the subscriber (DHCP client) receives the DHCP options:
 - Accounting—The RADIUS client sends Acct-Start and Interim-Accounting requests to the RADIUS server, including the RADIUS-sourced DHCP options in VSA 26-55. By default, the DHCP options are included in accounting requests.
 - Renewal—When the subscriber (DHCP client) renews, the cached DHCP options value is returned in the DHCP renew (or DHCPv6 ACK) message. The originally assigned DHCP options cannot be modified during a renew cycle.
 - Logout—When the subscriber (DHCP client) logs out, the RADIUS client sends an Acct-Stop message to the RADIUS server, including the RADIUS-sourced VSA 26-55.

Multiple VSA 26-55 Instances Configuration

VSA 26-55 supports a maximum size of 247 bytes. If your RADIUS-sourced DHCP options field is greater than 247 bytes, you must break the field up and manually configure multiple instances of VSA 26-55 for the RADIUS server to return. When using multiple instances for an options field, you must place the instances in the packet in the order in which the fragments are to be reassembled by the RADIUS client. The fragments can be of any size of 247 bytes or less.



BEST PRACTICE: For ease of configuration and management of your DHCP options, you might want to have one DHCP option per VSA 26-55 instance, regardless of the size of the option field.

When the RADIUS client returns a reassembled opaque options field in an accounting request to the RADIUS server, the client uses 247-byte fragments. If you had originally created instances of fewer than 247 bytes, the returned fragments might not be the same as you originally configured on the RADIUS server.



NOTE: If you are configuring Steel-Belted Radius (SBR) to support multiple VSA 26-55 instances, ensure that you specify VSA 26-55 with the RO flags in the Subscriber Management RADIUS dictionary file. The R value indicates a multivalued reply attribute and the O value indicates an ordered attribute.

DHCP Options That Cannot Be Centrally Configured

Table 16 on page 118 shows the DHCP options that you must not centrally configure on the RADIUS server.

Table 16: Unsupported Opaque DHCP Options

DHCP Option	Option Name	Comments
Option 0	Pad Option	Not supported.
Option 51	IP Address Lease Time	Value is provided by RADIUS attribute 27 (Session-Timeout).
Option 52	Option Overload	Not supported.
Option 53	DHCP Message Type	Value is provided by DHCP local server.
Option 54	Server Identifier	Value is provided by DHCP local server.
Option 55	Parameter Request List	Value is provided by DHCP local server.
Option 255	End	Value is provided by DHCP local server.
–	DHCP magic cookie	Not supported.

Related Documentation • [Monitoring DHCP Options Configured on RADIUS Servers on page 118](#)

Monitoring DHCP Options Configured on RADIUS Servers

Purpose View information for DHCP options that are centrally configured on a RADIUS server and that are distributed using Juniper Networks VSA 26-55 (DHCP-Options).

Action To display information for opaque DHCP options:

```

user@host> show subscribers detail
Type: DHCP
IP Address: 192.168.9.7
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-prof-23
MAC Address: 00:10:95:00:00:98
State: Active
Radius Accounting ID: jnpr :2304
Session Timeout (seconds): 3600
Idle Timeout (seconds): 600
Login Time: 2011-08-25 14:43:52 PDT
DHCP Options: len 52
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 08 33 04 00 00

```

```
00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 36 2f
33 2d 37 2d 30 37 05 01 06 0f 21 2c
```

Meaning DHCP Options: len 52
 35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 08 33 04 00 00
 00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 36 2f
 33 2d 37 2d 30 37 05 01 06 0f 21 2c

The DHCP options output provides the following information:

- The **len** field is the total number of hex values in the message.
- The hex values specify the type, length, and value (TLV) of DHCP options, and are converted to decimal to identify the DHCP options, as defined in RFC 2132.

The number of hex values that make up a particular DHCP option varies, depending on the length of the option. For example, the first DHCP option specified in the output includes three sets of hex values (**35 01 01**). The first hex value (**35**) identifies the option type, the second value (**01**) indicates the length of the value entry, which in this case is one set of hex values. The third hex value (**01**) specifies the value for the DHCP option.

In the second DHCP option specification (**39 02 02 40**), the hex value **39** is the type, and the length of **02** specifies that two sets of hex entries make up the value for the option. Therefore, this option specification uses four sets of hex entries; one for the type (**39**), one to specify the length (**02**), and two for the option value (**02 40**).

The third DHCP option is specified by the hex values **3d 07 01 00 10 94 00 00 08**. The hex value **3d** is the type, followed by the length (**07**), which specifies that the next seven sets of hex entries make up the value for the option. Therefore, this option specification uses a total of nine sets of hex entries; one for the type (**3d**), one to specify the length (**07**), and seven for the value of the DHCP option (**01 00 10 94 00 00 08**).

Table 17 on page 119 describes the first two options in more detail.

Table 17: DHCP Options Description

Option	Type	Length	Value
35 01 01	35 = decimal 53 (Code 53 in RFC 2132 is the DHCP Message Type option)	01 = the length of the option is one set of hex values (the next set in the list)	01 = value of the message type that is described in RFC 2132. The code 01 specifies a message type of DHCPDISCOVER.
39 02 02 40	39 = decimal 57 (Code 57 is the Maximum DHCP Message Size option)	02 = the length of the option is two sets of hex values (the next two sets in the list)	0240 = converted to a length of 576 octets

- Related Documentation**
- [Centrally Configured Opaque DHCP Options on page 114](#)
 - [show subscribers on page 1221](#)

CHAPTER 10

Configuring RADIUS Logical Line Identification

- [RADIUS Logical Line Identifier \(LLID\) Overview on page 121](#)
- [RADIUS Attributes for LLID Preauthentication Requests on page 122](#)
- [Configuring Logical Line Identification \(LLID\) Preauthentication on page 124](#)

RADIUS Logical Line Identifier (LLID) Overview

The logical line identification (LLID) feature helps service providers maintain a reliable and up-to-date customer database for those subscribers who frequently move from one physical line to another. The LLID feature is based on a virtual port — the LLID — rather than the physical line used by the subscriber.

The LLID is an alphanumeric string that is based on the subscriber user name and circuit ID. The LLID logically identifies the subscriber line, and is mapped to the subscriber's physical line in the service provider customer database. When the subscriber moves to a different location and different physical line, the database is updated to map the LLID to the new physical line. Because the subscriber's LLID remains constant, it provides service providers with a secure and reliable means for tracking subscribers and maintaining an accurate customer database. Subscriber management supports the LLID feature for PPP subscribers over PPPoE, PPPoA, and LAC.

To assign an LLID to a subscriber, the router issues two RADIUS access requests. The first request is a preauthentication request, which obtains the LLID from a RADIUS preauthentication server. The second request is the standard authentication request sent to the RADIUS authentication server.

The following sequence of steps describes how subscriber management obtains and uses the LLID. The procedure assumes that preauthentication is enabled on the router and that the RADIUS preauthentication and authentication servers are configured.

1. The PPP subscriber sends an Authentication-Request message to the router.
2. The router sends an Access-Request message to the RADIUS preauthentication server to obtain an LLID for the subscriber.
3. The preauthentication server returns the LLID to the router in the Calling-Station-Id attribute (RADIUS attribute 31) in the Access-Accept message.



NOTE: This step includes a non-standard use of the Calling-Station-Id attribute. This attribute is typically present in RADIUS request messages, such as an Access-Request, not in response messages. Also, the router ignores all RADIUS attributes, other than the Calling-Station-Id, that are returned in the preauthentication Access-Accept message. In addition, any radius options that are configured on the router, such as `calling-station-id-format`, have no effect on the Calling-Station-Id attribute in the preauthentication request.

4. The router encodes the Calling-Station-Id (the LLID) in a second Access-Request message and sends the message to the RADIUS authentication server. This authentication request is the standard use of the Calling-Station-Id attribute.
5. The RADIUS authentication server returns an Access-Accept message to the router. The Access-Accept message includes attributes for the subscriber session.



NOTE: Once the preauthenticated subscriber has been successfully authenticated by the RADIUS authentication server, all subsequent RADIUS request messages, such as Accounting-Request messages, will include the LLID in the Calling-Station-Id attribute.



NOTE: For tunneled PPP subscribers, the router, acting as an L2TP access concentrator (LAC), encodes the LLID into Calling Number AVP (L2TP attribute 22) and sends the attribute 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 the L2TP Calling Number AVP.

**Related
Documentation**

- [RADIUS Attributes for LLID Preauthentication Requests on page 122](#)
- [Configuring Logical Line Identification \(LLID\) Preauthentication on page 124](#)

RADIUS Attributes for LLID Preauthentication Requests

Table 18 on page 123 lists the RADIUS IETF attributes used in a preauthentication request to obtain a subscriber's LLID, and describes the information that is included in the attributes. In some cases, preauthentication uses an attribute for information that is different than the IETF description—the table indicates any non-standard use of RADIUS attributes.

Table 18: RADIUS Attributes for LLID Preauthentication Requests

Attribute Number	Attribute Name	Description
1	User-Name	<p>(Non-standard use of attribute.) Identifying information for the user associated with the LLID, in the following format.</p> <p><i>nas-port:nas-ip-address:nas-port-id</i></p> <p>Example: nas-port:172.28.30.117:ge-1/0/5:100</p> <p>NOTE: The router strips any dynamically generated information from the User-Name attribute during preauthentication.</p>
2	User-Password	<p>(Non-standard use of attribute.) Password of the user to be authenticated.</p> <p>Example: Always set to juniper</p>
4	NAS-IP-Address	<p>IP address of the network access server (NAS) that is requesting authentication of the user</p> <p>Example: 172.28.30.117</p>
5	NAS-Port	Physical port number of the NAS that is authenticating the user. Always interpreted as a bit field
6	Service-Type	<p>Type of service the user requested or the type of service to be provided.</p> <p>Example: gold-service</p>
61	NAS-Port-Type	Type of physical port the NAS is using to authenticate the user. You can use the ethernet-port-type-virtual statement to configure this to virtual (type 5).
77	Connect-Info	<p>(Non-standard use of attribute.) The user name.</p> <p>Example: jdoe@xyzcorp.east.com</p>
87	NAS-Port-Id	<p>Text string that identifies the physical interface of the NAS that is authenticating the user. Includes any dynamically generated information.</p> <p>Example: ge 1/0/5:100</p>

Related Documentation

- [RADIUS Logical Line Identifier \(LLID\) Overview on page 121](#)
- [Configuring Logical Line Identification \(LLID\) Preauthentication on page 124](#)

Configuring Logical Line Identification (LLID) Preauthentication

The logical line identification (LLID) feature enables service providers to track subscribers on the basis of a virtual port — the LLID — rather than by the physical port used by the subscriber. The LLID is assigned by a RADIUS preauthentication server, which you configure in an access profile.

To configure the router to support preauthentication for the LLID feature:



NOTE: You cannot configure the preauthentication statements in this procedure if you have configured the radius attributes `exclude` statement to exclude the Calling-Station-ID attribute from RADIUS Access-Request messages.

1. Specify the access profile you want to use for the subscriber preauthentication support.

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

2. Specify the order in which the router uses the supported preauthentication methods. **radius** is the only supported authentication method.

```
[edit access profile PreAuthLlid]
user@host# set preauthentication-order radius
```

3. Specify that you want to configure RADIUS support.

```
[edit access profile PreAuthLlid]
user@host# edit radius
```

4. Specify the IP address of the RADIUS server used for preauthentication.

```
[edit access profile PreAuthLlid radius]
user@host# set preauthentication-server 192.168.100.10
```



NOTE: The preauthentication feature uses the **retry** and **timeout** parameters that are configured for the RADIUS authentication server.

5. (Optional) Display AAA preauthentication statistics.

```
user@host> show network-access aaa statistics preauthentication
Preauthentication module statistics
  Requests received: 2118
  Multistack requests: 0
  Accepts: 261
  Rejects: 975
  Challenges: 0
  Requests timed out: 882
```

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

```
user@host1> show radius pre-authentication servers
```


RADIUS Pre-Authentication Configuration						
IP Address	Udp Port	Retry Count	Timeout	Maximum Sessions	Dead Time	Secret
10.192.168.10	1812	3	3	255	0	radius

- Related Documentation**
- [RADIUS Logical Line Identifier \(LLID\) Overview on page 121](#)
 - [RADIUS Attributes for LLID Preauthentication Requests on page 122](#)

CHAPTER 11

Configuring Domain Maps for Subscriber Management

- [Domain Mapping Overview on page 128](#)
- [Understanding Domain Maps and Logical System/Routing Instance Contexts on page 130](#)
- [Configuring a Domain Map on page 131](#)
- [Specifying an Access Profile in a Domain Map on page 132](#)
- [Specifying an Address Pool in a Domain Map on page 133](#)
- [Specifying a Dynamic Profile in a Domain Map on page 133](#)
- [Specifying an AAA Logical System/Routing Instance in a Domain Map on page 134](#)
- [Specifying a Target Logical System/Routing Instance in a Domain Map on page 135](#)
- [Configuring Domain and Realm Name Usage for Domain Maps on page 136](#)
- [Specifying Domain and Realm Name Delimiters on page 136](#)
- [Specifying the Parsing Order for Domain and Realm Names on page 137](#)
- [Specifying the Parsing Direction for Domain and Realm Names on page 138](#)
- [Enabling Domain Name Stripping on page 139](#)
- [Specifying a Tunnel Profile in a Domain Map on page 139](#)
- [Specifying a Tunnel Switch Profile in a Domain Map on page 140](#)
- [Configuring PADN Parameters for a Domain Map on page 140](#)

Domain Mapping Overview

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



NOTE: A subscriber's username is typically made up of two parts — the user's name followed by the user's domain name, which are separated by a delimiter character. The domain name is always to the right of the domain delimiter. For example, in the username, **juan@xyz.com**, the user's name, **juan** is followed by the domain name **xyz.com**, and the two are separated by the **@** delimiter character.

However, some systems use a username format in which the domain name *precedes* the user's name. To avoid confusion with the typical domain name usage, this type of preceding domain name is referred to as a realm name, and the realm name is to the left of the realm delimiter. For example, in the username, **top321.com/mary**, the **top321** part is the realm name, **mary** is the user's name, and the **/** character is the delimiter character.

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



NOTE: Subscriber management is supported in the default logical system only. The documentation for the subscriber management domain mapping feature describes using the **aaa-logical-system** and **target-logical-system** statements to configure mapping to a non-default logical system. These statements are for future extensions of subscriber management.

Table 19 on page 129 describes the access options and parameters you can configure in the domain map.

Table 19: Domain Map Options and Parameters

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

Default Domain Map

You can configure a default domain map that the router uses for subscribers whose domain or realm name does not explicitly match any existing domain map. Specify the name **default** as the **domain map *domain-map-name***.

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

Domain Map for Subscriber Usernames With No Domain or Realm Name

In some cases a subscriber username might not include a domain name or realm name—you can configure a specific domain map that the router uses for these subscribers. Specify the name **none** as the **domain map *domain-map-name***.

Related Documentation

- [Configuring a Domain Map on page 131](#)

Understanding Domain Maps and Logical System/Routing Instance Contexts

You can use a domain map to manage the logical system/routing instance that subscriber management uses for AAA and subscriber contexts. Subscriber management is supported in the default logical system only, so you manage the contexts by configuring the routing instance. The following list describes the two types of contexts.

- **Subscriber context**—The logical system/routing instance in which the subscriber interface is placed. For most dynamic subscriber sessions, the initial subscriber session context is the default logical system and default routing instance. One exception is LNS, in which the initial context for a dynamic LNS session (PPP over L2TP) is the same as the peer interface (the LAC facing interface). Therefore, for LNS sessions, if the peer interface uses a non-default routing instance, then the initial context of the subscriber session also uses that non-default routing instance.
- **AAA context**—The logical system/routing instance that the subscriber session uses for RADIUS interactions, such as authentication and accounting requests. By default, the AAA context is the same as the initial subscriber context. Therefore, for all subscriber sessions other than dynamic LNS sessions, authentication and authorization is performed in the default logical system/routing instance context, unless the default routing instance is explicitly changed.

You can optionally configure a domain map to use a specific subscriber or AAA context. For example, if a dynamic LNS session is initially created in a non-default routing instance (because the initial subscriber context uses the non-default routing instance), you might use the **target-routing-instance** statement to configure the domain map to place the subscriber in the default routing instance. Or, for security reasons, you might want to have all RADIUS interactions in a particular context. In this case, you would use the **aaa-routing-instance** statement to configure the domain map to change the initial AAA context to the new routing instance.

Using domain maps to manage AAA and subscriber contexts is also useful in layer 3 wholesale environments. For example, you might want to place dynamic VLAN interfaces in different non-default routing instances, while maintaining all RADIUS interactions in the default routing-instance. In this example, the initial AAA context is in the default routing instance, but RADIUS authorization places the subscriber VLAN session in a non-default routing instance. You can then include the **aaa-routing-instance** statement in the domain map, to specify that the AAA context uses the default routing instance for the dynamic VLAN session. The subscriber session is unchanged and remains in the non-default routing instance.

Related Documentation

- [Domain Mapping Overview on page 128](#)
- [Specifying a Target Logical System/Routing Instance in a Domain Map on page 135](#)

Configuring a Domain Map

To configure a domain map for subscriber management:

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

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

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

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

- To create a default domain map to be mapped to subscribers with non-matching domain names

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

- To create a domain map to be mapped to subscribers without a domain or realm name:

```
[edit access]
user@host# edit domain map none
```

2. (Optional) Specify the access profile used to apply access rules for the domain map.

See [“Specifying an Access Profile in a Domain Map” on page 132](#).

3. (Optional) For dynamic profiles, clarify the provided dynamic configuration for the subscriber session.

See [“Specifying a Dynamic Profile in a Domain Map” on page 133](#).

4. (Optional) Specify the address pool used to allocate address for the domain map.

See [“Specifying an Address Pool in a Domain Map” on page 133](#).

5. (Optional) Configure the target logical system/routing instance for the subscriber context.

See [“Specifying an AAA Logical System/Routing Instance in a Domain Map” on page 134](#).

6. (Optional) Configure the target logical system/routing instance in which AAA requests are sent for the domain map.

See [“Specifying a Target Logical System/Routing Instance in a Domain Map” on page 135](#).

7. (Optional) Configure rules for domain names; for example; delimiters, parsing direction, and domain stripping. Delimiters and parsing direction are configured globally for all domain maps. Domain stripping is enabled in the domain map.

See [“Configuring Domain and Realm Name Usage for Domain Maps” on page 136](#).

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

See [“Specifying a Tunnel Profile in a Domain Map”](#) on page 139.

9. (Optional) Assign a tunnel switch profile to be applied by the domain map.

See [“Specifying a Tunnel Switch Profile in a Domain Map”](#) on page 140.

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

See [“Configuring PADN Parameters for a Domain Map”](#) on page 140.

Related Documentation

- [Domain Mapping Overview on page 128](#)
- [Verifying and Managing Domain Map Configuration on page 183](#)

Specifying an Access Profile in a Domain Map

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

Access profiles can be specified or modified in several different ways. If conflicts occur, the router applies the access profiles based on the precedence rules shown in [Table 20 on page 132](#).

Table 20: Precedence Rules for Applying Access Profiles

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

To include an access profile in a domain map:

1. Specify the domain map you want to configure.

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

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

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


- Related Documentation**
- [Domain Mapping Overview on page 128](#)
 - [Configuring a Domain Map on page 131](#)

Specifying an Address Pool in a Domain Map

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

Address pools can be specified or modified in several different ways. If conflicts occur, the router applies the address pool based on the precedence rules shown in [Table 21 on page 133](#).

Table 21: Precedence Rules for Determining the Address Pool to Use

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

To specify the address pool used for a domain map:

1. Specify the domain map you want to configure.


```
[edit access]
user@host# edit domain map domain-map-name
```
2. Specify the address pool you want to use for the domain map.


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

- Related Documentation**
- [Domain Mapping Overview on page 128](#)
 - [Configuring a Domain Map on page 131](#)

Specifying a Dynamic Profile in a Domain Map

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

Dynamic profiles are configured at the **[edit dynamic-profiles]** hierarchy, and can be specified or modified in several different ways. If conflicts occur, the router applies the dynamic profiles based on the precedence rules shown in [Table 22 on page 134](#).

Table 22: Precedence Rules for Applying Dynamic Profiles

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

To include a dynamic profile in a domain map:

1. Specify the domain map you want to configure.

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

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

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

Related Documentation

- [Domain Mapping Overview on page 128](#)
- [Configuring a Domain Map on page 131](#)

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

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



NOTE: Changing the AAA context does not change the subscriber context. You use the **target-logical-system** statement to explicitly configure the logical system/routing instance for subscribers.

To configure the logical system/routing instance context used for AAA requests:

1. Specify the domain map you want to configure.

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

- Specify the routing instance. If a non-default routing instance is currently configured, you can use the **default** option to specify that the domain map use the default routing instance. The AAA logical system is automatically set to the default.

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



NOTE: Subscriber management is supported in the default logical system only.

Related Documentation

- [Domain Mapping Overview on page 128](#)
- [Understanding Domain Maps and Logical System/Routing Instance Contexts on page 130](#)
- [Configuring a Domain Map on page 131](#)
- [Understanding Domain Maps and Logical System/Routing Instance Contexts on page 130](#)
- [Specifying a Target Logical System/Routing Instance in a Domain Map on page 135](#)

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

By default, the router places a subscriber in the logical system/routing instance context of the interface on which the subscriber negotiations start. You can later change the routing instance of the subscriber's context through the use of either a domain map or the RADIUS authentication server.

Subscriber management is supported in the default logical system only, however you can configure the domain map to use a non-default routing instance. Also, if a non-default routing instance is already configured, you can configure the domain map to use the default routing instance.

To configure the logical system/routing instance context used for a subscriber's interface :

- Specify the domain map you want to configure.

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

- Specify the target routing instance (the default logical system is used by default). If a non-default routing instance is currently configured, you can use the **default** option to specify that the domain map use the default routing instance.

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



NOTE: Subscriber management is supported in the default logical system only.

- Related Documentation**
- [Domain Mapping Overview on page 128](#)
 - [Understanding Domain Maps and Logical System/Routing Instance Contexts on page 130](#)
 - [Configuring a Domain Map on page 131](#)
 - [Understanding Domain Maps and Logical System/Routing Instance Contexts on page 130](#)

Configuring Domain and Realm Name Usage for Domain Maps

You can configure how the router determines the domain names that are used for the domain mapping feature. At the global level, you can specify rules that are used for domain maps. The global rules enable you to specify additional characters that the router can recognize as domain or realm name delimiters and to specify the direction the router uses to parse domain or realm names. The purpose of parsing a domain or realm name is to identify a single, unique name that the router uses as the subscriber's domain name, regardless of whether the source of the name is in the typical domain name format (joseph@abc.com) or in the realm name format (abc.com\marilyn). The router uses the resulting domain name for operations such as domain map lookup and processing. At the domain map level, you can also enable domain name stripping. Domain name stripping specifies that the router remove the parsed domain or realm name from the subscriber username prior to performing any additional processing for the domain map.

To configure domain name usage rules for domain maps:

1. (Optional) For domain or realm names, configure the parsing order, which specifies whether the router searches for the domain name or the realm name first.
[See "Specifying the Parsing Order for Domain and Realm Names" on page 137.](#)
2. (Optional) For domain or realm names, configure the delimiters you want the router to recognize for domain maps.
[See "Specifying Domain and Realm Name Delimiters" on page 136.](#)
3. (Optional) For domain or realm names, configure the parse direction you want the router to use when determining domain names for domain maps.
[See "Specifying the Parsing Direction for Domain and Realm Names" on page 138.](#)
4. (Optional) For domain names, configure the router to remove the parsed domain or realm name from usernames in the domain map before using AAA services.
[See "Enabling Domain Name Stripping" on page 139.](#)

- Related Documentation**
- [Domain Mapping Overview on page 128](#)
 - [Configuring a Domain Map on page 131](#)

Specifying Domain and Realm Name Delimiters

A delimiter is the character that separates a subscriber username from the domain or realm name. Delimiters are commonly used for domain or realm name parsing or domain

name stripping. You can specify a maximum of eight delimiters that the router uses to recognize domain or realm names for a domain map. If you do not configure any delimiters, the router uses the @ character by default for domain names. There is no default delimiter for realm names.

For example, your network might include the subscribers **bob@abc.com**, **pete!xyz.com**, and **prq.com\maria**. In this case, you would configure the router to recognize the characters @ and ! as domain name delimiters, and the \ character as a realm name delimiter.

Keep the following guidelines in mind when specifying delimiters:

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

To configure domain and realm name delimiters for domain maps:

1. Specify that you want to configure domain attributes.

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

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

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

3. Specify the characters you want to use as realm name delimiters. Do not include spaces between the delimiters.

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

Related Documentation • [Configuring Domain and Realm Name Usage for Domain Maps on page 136](#)

Specifying the Parsing Order for Domain and Realm Names

The router parses the username domain or realm name in order to identify a single, unique name that the router uses as the subscriber's domain name, regardless of whether the source of the name is in the typical domain name format (joseph@abc.com) or in the realm name format (abc.com\marilyn). You can specify whether the router first searches the subscriber username for a domain name or for a realm name. If the router does not find the specified name (for example, you specify **realm-first** and there is no realm name in the username), then the router searches for the second type of name (domain name, in this case). If the router does not find either a realm-name or a domain name, then there is no domain that can be used for domain mapping operations.

To configure the domain name parsing direction for domain maps:

1. Specify that you want to configure domain attributes.

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

2. Specify the parsing order you want the router to use, either the domain name first or the realm name first.

```
[edit access domain]  
user@host# set parse-order domain-first
```

Related Documentation • [Configuring Domain and Realm Name Usage for Domain Maps on page 136](#)

Specifying the Parsing Direction for Domain and Realm Names

You can specify the direction in which the router performs the parsing operation it uses to identify subscriber domain or realm names for domain maps. During the parsing operation, the router searches the username until it recognizes a delimiter. It then considers anything to the right of the delimiter as the domain. By default, the router parses from right to left, starting at the right-most character in the username.

The router uses a subscriber's domain name to perform domain map lookup and processing operations. You can configure how the router identifies a unique domain name when the user's name is presented in a traditional domain name format or a realm name. In the traditional domain name format, the user's name is following by the domain name (for example, joe@abc.com). In the realm name format, the user's name is preceded by the domain name (referred to as the realm name, for example, abc.com@joe). The purpose of parsing a domain or realm name is to identify a single name that the router uses as the subscriber's domain name, regardless if the source of the name is the user's original domain name or realm name. The router uses the resulting domain name for operations such as domain map lookup and processing. At the domain map level, you can also enable domain name stripping.

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

To configure the domain name parsing direction for domain maps:

1. Specify that you want to configure domain attributes.

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

2. Specify the parsing direction you want the router to use if the username uses the typical domain name format, in which the domain name follows the user's name.

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

3. Specify the parsing direction you want the router to use if the username uses the realm name format, in which the realm name precedes the user's name.

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

**Related
Documentation**

- [Configuring Domain and Realm Name Usage for Domain Maps on page 136](#)

Enabling Domain Name Stripping

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

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

1. Specify the domain map for the stripping operation.

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

2. Enable domain name stripping.

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

**Related
Documentation**

- [Configuring Domain and Realm Name Usage for Domain Maps on page 136](#)

Specifying a Tunnel Profile in a Domain Map

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



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

To include a tunnel profile in a domain map:

1. Specify the domain map you want to configure.

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

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

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

- Related Documentation**
- [Domain Mapping Overview on page 128](#)
 - [Configuring a Domain Map on page 131](#)
 - [Configuring a Tunnel Profile for Subscriber Access](#)

Specifying a Tunnel Switch Profile in a Domain Map

Tunnel switch profiles determine whether packets in an L2TP subscriber session from a LAC are switched to another session that has a different destination LNS. The tunnel switch profile can also specify how certain L2TP AVPs are handled when the packets are switched to a second tunnel. The domain map feature enables you to apply a specific tunnel switch profile to subscribers in a particular domain.



NOTE: A tunnel switch profile specified by a RADIUS server in the Tunnel Switch-Profile VSA (26-91) takes precedence over the tunnel switch profile specified in the domain map. If the Tunnel-Group VSA (26-64) is received in addition to the Tunnel Switch-Profile VSA (26-91), the Tunnel Switch-Profile VSA (26-91) takes precedence over the Tunnel-Group VSA (26-64), ensuring that the subscribers are tunnel switched rather than LAC tunneled.

To include a tunnel switch profile in a domain map:

1. Specify the domain map you want to configure.

```
[edit access]  
user@host# edit domain map domain-map-name
```
2. Specify the tunnel switch profile you want to include in the domain map.

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

- Related Documentation**
- [Domain Mapping Overview on page 128](#)
 - [Configuring a Domain Map on page 131](#)
 - [Configuring L2TP Tunnel Switching](#)

Configuring PADN Parameters for a Domain Map

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

To configure PADN parameters in a domain map:

1. Specify the domain map you want to configure.

[edit access]

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

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

[edit access domain map *domain-map-name*]

user@host# **set** **padn** *destination-address* **mask** *destination-mask* **metric** *route-metric*

- Related Documentation**
- [Domain Mapping Overview on page 128](#)
 - [Configuring a Domain Map on page 131](#)

CHAPTER 12

Configuring Dynamic Service Activation for Subscriber Access

- [Using RADIUS Dynamic Requests for Subscriber Access Management on page 143](#)
- [Dynamic Service Activation During Login Overview on page 144](#)
- [Configuring RADIUS-Initiated Dynamic Request Support on page 144](#)
- [RADIUS-Initiated Change of Authorization \(CoA\) Overview on page 145](#)
- [Usage Thresholds for Subscriber Services on page 147](#)
- [RADIUS-Initiated Disconnect Overview on page 148](#)
- [Error-Cause Codes \(RADIUS Attribute 101\) for Dynamic Requests on page 149](#)

Using RADIUS Dynamic Requests for Subscriber Access Management

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

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

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

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

Related Documentation

- [Dynamic Service Activation During Login Overview on page 144](#)
- [RADIUS-Initiated Change of Authorization \(CoA\) Overview on page 145](#)
- [RADIUS-Initiated Disconnect Overview on page 148](#)
- [Configuring RADIUS-Initiated Dynamic Request Support on page 144](#)
- [RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework on page 13](#)
- [Error-Cause Codes \(RADIUS Attribute 101\) for Dynamic Requests on page 149](#)

Dynamic Service Activation During Login Overview

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

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

As part of dynamic service activation, you can also specify usage thresholds for the service—when the threshold is reached, the service is deactivated. You use Juniper Networks VSAs to set the thresholds for the maximum traffic volume for a service and for the length of time the service can be active.

Related Documentation

- [Using RADIUS Dynamic Requests for Subscriber Access Management on page 143](#)
- [Configuring RADIUS-Initiated Dynamic Request Support on page 144](#)
- [RADIUS-Initiated Disconnect Overview on page 148](#)
- [RADIUS-Initiated Change of Authorization \(CoA\) Overview on page 145](#)
- [Usage Thresholds for Subscriber Services on page 147](#)

Configuring RADIUS-Initiated Dynamic Request Support

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

To configure RADIUS dynamic request support:

- Specify the IP address of the RADIUS server.

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

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

- Specify the IP addresses of multiple RADIUS servers.

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

```
user@host# set authentication-server 192.168.1.3 192.168.10.15
```

Related Documentation

- [Using RADIUS Dynamic Requests for Subscriber Access Management on page 143](#)
- [Dynamic Service Activation During Login Overview on page 144](#)
- [RADIUS-Initiated Change of Authorization \(CoA\) Overview on page 145](#)
- [RADIUS-Initiated Disconnect Overview on page 148](#)
- [RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework on page 13](#)
- [Error-Cause Codes \(RADIUS Attribute 101\) for Dynamic Requests on page 149](#)

RADIUS-Initiated Change of Authorization (CoA) Overview

The AAA Service Framework uses CoA messages to dynamically modify active subscriber sessions. For example, RADIUS attributes in CoA messages might instruct the framework to create, modify, or terminate a subscriber service. You can also use CoA messages to set or modify usage thresholds for current subscriber services.

CoA Messages

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

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

Qualifications for Change of Authorization

To complete the change of authorization for a user, you specify identification attributes and session attributes. The identification attributes identify the subscriber. Session attributes specify the operation (activation or deactivation) to perform on the subscriber's session and also include any client attributes for the session (for example, QoS attributes). The AAA Service Framework handles the actual request.

[Table 23 on page 146](#) shows the identification attributes for CoA operations.



NOTE: Using the Acct-Session-ID attribute to identify the subscriber session is more explicit than using the User-Name attribute. When you use the User-Name as the identifier, the CoA operation is applied to the first session that was logged in with the specified username. However, because a subscriber might have multiple sessions associated with the same username, the first session might not be the correct session for the CoA operation.

When you use the Acct-Session-ID attribute, it identifies the specific subscriber session, avoiding that potential error. Although the Acct-Session-ID attribute can include an interface specifier in addition to the session ID—when the attribute is in the description format—only the session ID is used for subscriber matching. For example, if the subscriber has a subscriber session ID of 54785, then the subscriber is matched when the Acct-Session-ID attribute is 54785 (decimal format), or `jnpr demux0.1073759682:54785` (description format), or indeed *any value:54785* (description format).

Table 23: Identification Attributes

Attribute	Description
User-Name [RADIUS attribute 1]	Subscriber username.
Acct-Session-ID [RADIUS attribute 44]	Specific subscriber session.

Table 24 on page 146 shows the session attributes for CoA operations. Any additional client attributes that you include depend on your particular session requirements.

Table 24: Session Attributes

Attribute	Description
Activate-Service [Juniper Networks VSA 26-65]	Service to activate for the subscriber.
Deactivate-Service [Juniper Networks VSA 26-66]	Service to deactivate for the subscriber.
Service-Volume [Juniper Networks VSA 26-67]	Amount of traffic, in MB, that can use the service; service is deactivated when the volume is exceeded.
Service-Timeout [Juniper Networks VSA 26-68]	Number of seconds that the service can be active; service is deactivated when the timeout expires.
Service-Volume-Gigawords [Juniper Networks VSA 26-179]	Amount of traffic, in 4GB units, that can use the service; service is deactivated when the volume is exceeded.
Update-Service [Juniper Networks VSA 26-180]	New values of service and time quotas for existing service.

Message Exchange

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

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

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



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

Related Documentation

- [Using RADIUS Dynamic Requests for Subscriber Access Management on page 143](#)
- [Dynamic Service Activation During Login Overview on page 144](#)
- [RADIUS-Initiated Disconnect Overview on page 148](#)
- [Configuring RADIUS-Initiated Dynamic Request Support on page 144](#)
- [Usage Thresholds for Subscriber Services on page 147](#)

Usage Thresholds for Subscriber Services

Subscriber management enables you to manage subscriber services by establishing usage thresholds when a service is dynamically activated or when an existing service is modified by a RADIUS CoA action. The service is deactivated when the specified threshold is reached.

Subscriber management supports two types of usage thresholds—traffic volume and time. You use Juniper Networks VSAs to set the usage thresholds. The VSAs are transmitted in RADIUS Access-Accept messages for dynamically activated services, or in RADIUS-initiated CoA-Request messages for existing services. The volume threshold sets the maximum amount of the total input and output traffic that can use the service before the service is deactivated. A time threshold sets the maximum length of time that the service can be active. [Table 25 on page 148](#) shows the VSAs used for volume and time thresholds.

Table 25: Juniper Network VSAs Used for Service Thresholds

Attribute Number	Attribute Name	Description	Value
26-67	Service-Volume	Amount of input and output traffic, in MB, that can use the service; service is deactivated when the volume is exceeded. Tagged VSA, which supports 8 tags (1-8). The router polls the traffic in 10 minute intervals.	<ul style="list-style-type: none"> range = 0 through 16777215 MB 0 = no limit
26-68	Service-Timeout	Number of seconds that the service can be active; service is deactivated when the timeout expires. Tagged VSA, which supports 8 tags (1-8).	<ul style="list-style-type: none"> range = 0 through 16777215 seconds 0 = no timeout
26-179	Service-Volume-Gigabits	Amount of input and output traffic, in 4GB units, that can use the service; service is deactivated when the volume is exceeded. Tagged VSA, which supports 8 tags (1-8). The router polls the traffic in 10 minute intervals.	<ul style="list-style-type: none"> range = 0 through 16777215 4GB units 0 = no limit
26-180	Update-Service	New values of service and time quotas for an existing service. Tagged VSA, which supports 8 tags (1-8).	string: <i>service-name</i>

Related Documentation

- [Dynamic Service Activation During Login Overview on page 144](#)
- [RADIUS-Initiated Change of Authorization \(CoA\) Overview on page 145](#)

RADIUS-Initiated Disconnect Overview

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

Disconnect Messages

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

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

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

Qualifications for Disconnect

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

Message Exchange

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

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

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



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

Related Documentation

- [Using RADIUS Dynamic Requests for Subscriber Access Management on page 143](#)
- [Dynamic Service Activation During Login Overview on page 144](#)
- [Configuring RADIUS-Initiated Dynamic Request Support on page 144](#)

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

When a RADIUS-initiated CoA or disconnect operation is unsuccessful, the router includes an error-cause attribute (RADIUS attribute 101) in the CoA-NAK or Disconnect-NAK message that it sends back to the RADIUS server. If the detected error does not map to one of the supported error-cause attributes, the router sends the message without an error-cause attribute. [Table 26 on page 150](#) describes the error-cause codes.

Table 26: Error-Cause Codes (RADIUS Attribute 101)

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

- Related Documentation**
- [RADIUS-Initiated Change of Authorization \(CoA\) Overview on page 145](#)
 - [RADIUS-Initiated Disconnect Overview on page 148](#)

Configuring Terminate Reasons for Protocols

- [Mapping Application Terminate Reasons and RADIUS Terminate Codes on page 151](#)
- [Configuring Custom Terminate Reason Mappings on page 153](#)
- [AAA Terminate Reasons on page 154](#)
- [DHCP Terminate Reasons on page 155](#)
- [L2TP Terminate Reasons on page 156](#)
- [PPP Terminate Reasons on page 172](#)

Mapping Application Terminate Reasons and RADIUS Terminate Codes

The Junos OS software uses default configuration mapping of terminate reasons for various protocols (AAA, DHCP, L2TP, and PPP) to RADIUS Acct-Terminate-Cause attributes. You can optionally create customized mappings between a terminate reason and a RADIUS Acct-Terminate-Cause attribute, enabling you to provide different information about the cause of a termination.

When a AAA, DHCP, 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.



NOTE: A single mapping for RADIUS account termination is shared by all clients.

[Table 27 on page 151](#) 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 27: Supported RADIUS Acct-Terminate-Cause Codes

Code	Name	Description
1	User Request	User initiated the disconnect (log out)

Table 27: Supported RADIUS Acct-Terminate-Cause Codes (*continued*)

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

Table 27: Supported RADIUS Acct-Terminate-Cause Codes (*continued*)

Code	Name	Description
22	Port Administratively Disabled	The port has been administratively disabled

Related Documentation

- [Configuring Custom Terminate Reason Mappings on page 153](#)
- [AAA Terminate Reasons on page 154](#)
- [DHCP Terminate Reasons on page 155](#)
- [L2TP Terminate Reasons on page 156](#)
- [PPP Terminate Reasons on page 172](#)

Configuring Custom Terminate Reason Mappings

Junos OS supports default configuration mapping of terminate reasons for various protocols (AAA, DHCP, L2TP, and PPP) to RADIUS Acct-Terminate-Cause attributes. When a AAA, DHCP, 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 create customized mappings between a terminate reason and a RADIUS Acct-Terminate-Cause attribute to provide different information about the cause of a termination.

To configure customized mappings between a terminate reason and a RADIUS Acct-Terminate-Cause attribute:

1. Edit the **access** hierarchy.

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

2. Edit the **terminate-code** statement.



NOTE: Terminate codes do not appear as options on platforms where they are not supported.

```
[edit access]
user@host# edit terminate-code
```

3. Specify the protocol option (aaa (deny | shutdown) | dhcp | l2tp | ppp) that you want to modify.

```
[edit access terminate-code]
user@host# set protocol-option
```

4. Specify the terminate reason that you want to modify.

```
[edit access terminate-code protocol-option]
user@host# set term-reason
```



NOTE: Attempts to set a terminate reason mapping to its default value are rejected by the CLI.

- Specify the RADIUS termination cause value (from 1 through 4294967295) that you want to use for the termination reason.

```
[edit access terminate-code protocol-option term-reason]
user@host# set radius term-cause
```



NOTE: Deleting a customized mapping restores the default.

Related Documentation

- [Mapping Application Terminate Reasons and RADIUS Terminate Codes on page 151](#)
- [AAA Terminate Reasons on page 154](#)
- [DHCP Terminate Reasons on page 155](#)
- [L2TP Terminate Reasons on page 156](#)
- [PPP Terminate Reasons on page 172](#)

AAA Terminate Reasons

Table 28 on page 154 lists the default AAA terminate mappings. The table indicates the supported AAA deny and shutdown reasons and the RADIUS Acct-Terminate-Cause attributes they are mapped to by default.

Table 28: Default AAA Mappings

AAA Deny or Shutdown Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
deny address allocation failure	17	user error
deny no-resources	10	NAS request
deny server- request-timeout	17	user error
shutdown idle-timeout	4	idle timeout
		NOTE: The default mapping is to RADIUS accounting NAS Request (10) terminate cause.

Table 28: Default AAA Mappings (*continued*)

AAA Deny or Shutdown Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
shutdown session-timeout	5	session timeout
		NOTE: The default mapping is to RADIUS accounting NAS Request (10) terminate cause.
shutdown administrative-reset	6	admin reset
shutdown remote-reset	10	NAS request



NOTE: The `idle-timeout` and `session-timeout` terminate reasons both had a default mapping to RADIUS accounting NAS Request (10) terminate cause. To support backward compatibility, you can configure the router to support the previous mapping by using the `terminate-code aaa shutdown (idle-timeout | session-timeout) radius 10` statement at the `[edit access]` hierarchy level.

Related Documentation

- [Mapping Application Terminate Reasons and RADIUS Terminate Codes on page 151](#)
- [Configuring Custom Terminate Reason Mappings on page 153](#)

DHCP Terminate Reasons

Table 29 on page 155 lists the default DHCP terminate mappings. The table indicates the supported DHCP terminate reasons and the RADIUS Acct-Terminate-Cause attributes they are mapped to by default.

Table 29: Default DHCP Mappings

DHCP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
nak	15	service unavailable
nas logout	10	NAS request
no offers	4	idle timeout
lost-carrier	2	session terminated / modem dropped DCD
client request	1	user request

- Related Documentation**
- [Mapping Application Terminate Reasons and RADIUS Terminate Codes on page 151](#)
 - [Configuring Custom Terminate Reason Mappings on page 153](#)

L2TP Terminate Reasons

Table 30 on page 156 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 30: Default L2TP Mappings

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
issu in progress	9	NAS error
session access interface down	8	port error
session admin close	6	admin reset
session admin drain	6	admin reset
session call down	10	NAS request
session call failed	15	service unavailable
session create failed limit reached	9	NAS error
session create failed no resources	9	NAS error
session create failed single shot tunnel already fired	9	NAS error
session create failed too busy	9	NAS error
session failover protocol resync disconnect	6	admin reset
session hardware unavailable	8	port error
session no resources server port	9	NAS error
session not ready	9	NAS error
session rx cdn	10	NAS request
session rx cdn avp bad hidden	10	NAS request
session rx cdn avp bad value assigned session id	10	NAS request

Table 30: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 30: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session rx iccn avp unknown	10	NAS request
session rx iccn no resources	10	NAS request
session rx iccn unexpected	10	NAS request
session rx icrp avp bad hidden	10	NAS request
session rx icrp avp bad value assigned session id	10	NAS request
session rx icrp avp duplicate value assigned session id	10	NAS request
session rx icrp avp malformed bad length	10	NAS request
session rx icrp avp malformed truncated	10	NAS request
session rx icrp avp missing mandatory assigned session id	10	NAS request
session rx icrp avp missing random vector	10	NAS request
session rx icrp avp missing secret	10	NAS request
session rx icrp avp unknown	10	NAS request
session rx icrp no resources	10	NAS request
session rx icrp unexpected	10	NAS request
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

Table 30: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session rx icrq avp missing mandatory assigned session id	10	NAS request
session rx icrq avp missing mandatory call serial number	10	NAS request
session rx icrq avp missing random vector	10	NAS request
session rx icrq avp missing secret	10	NAS request
session rx icrq avp unknown	10	NAS request
session rx icrq no resources	10	NAS request
session rx icrq unexpected	10	NAS request
session rx occn avp bad hidden	10	NAS request
session rx occn avp bad value framing type	10	NAS request
session rx occn avp malformed bad length	10	NAS request
session rx occn avp malformed truncated	10	NAS request
session rx occn avp missing mandatory connect speed	10	NAS request
session rx occn avp missing mandatory framing type	10	NAS request
session rx occn avp missing random vector	10	NAS request
session rx occn avp missing secret	10	NAS request
session rx occn avp unknown	10	NAS request
session rx occn no resources	10	NAS request
session rx occn unexpected	10	NAS request
session rx ocrp avp bad hidden	10	NAS request
session rx ocrp avp bad value assigned session id	10	NAS request
session rx ocrp avp duplicate value assigned session id	10	NAS request
session rx ocrp avp malformed bad length	10	NAS request
session rx ocrp avp malformed truncated	10	NAS request

Table 30: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 30: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session rx ocrq avp missing secret	10	NAS request
session rx ocrq avp unknown	10	NAS request
session rx ocrq no resources	10	NAS request
session rx ocrq unexpected	10	NAS request
session rx ocrq unsupported	9	NAS error
session rx sli avp bad hidden	10	NAS request
session rx sli avp bad value accm	10	NAS request
session rx sli avp malformed bad length	10	NAS request
session rx sli avp malformed truncated	10	NAS request
session rx sli avp missing mandatory accm	10	NAS request
session rx sli avp missing random vector	10	NAS request
session rx sli avp missing secret	10	NAS request
session rx sli avp unknown	10	NAS request
session rx sli no resources	10	NAS request
session rx unexpected packet lac incoming	10	NAS request
session rx unexpected packet lac outgoing	10	NAS request
session rx unexpected packet lns incoming	10	NAS request
session rx unexpected packet lns outgoing	10	NAS request
session rx unknown session id	10	NAS request
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

Table 30: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
session rx wen avp missing random vector	10	NAS request
session rx wen avp missing secret	10	NAS request
session rx wen avp unknown	10	NAS request
session rx wen no resources	10	NAS request
session timeout connection	10	NAS request
session timeout inactivity	4	idle timeout
session timeout session	5	session timeout
session timeout upper create	9	NAS error
session transmit speed unavailable	9	NAS error
session tunnel down	15	service unavailable
session tunnel failed	15	service unavailable
session tunnel switch profile deleted	6	admin reset
session tunneled interface down	8	port error
session unknown cause	9	NAS error
session upper create failed	9	NAS error
session upper removed	15	service unavailable
session warmstart not operational	15	service unavailable
session warmstart recovery error	15	service unavailable
session warmstart upper not restacked	10	NAS request
tunnel admin close	6	admin reset
tunnel admin drain	6	admin reset
tunnel control channel failed	15	service unavailable
tunnel created no sessions	1	user request

Table 30: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 30: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 30: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 30: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx sccrq avp missing mandatory protocol version	15	service unavailable
tunnel rx sccrq avp missing random vector	15	service unavailable
tunnel rx sccrq avp missing secret	15	service unavailable
tunnel rx sccrq avp unexpected challenge without secret	15	service unavailable
tunnel rx sccrq avp unknown	15	service unavailable
tunnel rx sccrq bad address	15	service unavailable
tunnel rx sccrq no resources	15	service unavailable
tunnel rx sccrq no resources max tunnels	15	service unavailable
tunnel rx sccrq session id not null	15	service unavailable
tunnel rx sccrq unexpected	15	service unavailable
tunnel rx stopccn	1	user request
tunnel rx stopccn avp bad hidden	15	service unavailable
tunnel rx stopccn avp bad value assigned tunnel id	15	service unavailable
tunnel rx stopccn avp duplicate value assigned tunnel id	15	service unavailable
tunnel rx stopccn avp malformed bad length	15	service unavailable
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

Table 30: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx frs avp malformed truncated	15	service unavailable
tunnel rx frs avp missing mandatory failover session state	15	service unavailable
tunnel rx frs avp missing random vector	15	service unavailable
tunnel rx frs avp missing secret	15	service unavailable
tunnel rx frs avp unknown	15	service unavailable
tunnel rx frs no resources	15	service unavailable
tunnel rx frs session id not null	15	service unavailable
tunnel rx fsq avp bad hidden	15	service unavailable
tunnel rx fsq avp malformed bad length	15	service unavailable
tunnel rx fsq avp malformed truncated	15	service unavailable
tunnel rx fsq avp missing mandatory failover session state	15	service unavailable
tunnel rx fsq avp missing random vector	15	service unavailable
tunnel rx fsq avp missing secret	15	service unavailable
tunnel rx fsq avp unknown	15	service unavailable
tunnel rx fsq no resources	15	service unavailable
tunnel rx fsq session id not null	15	service unavailable
tunnel rx fsr avp bad hidden	15	service unavailable
tunnel rx fsr avp malformed bad length	15	service unavailable
tunnel rx unexpected packet	15	service unavailable
tunnel rx unexpected packet for session	15	service unavailable
tunnel rx unknown packet message type indecipherable	15	service unavailable
tunnel rx unknown packet message type unrecognized	15	service unavailable
tunnel rx recovery sccn authenticate failed challenge	17	user error

Table 30: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 30: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx recovery sccrp avp malformed bad length	15	service unavailable
tunnel rx recovery sccrp avp malformed truncated	15	service unavailable
tunnel rx recovery sccrp avp mismatched host name	15	service unavailable
tunnel rx recovery sccrp avp mismatched vendor name	15	service unavailable
tunnel rx recovery sccrp avp missing challenge response	17	user error
tunnel rx recovery sccrp avp missing mandatory assigned tunnel id	15	service unavailable
tunnel rx recovery sccrp avp missing mandatory framing capabilities	15	service unavailable
tunnel rx recovery sccrp avp missing mandatory host name	15	service unavailable
tunnel rx recovery sccrp avp missing mandatory protocol version	15	service unavailable
tunnel rx recovery sccrp avp missing random vector	15	service unavailable
tunnel rx recovery sccrp avp missing secret	15	service unavailable
tunnel rx recovery sccrp avp unexpected challenge response	15	service unavailable
tunnel rx recovery sccrp avp unexpected challenge without secret	15	service unavailable
tunnel rx recovery sccrp avp unknown	15	service unavailable
tunnel rx recovery sccrp no resources	15	service unavailable
tunnel rx recovery sccrp session id not null	15	service unavailable
tunnel rx recovery 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

Table 30: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
tunnel rx recovery sccrq avp bad value framing capabilities	15	service unavailable
tunnel rx recovery sccrq avp bad value protocol version	15	service unavailable
tunnel rx recovery sccrq avp bad value receive window size	15	service unavailable
tunnel rx recovery sccrq avp bad value tunnel recovery	15	service unavailable
tunnel rx recovery sccrq avp duplicate value assigned tunnel id	15	service unavailable
tunnel rx recovery sccrq avp duplicate value tie breaker	15	service unavailable
tunnel rx recovery sccrq avp malformed bad length	15	service unavailable
tunnel rx recovery sccrq avp malformed truncated	15	service unavailable
tunnel rx recovery sccrq avp mismatched host name	15	service unavailable
tunnel rx recovery sccrq avp mismatched vendor name	15	service unavailable
tunnel rx recovery sccrq avp missing mandatory assigned tunnel id	15	service unavailable
tunnel rx recovery sccrq avp missing mandatory framing capabilities	15	service unavailable
tunnel rx recovery sccrq avp missing mandatory host name	15	service unavailable
tunnel rx recovery sccrq avp missing mandatory protocol version	15	service unavailable
tunnel rx recovery sccrq avp missing mandatory tunnel recovery	15	service unavailable
tunnel rx recovery sccrq avp missing random vector	15	service unavailable
tunnel rx recovery sccrq avp missing secret	15	service unavailable
tunnel rx recovery sccrq avp missing tie breaker	15	service unavailable
tunnel rx recovery sccrq avp unexpected challenge without secret	15	service unavailable
tunnel rx recovery sccrq avp unknown	15	service unavailable

Table 30: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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
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

Table 30: Default L2TP Mappings (*continued*)

L2TP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
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**
- [Mapping Application Terminate Reasons and RADIUS Terminate Codes on page 151](#)
 - [Configuring Custom Terminate Reason Mappings on page 153](#)

PPP Terminate Reasons

Table 31 on page 172 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 31: Default PPP Mappings

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
admin logout	10	NAS request
authenticate authenticator timeout	17	user error
authenticate challenge timeout	10	NAS request
authenticate chap no resources	10	NAS request
authenticate chap peer authenticator timeout	17	user error
authenticate deny by peer	17	user error
authenticate inactivity timeout	4	idle timeout
authenticate max requests	10	NAS request
authenticate no authenticator	10	NAS request

Table 31: Default PPP Mappings (*continued*)

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
authenticate pap peer authenticator timeout	17	user error
authenticate pap request timeout	10	NAS request
authenticate session timeout	5	session timeout
authenticate too many requests	10	NAS request
authenticate tunnel fail immediate	10	NAS request
authenticate tunnel unsupported tunnel type	10	NAS request
bundle fail create	10	NAS request
bundle fail engine add	10	NAS request
bundle fail fragment size mismatch	10	NAS request
bundle fail fragmentation location	10	NAS request
bundle fail fragmentation mismatch	10	NAS request
bundle fail join	10	NAS request
bundle fail link selection mismatch	10	NAS request
bundle fail local mped not set yet	10	NAS request
bundle fail local mrru mismatch	10	NAS request
bundle fail local mru mismatch	10	NAS request
bundle fail peer mrru mismatch	10	NAS request
bundle fail reassembly location	10	NAS request
bundle fail reassembly mismatch	10	NAS request
bundle fail record network	10	NAS request
bundle fail server location mismatch	10	NAS request
bundle fail static link	10	NAS request
failover during authentication	6	admin reset

Table 31: Default PPP Mappings (*continued*)

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
interface admin disable	6	admin reset
interface down	2	lost carrier
interface no hardware	8	port error
ip admin disable	10	NAS request
ip inhibited by authentication	10	NAS request
ip link down	10	NAS request
ip max configure exceeded	10	NAS request
ip no local ip address	10	NAS request
ip no local ip address mask	10	NAS request
ip no local primary dns address	10	NAS request
ip no local primary nbns address	10	NAS request
ip no local secondary dns address	10	NAS request
ip no local secondary nbns address	10	NAS request
ip no peer ip address	10	NAS request
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

Table 31: Default PPP Mappings (*continued*)

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
ip peer renegotiate rx conf req	10	NAS request
ip peer terminate term ack	10	NAS request
ip peer terminate code rej	10	NAS request
ip peer terminate term req	10	NAS request
ip service disable	10	NAS request
ip stale stacking	10	NAS request
ipv6 admin disable	10	NAS request
ipv6 inhibited by authentication	10	NAS request
ipv6 link down	10	NAS request
ipv6 local and peer interface ids identical	10	NAS request
ipv6 max configure exceeded	10	NAS request
ipv6 no local ipv6 interface id	10	NAS request
ipv6 no peer ipv6 interface id	10	NAS request
ipv6 no service	10	NAS request
ipv6 peer renegotiate rx conf ack	10	NAS request
ipv6 peer renegotiate rx conf nak	10	NAS request
ipv6 peer renegotiate rx conf rej	10	NAS request
ipv6 peer renegotiate rx conf req	10	NAS request
ipv6 peer terminate code rej	10	NAS request
ipv6 peer terminate term ack	10	NAS request
ipv6 peer terminate term req	10	NAS request
ipv6 service disable	10	NAS request
ipv6 stale stacking	10	NAS request

Table 31: Default PPP Mappings (*continued*)

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
lcp authenticate terminate hold	10	NAS request
lcp configured mrru too small	10	NAS request
lcp configured mru invalid	10	NAS request
lcp configured mru too small	10	NAS request
lcp dynamic interface hold	10	NAS request
lcp keepalive failure	10	NAS request
lcp loopback rx conf req	10	NAS request
lcp loopback rx echo reply	10	NAS request
lcp loopback rx echo req	10	NAS request
lcp max configure exceeded	10	NAS request
lcp mru changed	10	NAS request
lcp negotiation timeout	10	NAS request
lcp no localacm	10	NAS request
lcp no localacfc	10	NAS request
lcp no local authentication	10	NAS request
lcp no local endpoint discriminator	10	NAS request
lcp no local magic number	10	NAS request
lcp no local mrru	10	NAS request
lcp no local mru	10	NAS request
lcp no localpfc	10	NAS request
lcp no peer accm	10	NAS request
lcp no peer authentication	10	NAS request
lcp no peer endpoint discriminator	10	NAS request

Table 31: Default PPP Mappings (*continued*)

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
lcp no peer magicnumber	10	NAS request
lcp no peer mrru	10	NAS request
lcp no peer mru	10	NAS request
lcp no peer pfc	10	NAS request
lcp peer terminate code rej	1	user request
lcp peer terminate term ack	1	user request
lcp peer terminate term req	1	user request
lcp peer terminate protocol reject	1	user request
lcp peer renegotiate rx conf ack	1	user request
lcp peer renegotiate rx conf nak	1	user request
lcp peer renegotiate rx conf rej	1	user request
lcp peer renegotiate rx conf req	1	user request
lcp tunnel disconnected	10	NAS request
lcp tunnel failed	10	NAS request
link interface no hardware	8	port error
lower interface attach failed	2	lost carrier
lower interface teardown	2	lost carrier
mpls admin disable	10	NAS request
mpls link down	10	NAS request
mpls max configure exceeded	10	NAS request
mpls no service	10	NAS request
mpls peer renegotiate rx conf ack	10	NAS request
mpls peer renegotiate rx conf nak	10	NAS request

Table 31: Default PPP Mappings (*continued*)

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
mpls peer renegotiate rx conf rej	10	NAS request
mpls peer renegotiate rx conf req	10	NAS request
mpls peer terminate code rej	10	NAS request
mpls peer terminate term ack	10	NAS request
mpls peer terminate term req	10	NAS request
mpls service disable	10	NAS request
mpls stale stacking	10	NAS request
network interface admin disable	6	admin reset
no bundle	10	NAS request
no interface	8	port error
no link interface	8	port error
no ncps available	10	NAS request
no network interface	10	NAS request
no upper interface	9	NAS error
osi admin disable	10	NAS request
osi link down	10	NAS request
osi max configure exceeded	10	NAS request
osi no local align npdu	10	NAS request
osi no peer align npdu	10	NAS request
osi no service	10	NAS request
osi peer renegotiate rx conf ack	10	NAS request
osi peer renegotiate rx conf nak	10	NAS request
osi peer renegotiate rx conf rej	10	NAS request

Table 31: Default PPP Mappings (*continued*)

PPP Terminate Reason	RADIUS Acct-Terminate-Cause	
	Code	Description
osi peer renegotiate rx conf req	10	NAS request
osi peer terminate code rej	10	NAS request
osi peer terminate term ack	10	NAS request
osi peer terminate term req	10	NAS request
osi service disable	10	NAS request
osi stale stacking	10	NAS request
recovery active state cleanup	9	NAS error
recovery configured state cleanup	9	NAS error
recovery init state cleanup	9	NAS error
recovery terminated state cleanup	9	NAS error
recovery terminating state cleanup	9	NAS error
session init failed	9	NAS error
subscriber mgr activation failed	9	NAS error
subscriber mgr get credentials failed	9	NAS error
subscriber mgr link interface not found	9	NAS error
subscriber mgr set state active failed	9	NAS error

**Related
Documentation**

- [Mapping Application Terminate Reasons and RADIUS Terminate Codes on page 151](#)
- [Configuring Custom Terminate Reason Mappings on page 153](#)

Monitoring and Managing AAA Information for Subscriber Access

- [Verifying and Managing Subscriber AAA Information on page 181](#)
- [Monitoring Pending RADIUS Accounting Stop Messages on page 182](#)
- [Verifying and Managing the RADIUS Dynamic-Request Feature on page 183](#)
- [Verifying and Managing Domain Map Configuration on page 183](#)
- [Verifying and Managing LLID Preauthentication Configuration on page 184](#)

Verifying and Managing Subscriber AAA Information

Purpose View or clear subscriber access statistics and information.

- Action**
- To display subscriber AAA statistics:
user@host> [show network-access aaa statistics](#)
user@host> [show network-access aaa statistics authentication](#)
 - To display RADIUS server status and information:
user@host> [show network-access aaa radius-servers](#)
 - To display subscriber access AAA information:
user@host> [show network-access aaa subscribers](#)
 - To display subscriber session information:
user@host> [show network-access aaa subscribers session-id session-id](#)
 - To clear subscriber access statistics and to log out specific subscribers:
user@host> [clear network-access aaa subscriber](#)
 - To clear AAA accounting statistics:
user@host> [clear network-access aaa statistics accounting](#)
 - To clear AAA address-assignment statistics for a client:
user@host> [clear network-access aaa statistics address-assignment client](#)
 - To clear AAA address-assignment pool statistics:
user@host> [clear network-access aaa statistics address-assignment pool pool-name](#)

- To clear AAA authentication statistics:

```
user@host> clear network-access aaa statistics authentication
```

Related Documentation

- [CLI Explorer](#)

Monitoring Pending RADIUS Accounting Stop Messages

Purpose Display information about RADIUS accounting stop messages that are being withheld due to an inability to contact the RADIUS accounting server.

Action When you want to know whether the number of pending accounting-stop messages is nearing the maximum, you can display a simple count of pending requests:

```
user@host> show network-access aaa statistics pending-accounting-stops
Pending accounting stops: 10,000
```

You can use other commands to display more information about the accounting messages. The next example displays information for all services in the accounting session for the user, `vjshah29@example.com`. Although this example shows only one user, this command actually displays the information for all subscribers for whom accounting is being backed up.

```
user@host> show accounting pending-accounting-stops detail
Type: pppoe
Username: vjshah29@example.com
AAA Logical system/Routing instance: default:default
Access-profile: ce-ppp-profile
Session ID: 84
Accounting Session ID: 84
IP Address: 192.168.0.25
IPv6 Prefix: 2010:9999:18::/48
Authentication State: AuthAcctStopAckWait
Accounting State: Acc-Stop-Stats-Pending
Service name: cos-service
  Service State: SvcInactive
  Session ID: 94
  Session uptime: 00:08:02
  Accounting status: on/time
  Service accounting session ID: 84:94-1352294677
  Service accounting state: Acc-Stop-Stats-Pending
  Accounting interim interval: 600
Service name: filter-service
  Service State: SvcInactive
  Session ID: 93
  Session uptime: 00:08:02
  Accounting status: on/volume+time
  Service accounting session ID: 84:93-1352294677
  Service accounting state: Acc-Stop-Stats-Pending
  Accounting interim interval: 600
Service name: filter-service6
  Service State: SvcInactive
  Session ID: 95
  Session uptime: 00:08:02
  Accounting status: on/volume+time
  Service accounting session ID: 84:95-1352294677
```

```
Service accounting state: Acc-Stop-Stats-Pending
Accounting interim interval: 600
```

You can display summary information for all users with a particular access profile. In the following example, only a single user, `vjshah29@example.com`, has the specified access profile, `ce-ppp-profile`:

```
user@host> show accounting pending-accounting-stops ce-ppp-profile
```

Type:	Username:	Session ID:	Service ID:	Service
pppoe	vjshah29@example.com	84		
pppoe	vjshah29@example.com	84	94	cos-service
pppoe	vjshah29@example.com	84	93	filter-service
pppoe	vjshah29@example.com	84	95	filter-service6

You can also display summary information for all subscribers that have accounting-stop messages pending, regardless of access profile. The next example displays information for two users. Because the subscriber `larry@example.com` is not shown in the previous example, he must have a different access profile than `vjshah29@example.com`, even though he has received the same services.

```
user@host> show accounting pending-accounting-stops terse
```

Type:	Username:	Session ID:	Service ID:	Service
pppoe	vjshah29@example.com	84		
pppoe	vjshah29@example.com	84	94	cos-service
pppoe	vjshah29@example.com	84	93	filter-service
pppoe	vjshah29@example.com	84	95	filter-service6
pppoe	larry@example.com	85		
pppoe	larry@example.com	85	94	cos-service
pppoe	larry@example.com	85	93	filter-service
pppoe	larry@example.com	85	95	filter-service6

- Related Documentation**
- [Preservation of RADIUS Accounting Information During an Accounting Server Outage on page 88](#)
 - [Configuring Back-up Options for RADIUS Accounting on page 97](#)

Verifying and Managing the RADIUS Dynamic-Request Feature

Purpose Display RADIUS dynamic request statistics and information.

Action • To display RADIUS dynamic request statistics:

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

- Related Documentation**
- [CLI Explorer](#)

Verifying and Managing Domain Map Configuration

Purpose Display information related to a domain map.

Action • To display statistics for the domain map:

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

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

user@host> [show network-access aaa subscribers session-id](#)

**Related
Documentation**

- [Domain Mapping Overview on page 128](#)
- [Configuring a Domain Map on page 131](#)

Verifying and Managing LLID Preauthentication Configuration

Purpose Display statistics and configuration information related to logical line identification (LLID) preauthentication.

Action

- To display LLID preauthentication statistics:
user@host> [show network-access aaa statistics preauthentication](#)
- To display information about preauthentication servers:
user@host> [show network-access aaa radius-servers](#)

**Related
Documentation**

- [RADIUS Logical Line Identifier \(LLID\) Overview on page 121](#)
- [Configuring Logical Line Identification \(LLID\) Preauthentication on page 124](#)

PART 2

Configuring DHCP for Subscriber Management

- [Using DHCP Overview on page 187](#)
- [Configuring Default Services That are Activated at Subscriber Login on page 199](#)
- [Assigning IP Addresses on page 201](#)
- [Configuring Lease Times for IP Addresses on page 209](#)
- [Requesting DHCP Client Configuration Information From an Address Pool on page 213](#)
- [Authenticating DHCP Clients Using An External AAA Authentication Service on page 217](#)
- [Grouping Interfaces and Applying a Common DHCP Configuration to the Group on page 223](#)
- [Configuring the Number of DHCP Clients Per Interface on page 233](#)
- [Maintaining Subscribers During Interface Delete Events on page 237](#)
- [Forcing Dynamic Reconfiguration of Clients From a DHCP Local Server on page 241](#)
- [Conserving IP Addresses Using DHCP Auto Logout on page 249](#)
- [Overriding Default DHCP Local Server Configuration Settings on page 255](#)
- [Applying a Common DHCP Relay Agent Configuration to Groups of DHCP Servers on page 259](#)
- [Changing the Gateway IP Address \(giaddr\) Field and DHCP Relay Request and Release Packet Source Address on page 261](#)
- [Configuring DHCP Relay Agent on page 263](#)
- [Configuring DHCP Relay Proxy Mode on page 281](#)
- [Configuring DHCP Local Server Authentication on page 283](#)
- [Configuring a Minimum DHCP Local Server Configuration on page 285](#)
- [Configuring DHCPv6 Local Server on page 287](#)
- [Configuring DHCPv6 Relay Agent on page 295](#)
- [Protecting the Routing Engine Using DHCP Firewall Filters on page 301](#)
- [Monitoring and Managing DHCP on page 307](#)

CHAPTER 15

Using DHCP Overview

- [Extended DHCP Local Server Overview on page 188](#)
- [Extended DHCP Relay Agent Overview on page 194](#)
- [DHCP Relay Proxy Overview on page 197](#)

Extended DHCP Local Server Overview

Junos OS includes an extended DHCP local server that enhances traditional DHCP server operation by providing additional address assignment and client configuration functionality and flexibility in a subscriber-aware environment. The extended DHCP local server enables service providers to take advantage of external address-assignment pools and integrated RADIUS-based configuration capabilities in addition to the continued support of traditional local address pools. The address-assignment pools are considered external because they are external to the DHCP local server. The pools are managed independently of the DHCP local server, and can be shared by different client applications, such as DHCP or PPPoE access. [Table 32 on page 189](#) provides a comparison of the extended DHCP local server and a traditional DHCP local server.

The extended DHCP local server provides an IP address and other configuration information in response to a client request. The server supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide DHCP client authentication. You can configure the dynamic profile and authentication support on a global basis or for a specific group of interfaces.

Table 32: Comparing the Extended DHCP Local Server to the Traditional DHCP Local Server

Feature	Extended DHCP Local Server	Traditional DHCP Local Server
Local address pools	X	X
External, centrally-managed address pools	X	—
Local configuration	X	X
External configuration using information from address-assignment pools or RADIUS servers	X	—
Dynamic-profile attachment	X	—
RADIUS-based subscriber authentication, and configuration using RADIUS attributes and Juniper Networks VSAs	X	—
IPv6 client support	X	—
Default minimum client configuration	X	X

You can also configure the extended DHCP local server to support IPv6 clients. Both DHCP local server and DHCPv6 local server support the specific address request feature, which enables you to assign a particular address to a client.



NOTE: If you delete the DHCP server configuration, DHCP server bindings might still remain. To ensure that DHCP bindings are removed, issue the `clear dhcp server binding` command before you delete the DHCP server configuration.

This overview covers:

- [Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools on page 190](#)
- [Providing DHCP Client Configuration Information on page 190](#)
- [Minimal Configuration for Clients on page 192](#)
- [DHCP Local Server and Address-Assignment Pools on page 192](#)

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

The pattern of interaction between the DHCP local server, the DHCP client, and address-assignment pools is the same regardless of whether you are using a router or a switch. However, there are some differences in the details of usage.

- On routers—In a typical carrier edge network configuration, the DHCP client is on the subscriber's computer or customer premises equipment (CPE), and the DHCP local server is configured on the router.
- On switches—In a typical network configuration, the DHCP client is on an access device, such as a personal computer, and the DHCP local server is configured on the switch.

The following steps provide a high-level description of the interaction among the DHCP local server, DHCP client, and address-assignment pools:

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

Providing DHCP Client Configuration Information

When the extended DHCP application receives a response from an external authentication server, the response might include information in addition to the IP address and subnet

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

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

When you use RADIUS to provide the authentication, the additional information might be in the form of RADIUS attributes and Juniper Networks VSAs. [Table 33 on page 191](#) lists the information that RADIUS might include in the authentication grant. See [“RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework” on page 13](#) for a complete list of RADIUS attributes and Juniper Networks VSAs that the extended DHCP applications supports for subscriber access management or DHCP management.

Table 33: Information in Authentication Grant

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

Minimal Configuration for Clients

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

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

DHCP Local Server and Address-Assignment Pools

In the traditional DHCP server operation, the client address pool and client configuration information reside on the DHCP server. With the extended DHCP local server, the client address and configuration information reside in external address-assignment pools (external to the DHCP local server). The external address-assignment pools are managed by the **authd** process, independently of the DHCP local server, and can be shared by different client applications.

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

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



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

Related Documentation

- [Address-Assignment Pools Overview on page 315](#)

- [Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 203](#)
- *Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview*
- [Using External AAA Authentication Services with DHCP on page 217](#)
- [Assign a Specific IP Address to a Client Using DHCP Option 50 and DHCPv6 IA_NA Option on page 204](#)
- *Graceful Routing Engine Switchover for DHCP*
- *High Availability Using Unified ISSU in the PPP Access Network*
- [Tracing Extended DHCP Operations on page 521](#)
- [Verifying and Managing DHCP Local Server Configuration on page 311](#)
- [Example: Minimum Extended DHCP Local Server Configuration on page 285](#)
- [Example: Extended DHCP Local Server Configuration with Optional Pool Matching on page 206](#)
- [Example: Configuring a DHCP Firewall Filter to Protect the Routing Engine on page 301](#)

Extended DHCP Relay Agent Overview

You can configure extended DHCP relay options on the router or on the switch and enable the router (or switch) to function as a DHCP relay agent. A DHCP relay agent forwards DHCP request and reply packets between a DHCP client and a DHCP server.

DHCP relay supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide subscriber authentication or DHCP client authentication. You can attach dynamic profiles and configure authentication support on a global basis or for a specific group of interfaces.



NOTE: The PTX Series Packet Transport Routers do not support authentication for DHCP relay agents.

On the routers, you can use DHCP relay in carrier edge applications such as video/IPTV to obtain configuration parameters, including an IP address, for your subscribers. For information about how to use the DHCP relay agent in a video/IPTV application, see *Broadband Subscriber Management Edge Router Overview*.

On the switches, you can use DHCP relay to obtain configuration parameters including an IP address for DHCP clients.



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

For information about the DHCP/BOOTP relay agent, see *Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents*.

You can also configure the extended DHCP relay agent to support IPv6 clients. See *DHCPv6 Relay Agent Overview* for information about the DHCPv6 relay agent feature.

To configure the extended DHCP relay agent on the router (or switch), include the `dhcp-relay` statement at the `[edit forwarding-options]` hierarchy level. See the “[[edit forwarding-options dhcp-relay](#)] Hierarchy Level” on page 612 for the complete DHCP relay agent syntax.

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

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

This overview covers:

- [Interaction Among the DHCP Relay Agent, DHCP Client, and DHCP Servers on page 195](#)
- [DHCP Liveness Detection on page 196](#)

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

The pattern of interaction among the DHCP Relay agent, DHCP client, and DHCP servers is the same regardless of whether the software installation is on a router or a switch. However, there are some difference in the details of usage.

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

On switches—In a typical network configuration, the DHCP client is on an access device such as a personal computer and the DHCP relay agent is configured on the switch between the DHCP client and one or more DHCP servers.

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

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

agent “snoops” on all of the packets unicast between the client and the server that pass through the router (or switch) to determine when the lease for this client has expired or been released. This process is referred to as *lease shadowing* or *passive snooping*.

DHCP Liveness Detection

Liveness detection for DHCP subscriber or DHCP client IP sessions utilizes an active liveness detection protocol to institute liveness detection checks for relevant clients. Clients are expected to respond to liveness detection requests within a specified amount of time. If the responses are not received within that time for a given number of consecutive attempts, then the liveness detection check fails and a failure action is implemented.



NOTE: DHCP liveness detection either globally or per DHCP group.

Related Documentation

- [DHCPv6 Relay Agent Overview](#)
- [Access and Access-Internal Routes for Subscriber Management](#)
- [Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview](#)
- [Using External AAA Authentication Services with DHCP on page 217](#)
- [DHCP Relay Proxy Overview on page 197](#)
- [Graceful Routing Engine Switchover for DHCP](#)
- [High Availability Using Unified ISSU in the PPP Access Network](#)
- [Verifying and Managing DHCP Relay Configuration on page 312](#)
- [Tracing Extended DHCP Operations on page 521](#)
- [Example: Minimum DHCP Relay Agent Configuration on page 274](#)
- [Example: DHCP Relay Agent Configuration with Multiple Clients and Servers on page 279](#)
- [Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings on page 275](#)
- [Example: Configuring DHCP and DHCPv6 Relay Agent Group-Level Selective Traffic Processing on page 227](#)
- [Example: Configuring a DHCP Firewall Filter to Protect the Routing Engine on page 301](#)

DHCP Relay Proxy Overview

DHCP relay proxy mode is an enhancement to extended DHCP relay. DHCP relay proxy supports all DHCP relay features while providing additional features and benefits.

Normally, extended DHCP relay operates as a helper application for DHCP operations. Except for the ability to add DHCP relay agent options and the gateway address (giaddr) to DHCP packets, DHCP relay is transparent to DHCP clients and DHCP servers, and simply forwards messages between DHCP clients and servers.

When you configure DHCP relay to operate in proxy mode, the relay is no longer transparent. In proxy mode, DHCP relay conceals DHCP server details from DHCP clients, which interact with a DHCP relay in proxy mode as though it is the DHCP server. For DHCP servers there is no change, because proxy mode has no effect on how the DHCP server interacts with the DHCP relay.

DHCP relay proxy provides the following benefits:

- DHCP server isolation and DoS protection—DHCP clients are unable to detect the DHCP servers, learn DHCP server addresses, or determine the number of servers that are providing DHCP support. Server isolation also provides denial-of-service (DoS) protection for the DHCP servers.
- Multiple lease offer selection—DHCP relay proxy receives lease offers from multiple DHCP servers and selects a single offer to send to the DHCP client, thereby reducing traffic in the network. Currently, the DHCP relay proxy selects the first offer received.
- Support for both numbered and unnumbered Ethernet interfaces—For DHCP clients connected through Ethernet interfaces, when the DHCP client obtains an address, the DHCP relay proxy adds an access internal host route specifying that interface as the outbound interface. The route is automatically removed when the lease time expires or when the client releases the address.
- Logical system support—DHCP relay proxy can be configured in a logical system, whereas a non-proxy mode DHCP relay cannot.



NOTE: You cannot configure both DHCP relay proxy and extended DHCP local server on the same interface.

Interaction Among DHCP Relay Proxy, DHCP Client, and DHCP Servers

The DHCP relay agent is configured on the router (or switch), which operates between the DHCP client and one or more DHCP servers.

The following steps provide a high-level description of how DHCP relay proxy interacts with DHCP clients and DHCP servers.

1. The DHCP client sends a discover packet to locate a DHCP server in the network from which to obtain configuration parameters for the subscriber.
2. The DHCP relay proxy receives the discover packet from the DHCP client and forwards copies of the packet to each supporting DHCP server. The DHCP relay proxy then creates a client table entry to keep track of the client state.
3. In response to the discover packet, each DHCP server sends an offer packet to the client, which the DHCP relay proxy receives. The DHCP relay proxy does the following:
 - a. Selects the first offer received as the offer to sent to the client
 - b. Replaces the DHCP server address with the address of the DHCP relay proxy
 - c. Forwards the offer to the DHCP client.
4. The DHCP client receives the offer from the DHCP relay proxy.
5. The DHCP client sends a request packet that indicates the DHCP server from which to obtain configuration information—the request packet specifies the address of the DHCP relay proxy.
6. The DHCP relay proxy receives the request packet and forwards copies, which include the address of selected server, to all supporting DHCP servers.
7. The DHCP server requested by the client sends an acknowledgement (ACK) packet that contains the client configuration parameters.
8. The DHCP relay proxy receives the ACK packet, replaces the DHCP server address with its own address, and forwards the packet to the client.
9. The DHCP client receives the ACK packet and stores the configuration information.
10. If configured to do so, the DHCP relay proxy installs a host route and Address Resolution Protocol (ARP) entry for the DHCP client.
11. After the initial DHCP lease is established, the DHCP relay proxy receives all lease renewals and lease releases from the DHCP client and forwards them to the DHCP server.

**Related
Documentation**

- [Extended DHCP Relay Agent Overview on page 194](#)
- [Enabling DHCP Relay Proxy Mode on page 281](#)
- *Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity*

Configuring Default Services That are Activated at Subscriber Login

- [Default Subscriber Service Overview on page 199](#)
- [Configuring a Default Subscriber Service on page 200](#)

Default Subscriber Service Overview

Subscriber management enables you to specify a default subscriber service for DHCP subscribers. The default service (dynamic profile) is applied to subscribers when the subscriber logs in. By configuring a default service, you can apply a particular service (for example, a basic service) to subscribers who are not explicitly assigned a service.

When a subscriber logs in, the configured default service is always activated, even when remote service provisioning or RADIUS service activation is configured for the subscriber. The default service is deactivated only when the subscriber is successfully provisioned by the PCRF by means of the GX-Plus application. (Remote provisioning is configured by the **provisioning-order** statement at the **[edit access profile]** hierarchy level.)

In all other cases, the default service remains active. For example, if RADIUS authentication is configured but service activation is not, the default subscriber service remains activated. Likewise, if RADIUS authentication is not configured, the default subscriber service remains activated.

Default services can also be deactivated either with a RADIUS CoA deactivate request or with the **request network-access aaa subscriber delete session-id** command.

To create and assign a default subscriber service, you must complete the following operations:

- Create the service—Ensure that the service you want to use has been configured in a dynamic profile. The actual service is no different than any other service used for subscriber management.
- Specify the default service—Use the Junos OS CLI to specify the service that is used as the default service.
- Specify the interfaces on which the default service is assigned —Use the Junos OS CLI to specify that the default service is used globally, for a group of interfaces, or for a specific interface.

- Related Documentation**
- [Configuring a Default Subscriber Service on page 200](#)
 - [CLI-Activated Subscriber Services on page 331](#)
 - [Activating and Deactivating Subscriber Services Locally with the CLI on page 332](#)
 - [Understanding Gx-Plus Interactions Between the Router and the PCRF on page 441](#)

Configuring a Default Subscriber Service

Subscriber management enables you to specify a default subscriber service for DHCP (and DHCPv6) local server and DHCP relay agent. The default service is the service (dynamic profile) that is applied to subscribers when they log in.

Default services are subsequently deactivated in any of the following circumstances:

- A PCRF responds to AAA for the subscriber.
- A RADIUS CoA deactivation request is issued.
- You deactivate the service manually through the CLI.

To configure a default subscriber service:

1. Ensure that the service you want to use as the default has been configured in a dynamic profile.
2. Specify the default service.

The following example configures the default service for DHCP local server subscribers.

```
[edit system services dhcp-local-server]
user@host# set service-profile retailer1-subscriber
```

3. Attach the default service—you can attach the profile globally, for a group of interfaces, or for a specific interface.

The following example attaches the profile to a named group of interfaces for DHCP local server.

- Specify the group to which the default service is attached.

```
[edit system services dhcp-local-server]
user@host# set group subscriber-svl
```

- Specify the dynamic profile that defines the default service.

```
[edit system services dhcp-local-server group subscriber-svl]
user@host# set dynamic-profile retailer1-subscriber
```

- Related Documentation**
- [Default Subscriber Service Overview on page 199](#)
 - [Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces](#)

Assigning IP Addresses

- [DHCP Attributes for Address-Assignment Pools on page 201](#)
- [Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 203](#)
- [Assign a Specific IP Address to a Client Using DHCP Option 50 and DHCPv6 IA_NA Option on page 204](#)
- [Configuring DHCP Client-Specific Attributes Applied When Clients Obtain an Address on page 205](#)
- [Specifying the Subnet for DHCP Client Address Assignment on page 206](#)
- [Example: Extended DHCP Local Server Configuration with Optional Pool Matching on page 206](#)
- [DNS Address Assignment Precedence on page 207](#)

DHCP Attributes for Address-Assignment Pools

Table 34 on page 201 describes the DHCP client attributes that you can use with the **dhcp-attributes** statement when you configure address-assignment pools. Table 35 on page 202 describes the DHCPv6 client attributes for configuring IPv6 address-assignment pools.

Table 34: DHCP Attributes

Attribute	Description	DHCP Option
boot-file	Boot filename advertised to the client, and used by the client to complete configuration.	67
boot-server	Boot server containing the boot file.	66
domain-name	Domain in which clients search for a DHCP server host.	15
grace-period	Grace period offered with the lease.	—
maximum-lease-time	Maximum lease time allowed by the DHCP server.	51

Table 34: DHCP Attributes (*continued*)

Attribute	Description	DHCP Option
<code>name-server</code>	IP address of DNS server to which clients can send DNS queries.	6
<code>netbios-node-type</code>	NetBIOS node type.	46
<code>option</code>	User-defined options.	—
<code>option-match</code>	Option 82 value is mapped to named address range.	—
<code>router</code>	IP address for routers on the subnetwork.	3
<code>server-identifier</code>	IP address used as the DHCP source address	54
<code>tftp-server</code>	Trivial File Transfer Protocol (TFTP) server that the client uses to obtain the client configuration file.	150
<code>wins-server</code>	IP address of the Windows NetBIOS name server.	44

Table 35: DHCPv6 Attributes

Attribute	Description	DHCPv6 Option
<code>dns-server</code>	IPv6 address of DNS server to which clients can send DNS queries.	23
<code>grace-period</code>	Grace period offered with the lease.	—
<code>maximum-lease-time</code>	Maximum lease time allowed by the DHCP server.	—
<code>option</code>	User-defined options.	—
<code>preferred-lifetime</code>	Length of time that a valid address is in the preferred state. When the preferred lifetime expires, the address becomes deprecated.	—
<code>sip-server-address</code>	IPv6 address of SIP outbound proxy server.	22
<code>sip-server-domain-name</code>	Domain name of the SIP outbound proxy server.	21
<code>t1-percentage</code>	Percentage of the preferred-lifetime that the client (router) waits before sending renew messages to the DHCPv6 server that granted the original lease to extend the client's lease.	—
<code>t2-percentage</code>	Percentage of the preferred-lifetime that the client (router) waits before sending rebind messages to any available DHCPv6 server to extend the client's lease.	—

Table 35: DHCPv6 Attributes (*continued*)

Attribute	Description	DHCPv6 Option
<code>valid-lifetime</code>	Length of time that the address remains in the valid state. When the lifetime expires, the address becomes invalid.	—

Related Documentation

- [Address-Assignment Pools Overview on page 315](#)
- [Configuring Address-Assignment Pools on page 316](#)
- [Configuring DHCP Client-Specific Attributes Applied When Clients Obtain an Address on page 205](#)
- [dhcp-attributes \(Address-Assignment Pools\) on page 683](#)

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

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

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

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

For IPv4 address-assignment pools, you can optionally configure the extended DHCP local server to match the DHCP relay agent information option (option 82) in the client DHCP packets to a named range in the address-assignment pool used for the client. Named ranges are subsets within the overall address-assignment pool address range, which you can configure when you create the address-assignment pool.



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

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

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

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

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

- Configure the router (switch) to use an external addressing authority.

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

- Configure the router (switch) to use the ip-address-first method.

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

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

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

Related Documentation

- [Address-Assignment Pools Overview on page 315](#)
- [Configuring Address-Assignment Pools on page 316](#)
- [Extended DHCP Local Server Overview on page 188](#)
- [Example: Extended DHCP Local Server Configuration with Optional Pool Matching on page 206](#)

Assign a Specific IP Address to a Client Using DHCP Option 50 and DHCPv6 IA_NA Option

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

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



NOTE: Subscriber management (DHCP management) supports only one address for each of the DHCPv6 IA_NA or IA_PD address types. If the DHCPv6 client requests more than one address for a given type, the DHCPv6 local server uses only the first address and ignores the other addresses.

**Related
Documentation**

- [Extended DHCP Local Server Overview on page 188](#)
- [DHCPv6 Local Server Overview on page 287](#)

Configuring DHCP Client-Specific Attributes Applied When Clients Obtain an Address

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

You use the `dhcp-attributes` statement to configure DHCP client-specific attributes for address-assignment pools. “[DHCP Attributes for Address-Assignment Pools](#)” on page 201 describes the supported attributes you can configure for IPv4 and IPv6 address-assignment pools.

To configure address-assignment pool attributes for DHCP clients:

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

[edit access]

user@host# **edit** `address-assignment pool isp_1 family inet`

2. Configure optional DHCP client attributes.

[edit access address-assignment pool isp_1 family inet]

user@host# **set** `dhcp-attributes boot-server 192.168.200.100 grace-period 3600 maximum-lease-time 18000`



NOTE: The DNS name server addresses that are configurable as DHCP attributes can also be configured globally at the routing instance level and in access profiles. For more information, see *DNS Name Server Address Overview*.

**Related
Documentation**

- [Address-Assignment Pools Overview on page 315](#)
- [Configuring Address-Assignment Pools on page 316](#)
- [DHCP Attributes for Address-Assignment Pools on page 201](#)

Specifying the Subnet for DHCP Client Address Assignment

Subscriber management enables you to explicitly specify the subnet to which the DHCP local server matches the requested IP address. The server accepts and uses an active client's requested IP address for address assignment only when the requested address and the IP address of the DHCP server interface are in the same subnet. The server accepts and uses a passive client's requested IP address only when the requested address and the IP address of the relay interface are in the same subnet. The DHCPv6 local server supports the same process for DHCPv6 clients and addresses.

To specify the subnet used for client address assignment:

- For DHCP local server:

```
[edit system services dhcp-local-server]
user@host# set requested-ip-network-match 10
```

- For DHCPv6 local server:

```
[edit forwarding-options dhcp-local-server dhcpv6]
user@host# set requested-ip-network-match 30
```

Related Documentation

- [Extended DHCP Local Server Overview on page 188](#)
- [requested-ip-network-match on page 909](#)

Example: Extended DHCP Local Server Configuration with Optional Pool Matching

This example shows an extended DHCP local server configuration that includes optional IPv4 address-assignment pool matching and interface groups. For pool matching, this configuration specifies that the DHCP local server first check the response from an external authentication authority (for example, RADIUS) and use the Framed-IPv6-Pool attribute to determine the address-assignment pool to use for the client address. If no external authority match is found, the DHCP local server then uses ip-address-first matching together with the option 82 information to match the named address range for client IPv4 address assignment. The option 82 matching must also be included in the address-assignment pool configuration.

```
[edit system services]
dhcp-local-server {
  group group_one {
    interface fe-0/0/2.0;
    interface fe-0/0/2.1;
  }
  group group_two {
    interface fe-0/0/3.0;
    interface fe-0/0/3.1;
  }
  pool-match-order {
    external-authority
    ip-address-first;
    option-82;
  }
}
```

```
}
}
```



NOTE: The interface type in this topic is just an example. The fe- interface type is not supported by EX Series switches.

- Related Documentation**
- [Extended DHCP Local Server Overview on page 188](#)
 - [Address-Assignment Pools Overview on page 315](#)

DNS Address Assignment Precedence

Subscriber management supports three methods for assigning addresses to DHCP clients. When multiple methods are configured, the router uses the following precedence to determine which address to assign to the client.

1. Address defined on the RADIUS server by Internet Assigned Numbers Authority (IANA) vendor ID 4874 attributes 26-4 (Primary-DNS) and 26-5 (Secondary-DNS).
2. Address defined on the RADIUS server by IANA vendor ID 2636 attributes 26-31 (Primary-DNS) and 26-33 (Secondary-DNS).
3. Address defined in the local address pool on the router.

- Related Documentation**
- [Juniper Networks VSAs Supported by the AAA Service Framework on page 21](#)
 - [Address-Assignment Pools Overview on page 315](#)

Configuring Lease Times for IP Addresses

- [Configuring a DHCP Lease-Time Threshold on page 209](#)
- [DHCP Lease-Time Validation Overview on page 210](#)
- [DHCPv6 Lease Timers on page 212](#)

Configuring a DHCP Lease-Time Threshold

Subscriber management provides a lease-time validation feature that enables you to specify the minimum DHCP lease time allowed in your subscriber access environment. When you configure lease-time validation, you specify the lease-time threshold and the action the router performs when an offered lease time is less than the threshold (such as dropping the lease).

Lease-time validation ensures that leases that are offered by third-party DHCP servers or address assignment pools always meet the requirements of your network. For example, you want short leases to be rejected because they can result in excessive renewal traffic that can impact network performance.

You can configure lease-time validation on DHCPv4 and DHCPv6 local servers, and DHCPv4 and DHCPv6 relay agents, and for individual interfaces or interface groups. DHCP relay proxy also supports lease-time validation.

The following procedure describes the steps you use to configure lease-time validation. This example describes a configuration for DHCP relay agent. You use similar steps at the appropriate hierarchy levels for DHCP local server, DHCPv6 local server, and DHCPv6 relay agent.

To configure lease time validation for DHCP relay agent:

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

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

2. Specify that you want to configure the DHCP lease time validation feature.

```
[edit forwarding-options dhcp-relay]  
user@host# set lease-time-validation
```

3. Configure the threshold that specifies the minimum DHCP client lease time allowed in your network.

```
[edit forwarding-options dhcp-relay lease-time-validation]
user@host# set lease-time-threshold 3600
```

4. Configure the action the router takes when a lease time violation occurs.

```
[edit forwarding-options dhcp-relay lease-time-validation]
user@host# set violation-action drop
```



NOTE: DHCP relay agent and DHCP local server support different violation actions. See the [violation-action](#) statement for descriptions of the actions.

If you do not specify a violation action, DHCP binds the client using the third-party lease but marks the binding as lease-time violating.

5. (Optional) Configure how often you want the router to consolidate and log syslog warning messages.

```
[edit system processes dhcp-service]
user@host# set ltv-syslog-interval 3600
```

**Related
Documentation**

- [DHCP Lease-Time Validation Overview on page 210](#)
- [Extended DHCP Local Server Overview on page 188](#)
- [Extended DHCP Relay Agent Overview on page 194](#)

DHCP Lease-Time Validation Overview

In a subscriber access environment, a DHCP server obtains an address lease from either local configuration or from an external DHCP server, and assigns the lease to the DHCP client address.

Obtaining leases from external sources can present issues when the external source is owned or managed by a third party—the third party might configure the external source to provide address leases that are unsuitable for the subscriber access environment. For example, extremely short lease times can create unnecessary traffic that results in reduced performance in the network.

To avoid potential issues caused by short DHCP lease times, subscriber management provides a lease-time validation feature. Lease-time validation enables you to explicitly configure a threshold for the minimum lease time allowed in your subscriber access environment, and to specify a violation action (such as dropping the lease offer) the router takes when a short lease time is offered by a third party. You can specify the following violation actions:

- **drop**—(DHCPv4 and DHCPv6 relay agent) The third-party lease offer is dropped and the client binding fails.
- **override-lease**—(DHCPv4 and DHCPv6 local server) The third-party lease time is overridden by the specified threshold value.

- **strict**—(DHCPv4 and DHCPv6 local server) The third-party lease is ignored and the client binding fails.
- **no action**—If you do not specify a violation action, DHCP binds the client using the third-party lease but marks the binding as lease-time violating.

A lease-time violation can occur during the initial lease grant or during a rebinding or renewal operation. To reduce excessive and redundant log messages, the router consolidates lease-time violation reporting, as shown in [Table 36 on page 211](#).

Table 36: Lease-Time Violation Event Logging

Event	syslog	Extended DHCP Traceoptions
Initial lease-time violation for the specific DHCP server	warning	warning
Number of lease-time violations return to zero for the specific DHCP server	warning	warning
Status of lease-time violations caused by specific DHCP server, reported in the interval configured in ltv-syslog-interval command	warning	—
Violation action of drop occurred, or the DHCP packet was not generated	—	warning
Violation action of override-lease occurred (DHCP local server only)	—	warning
Lease-time violation	—	warning

Related Documentation

- [Configuring a DHCP Lease-Time Threshold on page 209](#)
- [Extended DHCP Local Server Overview on page 188](#)
- [DHCPv6 Local Server Overview on page 287](#)
- [Extended DHCP Relay Agent Overview on page 194](#)
- [DHCPv6 Relay Agent Overview](#)

DHCPv6 Lease Timers

Subscriber management supports configurable timers that you can use to manage the DHCPv6 address leases provided by address-assignment pools. In addition to the maximum-lease-time timer, which sets the maximum time for which the DHCPv6 server can grant a lease, you can use DHCP client-specific attributes to configure timers that govern the lifetimes of existing leases that have been obtained from an address-assignment pool.

The following list describes the configurable timers for DHCPv6 address-assignment pools:

- **preferred-lifetime**—Length of time that a valid address is in the preferred state and can be used without any restrictions. When the preferred-lifetime expires, the address becomes deprecated. A deprecated address should not be used for new communications, but might continue to be used for existing communications in certain cases.

If the valid-lifetime is also configured, the preferred-lifetime must be less than the valid-lifetime. The preferred-lifetime and the maximum-lease-time are mutually exclusive and cannot both be configured.

- **valid-lifetime**—Length of time that an address remains in the valid state, during which the address can be used for new or existing communications. When the valid-lifetime expires, the address becomes invalid, and can no longer be used.

If the preferred-lifetime is also configured, the valid-lifetime must be greater than the preferred-lifetime. The valid-lifetime and the maximum-lease-time are mutually exclusive and cannot both be configured.

- **t1 percentage**—Percentage of the **preferred-lifetime** that the client waits before contacting the DHCPv6 server that originally granted the lease to request that the address lease be extended. This timer is also called the renewal time.
- **t2 percentage**—Percentage of the **preferred-lifetime** that the client waits before sending a request to any available DHCPv6 server to extend the address lease. This timer is also called the rebind time.

Related Documentation

- [Configuring DHCP Client-Specific Attributes Applied When Clients Obtain an Address on page 205](#)
- [DHCP Attributes for Address-Assignment Pools on page 201](#)

Requesting DHCP Client Configuration Information From an Address Pool

- [DHCP Local Server Handling of Client Information Request Messages on page 213](#)
- [Enabling Processing of Client Information Requests on page 214](#)

DHCP Local Server Handling of Client Information Request Messages

DHCP clients that already have externally provided addresses may solicit further configuration information from a DHCP server by sending a DHCP information request that indicates what information is desired. By default, DHCP local server and DHCPv6 local server ignore any DHCP information requests that they receive. You can override this default behavior to enable processing of these messages.

If you enable processing of information requests, DHCP local server responds to the client with a DHCP acknowledgment message that includes the requested information—if it is available. DHCPv6 local server responds in the same manner but uses a DHCP reply message. No subscriber management or DHCP-management is applied as a result of the DHCP information request message.

By default, DHCP relay and DHCP relay proxy automatically forward DHCP information request messages without modification if the messages are received on an interface configured for a DHCP server group. DHCP relay and relay proxy drop information request messages received on any other interfaces. You cannot disable this default DHCP relay and relay proxy behavior.

The information requested by these clients has typically been configured with the **dhcp-attributes** statement for an address pool defined by the **address-assignment pool** *pool-name* statement at the **[edit access]** hierarchy level.

When you enable processing of DHCP information requests, you can optionally specify the name of the pool from which the local server retrieves the requested configuration information for the client. If you do not specify a local pool, then the local server requests that AAA selects and returns only the name of the relevant pool.



NOTE: PPP interfaces are not supported on EX Series switches.

When DHCPv6 is configured over PPP interfaces, the PPP RADIUS authentication data can be used to select the pool from which the response information is taken. Additionally other RADIUS attributes can also be inserted into the DHCPv6 reply message. If an overlap exists between RADIUS attributes and local pool attributes, the RADIUS values are used instead of the local configuration data. If no RADIUS information is received from the underlying PPP interface, then the behavior is the same as described previously for non-PPP interfaces.

**Related
Documentation**

- [Overriding Default DHCP Local Server Configuration Settings on page 255](#)
- [Enabling Processing of Client Information Requests on page 214](#)

Enabling Processing of Client Information Requests

By default, DHCP local server and DHCPv6 local server do not respond to information request messages from the client. You can enable DHCP local server and DHCPv6 local server to process these messages and respond to them with an acknowledgment (ack or reply message, respectively) and the requested information.

DHCP relay agent automatically forwards the information request messages without modification to the configured server group by means of the interfaces configured for the respective server group. The messages are dropped if they are received on an unconfigured interface. DHCP relay proxy also supports forwarding these messages. You cannot disable forwarding of the information request messages.

Configure one or more local address pools if you want to use a local pool rather than one provided by AAA. See [“Configuring an Address-Assignment Pool Name and Addresses” on page 318](#). For processing information request messages, the address configuration is not necessary. For DHCP local server, you must specify the IPv4 family; for DHCPv6 local server, you must specify the IPv6 family.

See [“Configuring DHCP Client-Specific Attributes Applied When Clients Obtain an Address” on page 205](#) for details about how to configure the information sought by clients that send information request messages.

To enable processing of DHCP client information request messages:

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

```
[edit system services dhcp-local-server overrides]
user@host# set process-inform
```
 - For DHCPv6 local server:

```
[edit system services dhcp-local-server dhcpv6 overrides]
user@host# set process-inform
```
2. (Optional) Specify a pool name from which DHCP information is returned to the client.
 - For DHCP local server:

```
[edit system services dhcp-local-server overrides process-inform]
user@host# set pool pool-name
```

- For DHCPv6 local server:

```
[edit system services dhcp-local-server dhcpv6 overrides process-inform]  
user@host# set pool pool-name
```

**Related
Documentation**

- [Overriding Default DHCP Local Server Configuration Settings on page 255](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 258](#)
- [Extended DHCP Local Server Overview on page 188](#)
- [Extended DHCP Relay Agent Overview on page 194](#)

Authenticating DHCP Clients Using An External AAA Authentication Service

- Using External AAA Authentication Services with DHCP on page 217
- Creating Unique Usernames for DHCP Clients on page 218
- Configuring Passwords for Usernames on page 221

Using External AAA Authentication Services with DHCP

The extended DHCP local server, including DHCPv6 local server, and the extended DHCP relay agent, including DHCPv6 relay agent, support the use of external AAA authentication services, such as RADIUS, to authenticate DHCP clients. When the extended DHCP local server or relay agent receives a discover PDU from a client, the extended DHCP application contacts the AAA server to authenticate the DHCP client. The extended DHCP application can obtain client addresses and DHCP configuration options from the external AAA authentication server.



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

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

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

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

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

1. Specify that you want to configure authentication options.

- For DHCP local server:

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

- For DHCP relay agent:

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

- For DHCPv6 local server:

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

- For DHCPv6 relay agent:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit authentication
```

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

See [“Configuring Passwords for Usernames” on page 221](#).

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

See [“Creating Unique Usernames for DHCP Clients” on page 218](#).

Related Documentation

- [Extended DHCP Local Server Overview on page 188](#)
- [Extended DHCP Relay Agent Overview on page 194](#)
- [DHCPv6 Local Server Overview on page 287](#)
- [DHCPv6 Relay Agent Overview](#)

Creating Unique Usernames for DHCP Clients

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



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

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

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

- **circuit-type**—The circuit type used by the DHCP client, for example **enet**.
- **client-id**—The client identifier option (option 1). (DHCPv6 local server DHCPv6 relay agent only)
- **delimiter**—The delimiter character that separates components that make up the concatenated username. The default delimiter is a period (.). The semicolon (;) is not supported as a delimiter character.
- **domain-name**—The client domain name as a string. The router adds the @ delimiter to the username.
- **interface-name**—The interface name, including the interface device and associated VLAN IDs.
- **logical-system-name**—The name of the logical system, if the receiving interface is in a logical system.
- **mac-address**—The client MAC address, in a string of the format *xxxx.xxxx.xxxx*. (Not supported for DHCPv6 local server)
- **option-60**—The portion of the option 60 payload that follows the length field. (Not supported for DHCPv6 local server)
- **option-82 <circuit-id> <remote-id>**—The specified contents of the option 82 payload. (Not supported for DHCPv6 local server)
 - **circuit-id**—The payload of the Agent Circuit ID suboption.
 - **remote-id**—The payload of the Agent Remote ID suboption.
 - Both **circuit-id** and **remote-id**—The payloads of both suboptions, in the format: **circuit-id[delimiter]remote-id**.
 - Neither **circuit-id** or **remote-id**—The raw payload of the option 82 from the PDU is concatenated to the username.



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

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

- **routing-instance-name**—The name of the routing instance, if the receiving interface is in a routing instance.
- **user-prefix**—A string indicating the user prefix.

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

For DHCP local server and DHCP relay agent:

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

For DHCPv6 local server:

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

To configure a unique username:

1. Specify that you want to configure authentication.

- For DHCP local server:

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

- For DHCPv6 local server:

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

- For DHCP relay agent:

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

2. Specify that you want to include optional information in the username. (DHCP local server, DHCPv6 local server, and DHCP relay agent all support the **username-include** statement.)

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

3. (Optional) Specify the optional information you want to include in the username.

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

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

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

**Related
Documentation**

- [Extended DHCP Local Server Overview on page 188](#)
- [DHCPv6 Local Server Overview on page 287](#)

- [Extended DHCP Relay Agent Overview on page 194](#)
- [Using External AAA Authentication Services with DHCP on page 217](#)

Configuring Passwords for Usernames

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

To configure a password that authenticates the username:

1. Specify that you want to configure authentication options.

- For DHCP local server:

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

- For DHCPv6 local server:

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

- For DHCP relay agent:

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

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

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

Related Documentation

- [Extended DHCP Local Server Overview on page 188](#)
- [DHCPv6 Local Server Overview on page 287](#)
- [Extended DHCP Relay Agent Overview on page 194](#)
- [Using External AAA Authentication Services with DHCP on page 217](#)
- [*Special Requirements for Junos OS Plain-Text Passwords*](#)

CHAPTER 21

Grouping Interfaces and Applying a Common DHCP Configuration to the Group

- [Grouping Interfaces with Common DHCP Configurations on page 223](#)
- [Guidelines for Configuring Interface Ranges for Groups of DHCP Interfaces on page 224](#)
- [Configuring Group-Specific DHCP Local Server Options on page 225](#)
- [Configuring Group-Specific DHCP Relay Options on page 226](#)
- [Example: Configuring DHCP and DHCPv6 Relay Agent Group-Level Selective Traffic Processing on page 227](#)

Grouping Interfaces with Common DHCP Configurations

You use the group feature to group a set of interfaces and then apply a common DHCP configuration to the named interface group. The extended DHCP local server, DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent all support interface groups.

The following steps create a DHCP local server group; the steps are similar for the DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent.

To configure a DHCP local server interface group:

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

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

2. Create the group and assign a name.

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

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

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

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

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

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

```
[edit system services dhcp-local-server group boston]
user@host# set interface fe-1/0/1.1 upto fe-1/0/1.102
user@host# set interface fe-1/0/1.6 exclude
user@host# set interface fe-1/0/1.70 upto fe-1/0/1.80 exclude
```

**Related
Documentation**

- [Extended DHCP Local Server Overview on page 188](#)
- [Extended DHCP Relay Agent Overview on page 194](#)
- [DHCPv6 Local Server Overview on page 287](#)
- [DHCPv6 Relay Agent Overview](#)
- [Configuring Group-Specific DHCP Local Server Options on page 225](#)
- [Configuring Group-Specific DHCP Relay Options on page 226](#)
- [Guidelines for Configuring Interface Ranges for Groups of DHCP Interfaces on page 224](#)

Guidelines for Configuring Interface Ranges for Groups of DHCP Interfaces

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

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

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

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

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

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

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

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

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

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

In the following example, the three ranges nest properly:

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

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

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

Related Documentation

- [Grouping Interfaces with Common DHCP Configurations on page 223](#)

Configuring Group-Specific DHCP Local Server Options

You can include the following statements at the **[edit system services dhcp-local-server group group-name]** hierarchy level to set group-specific DHCP local server configuration options. Statements configured at the **[edit system services dhcp-local-server group group-name]** hierarchy level apply only to the named group of interfaces, and override any global DHCP local server settings configured with the same statements at the **[edit system services dhcp-local-server]** hierarchy level.

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

- **authentication**—Configure the parameters the router sends to the external AAA server.
- **dynamic-profile**—Specify the dynamic profile that is attached to a group of interfaces.

- **interface**—Specify one or more interfaces, or a range of interfaces, that are within the specified group.
- **overrides**—Override the default configuration settings for the extended DHCP local server. For information, see [“Overriding Default DHCP Local Server Configuration Settings” on page 255](#).

**Related
Documentation**

- [Grouping Interfaces with Common DHCP Configurations on page 223](#)

Configuring Group-Specific DHCP Relay Options

You can include the following statements at the **[edit forwarding-options dhcp-relay group group-name]** hierarchy level to set group-specific DHCP relay agent configuration options. Group-specific statements apply only to the named group of interfaces, and override any global DHCP relay agent settings for the same statement.

Include the statements at the **[edit forwarding-options dhcp-relay dhcpv6 group group-name]** hierarchy level to configure group-specific options for DHCPv6 relay agent.

- **active-server-group**—Configure an active server group to apply a common DHCP relay agent configuration to a named group of DHCP server addresses. For information, see [“Configuring Active Server Groups” on page 259](#).
- **authentication**—Configure the parameters the router (or switch) sends to the external AAA server.
- **dynamic-profile**—Specify the dynamic profile that is attached to a group of interfaces.
- **interface**—Specify one or more interfaces, or a range of interfaces, that are within the specified group.
- **liveness-detection**—Configure bidirectional failure detection timers and authentication criteria for static routes. For more information, see *DHCP Liveness Detection Overview*.
- **overrides**—Override the default configuration settings for the extended DHCP relay agent. For information, see [“Overriding the Default DHCP Relay Configuration Settings” on page 256](#).
- **relay-agent-interface-id**—(DHCPv6 only) Insert the DHCPv6 Relay Agent Interface-ID option (option 18) in DHCPv6 packets destined for the DHCPv6 server.
- **relay-agent-remote-id**—(DHCPv6 only) Insert the DHCPv6 Relay Agent Remote-ID option (option 37) in DHCPv6 packets destined for the DHCPv6 server.
- **relay-option**—Configure selective processing, which uses DHCP options in client packets to identify and filter client traffic, and to specify the action DHCP relay agent takes with the traffic. For more information, see [“Using DHCP Option Information to Selectively Process DHCP Client Traffic” on page 273](#).

- **relay-option-82**—(DHCPv4 only) Enable or disable the insertion of option 82 information in packets destined for a DHCP server. For information, see [“Using DHCP Relay Agent Option 82 Information” on page 266](#).
- **service-profile**—Specify the default subscriber service, (or default profile) which is activated when the subscriber (or DHCP client) logs in and no other service is activated by a RADIUS server or a provisioning server. For more information, see [“Default Subscriber Service Overview” on page 199](#).

Related Documentation

- [Grouping Interfaces with Common DHCP Configurations on page 223](#)

Example: Configuring DHCP and DHCPv6 Relay Agent Group-Level Selective Traffic Processing

This example shows how to configure named interface group-based support for DHCPv6 relay agent selective processing, which uses DHCP option strings to identify, filter, and process client traffic.

This example describes DHCPv6 relay agent configuration—you can configure the related procedure for DHCP relay agent groups at the **[edit forwarding-options dhcp-relay]** hierarchy level. DHCPv6 selective processing supports DHCPv6 options 15 and 16. DHCP selective processing supports option 60 (MX Series routers only) and option 77.

- [Requirements on page 227](#)
- [Overview on page 228](#)
- [Configuration on page 228](#)
- [Verification on page 230](#)

Requirements

This example uses the following hardware and software components:

- MX Series 3D Universal Edge Routers or PTX Series Packet Transport Routers

Before you configure DHCPv6 relay agent selective processing support, be sure you:

- Configure DHCPv6 relay agent.
See [“Extended DHCP Relay Agent Overview” on page 194](#) and *DHCPv6 Relay Agent Overview*.
- Configure the DHCPv6 named interface groups used for the configuration.
See [“Grouping Interfaces with Common DHCP Configurations” on page 223](#).
- Configure the DHCPv6 server groups used for the processing actions.
See [“Grouping Interfaces with Common DHCP Configurations” on page 223](#).

Overview

In this example, you configure group-level DHCPv6 relay agent named interface support for selective processing of client packets based on DHCPv6 option strings. To configure selective processing, you perform the following procedures:

1. Identify the client traffic—Specify the DHCPv6 option that DHCPv6 relay agent uses to identify the client traffic you want to process. The DHCPv6 option you specify matches the option in the client traffic.
2. Configure the default action—Specify the default processing action, which DHCPv6 relay uses for identified client traffic that does not satisfy any configured match criteria.
3. Create match filters and associate an action with each filter—Specify match criteria that filters the client traffic. The criteria can be an exact match or a partial match with the DHCPv6 option string in the client traffic. Associate a processing action with each match criteria.

Configuration

To configure group-level DHCPv6 relay agent selective processing based on DHCPv6 option information, perform these tasks:

- [Configuring a DHCPv6 Relay Agent Named Interface Group To Selectively Process Client Traffic Based on DHCPv6 Option Strings on page 228](#)
- [Results on page 229](#)

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the command into the CLI at the **[edit]** hierarchy level. The quick configuration assumes that the named interface group and the DHCP server groups have been previously configured.

```
set forwarding-options dhcp-relay dhcpv6 group groupv6-east-27
set forwarding-options dhcp-relay dhcpv6 relay-option option-number 15
set forwarding-options dhcp-relay dhcpv6 relay-option equals ascii triple-gold
  relay-server-group relayserver-triple-8
set forwarding-options dhcp-relay dhcpv6 relay-option equals ascii triple-silver
  relay-server-group relayserver-triple-23
set forwarding-options dhcp-relay dhcpv6 relay-option starts-with ascii single
  relay-server-group relayserver-1-aa
set forwarding-options dhcp-relay dhcpv6 relay-option default-action drop
```

[Configuring a DHCPv6 Relay Agent Named Interface Group To Selectively Process Client Traffic Based on DHCPv6 Option Strings](#)

Step-by-Step Procedure

This procedure assumes that you have previously created the named interface group and the DHCPv6 server groups. To configure DHCPv6 relay group-level selective processing:

1. Specify that you want to configure DHCPv6 relay agent support.
[edit forwarding-options]


```
user@host# edit dhcp-relay dhcpv6
```

- Specify that you want to configure group-level DHCPv6 relay agent support.

```
[edit forwarding-options dhcp-relay dhcpv6]
```

```
user@host# edit group groupv6-east-27
```

- Specify the DHCPv6 option number that DHCPv6 relay agent uses to identify incoming client traffic.

```
[edit forwarding-options dhcp-relay dhcpv6 group groupv6-east-27]
```

```
user@host# set relay-option option-number 15
```

- Configure the default action, which DHCPv6 relay agent uses when the incoming client traffic does not satisfy any configured match criteria.

```
[edit forwarding-options dhcp-relay dhcpv6 group groupv6-east-27]
```

```
user@host# set relay-option default-action relay-server-group relayserver-def-4
```

- Configure an exact match condition and associated action that DHCPv6 relay uses to process the identified client traffic.

```
[edit forwarding-options dhcp-relay dhcpv6 group groupv6-east-27]
```

```
user@host# set relay-option equals ascii triple-gold relay-server-group  
relayserver-triple-8
```

- Configure a second exact match condition and associated action that DHCPv6 relay uses to process client traffic.

```
[edit forwarding-options dhcp-relay dhcpv6 group groupv6-east-27]
```

```
user@host# set relay-option equals ascii triple-silver relay-server-group  
relayserver-triple-23
```

- Configure a partial match criteria and associated action that DHCPv6 relay uses to process client traffic.

```
[edit forwarding-options dhcp-relay dhcpv6 group groupv6-east-27]
```

```
user@host# set relay-option starts-with ascii single relay-server-group  
relayserver-1-aa
```

Results

From configuration mode, confirm the results of your configuration by issuing the **show** statement at the **[edit forwarding-options dhcp]** hierarchy level. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
dhcpv6 {  
  group test-1 {  
    relay-option {  
      option-number 15;  
      equals {  
        ascii triple-gold {  
          relay-server-group relayserver-triple-8;  
        }  
        ascii triple-silver {  
          relay-server-group relayserver-triple-23;  
        }  
      }  
    }  
  }  
}
```

```
    default-action {
        relay-server-group relayserver-def-4;
    }
    starts-with {
        ascii single {
            relay-server-group relayserver-1-aa;
        }
    }
}
interface ge-1/0/0.0 upto ge-1/1/0.0;
}
server-group {
    relayserver-1-aa;
    relayserver-triple-8;
    relayserver-triple-23;
    relayserver-def-4;
}
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To verify the status of DHCPv6 relay agent selective traffic processing, perform this task:

- [Verifying the Status of DHCPv6 Relay Agent Selective Traffic Processing on page 230](#)

Verifying the Status of DHCPv6 Relay Agent Selective Traffic Processing

Purpose Verify the DHCPv6 relay agent selective traffic processing status.

Action Display statistics for DHCPv6 relay agent.

```
user@host> show dhcpv6 relay statistics
DHCPv6 Packets dropped:
  Total 0

Messages received:
  DHCPV6_DECLINE 0
  DHCPV6_SOLICIT 10
  DHCPV6_INFORMATION_REQUEST 0
  DHCPV6_RELEASE 0
  DHCPV6_REQUEST 10
  DHCPV6_CONFIRM 0
  DHCPV6_RENEW 0
  DHCPV6_REBIND 0
  DHCPV6_RELAY_REPL 0

Messages sent:
  DHCPV6_ADVERTISE 0
  DHCPV6_REPLY 0
  DHCPV6_RECONFIGURE 0
  DHCPV6_RELAY_FORW 0

Packets forwarded:
  Total 4
  FWD REQUEST 2
  FWD REPLY 2
```

Meaning The **Packets forwarded** field in the **show dhcpv6 relay statistics** command output displays the number of client packets that have been forwarded as a result of the selective traffic processing configuration. In this example, the output indicates the total number of packets that DHCPv6 relay agent has forwarded, as well as a breakdown for the number of **FWD REQUEST** and **FWD REPLY** packets forwarded.

- Related Documentation**
- [Extended DHCP Relay Agent Overview on page 194](#)
 - [DHCPv6 Relay Agent Overview](#)
 - [DHCP Options and Selective Traffic Processing Overview](#)
 - [Using DHCP Option Information to Selectively Process DHCP Client Traffic on page 273](#)
 - [Grouping Interfaces with Common DHCP Configurations on page 223](#)
 - [Displaying a Count of DHCP Packets That Are Dropped or Forwarded During Selective Processing That Is Based on DHCP Option Strings on page 310](#)
 - [Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings on page 275](#)

Configuring the Number of DHCP Clients Per Interface

- [Specifying the Maximum Number of DHCP Clients Per Interface on page 233](#)
- [Allowing Only One DHCP Client Per Interface on page 234](#)

Specifying the Maximum Number of DHCP Clients Per Interface

By default, there is no limit to the number of DHCP local server or DHCP relay clients allowed on an interface. However, you can override the default setting and specify the maximum number of clients allowed per interface, in the range 1 through 500,000. When the number of clients on the interface reaches the specified limit, no additional DHCP Discover PDUs or DHCPv6 Solicit PDUs are accepted. When the number of clients subsequently drops below the limit, new clients are again accepted.



NOTE: The maximum number of DHCP (and DHCPv6) local server clients or DHCP (and DHCPv6) relay clients can also be specified by Juniper Networks VSA 26-143 during client login. The VSA-specified value always takes precedence if the `interface-client-limit` statement specifies a different number.

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

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

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

```
[edit system services dhcp-local-server]
user@host# edit overrides
```
 - For DHCPv6 local server:

```
[edit system services dhcp-local-server dhcpv6]
user@host# edit overrides
```
 - For DHCP relay agent:

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

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

- For DHCPv6 relay agent:

```
[edit forwarding-options dhcp-relay dhcpv6]
```

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

2. Configure the maximum number of clients allowed per interface. (DHCP local server, DHCPv6 local server, DHCP relay agent and DHCPv6 relay agent all support the **interface-client-limit** statement.)

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

```
user@host# set interface-client-limit number
```



NOTE: For DHCP local server and DHCP relay agent, you can use either the **interface-client-limit** statement or the **client-discover-match incoming-interface** statement to set a limit of one client per interface. The **interface-client-limit** statement with a value of 1 retains the existing client and rejects any new client connections. The **client-discover-match incoming-interface** statement deletes the existing client and allows a new client to connect.

Related Documentation

- [Overriding Default DHCP Local Server Configuration Settings on page 255](#)
- [Allowing Only One DHCP Client Per Interface on page 234](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 258](#)
- [Extended DHCP Local Server Overview on page 188](#)
- [Extended DHCP Relay Agent Overview on page 194](#)

Allowing Only One DHCP Client Per Interface

Subscriber management provides two methods that you can use to configure DHCP local server and DHCP relay agent to allow only one DHCP client per interface. The two methods differ on which client is allowed on the interface—the new client or the existing client. The two methods are supported by both DHCP local server and DHCP relay agent, and can be configured globally, for a group of interfaces, or for a specific interface.

- **Accept new client**—Delete the existing client binding and allow the new client to connect. To configure this action, use the ... **overrides client-discover-match incoming-interface** statement.
- **Keep existing client**—Retain the existing client binding on the interface and reject any requests from new DHCP clients. To configure this action, use the ... **overrides interface-client-limit 1** statement to specify a maximum of one client.

To configure the router to delete the existing client binding on the interface and allow the new client to connect:

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

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

- For DHCP relay agent:

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

2. Configure the router to view all client connections on the interface as coming from the same client, which allows a new client to replace the existing client. This example shows the DHCP local server configuration. The DHCP relay agent configuration is similar.

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

To configure the router to keep the existing client binding on the interface and refuse connections from new clients:

1. Specify that you want to configure override options.

- For DHCP local server:

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

- For DHCP relay agent:

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

2. Set the maximum number of clients allowed per interface to one. This example shows the DHCP local server configuration. The DHCP relay agent configuration is similar.

```
[edit system services dhcp-local-server overrides]
user@host# set interface-client-limit 1
```

Related Documentation

- [DHCP Auto Logout Overview on page 249](#)
- [Automatically Logging Out DHCP Clients on page 251](#)

Maintaining Subscribers During Interface Delete Events

- [Subscriber Binding Retention During Interface Delete Events on page 237](#)
- [Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events on page 238](#)
- [Verifying and Managing the DHCP Maintain Subscribers Feature on page 238](#)

Subscriber Binding Retention During Interface Delete Events

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



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

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

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

- `clear dhcp server binding`
- `clear dhcpv6 server binding`
- `clear dhcp relay binding`

- Related Documentation**
- [Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events on page 238](#)
 - [Verifying and Managing the DHCP Maintain Subscribers Feature on page 238](#)

Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events

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

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

1. Specify that you want to configure subscriber management.

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

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

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

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

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

- Related Documentation**
- [Subscriber Binding Retention During Interface Delete Events on page 237](#)
 - [Verifying and Managing the DHCP Maintain Subscribers Feature on page 238](#)

Verifying and Managing the DHCP Maintain Subscribers Feature

Purpose Display information related to the DHCP maintain-subscribers feature and explicitly log out maintained clients.

- Action**
- To display DHCP local server binding information for the DHCP maintain subscribers feature:

```
user@host>show dhcp server binding detail
```
 - To display DHCPv6 local server binding information for the DHCP maintain subscribers feature:

```
user@host>show dhcpv6 server binding detail
```
 - To display DHCP relay binding information for the DHCP maintain subscribers feature:

```
user@host>show dhcp relay binding detail
```
 - To explicitly log out a DHCP local server subscriber when the maintain subscriber feature is enabled:

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

- To explicitly log out a DHCPv6 local server subscriber when the maintain subscriber feature is enabled:

```
user@host>clear dhcpv6 server binding binding-type
```

- To explicitly log out a DHCP relay subscriber when the maintain subscriber feature is enabled:

```
user@host>clear dhcp relay binding binding-type
```

**Related
Documentation**

- [Subscriber Binding Retention During Interface Delete Events on page 237](#)
- [Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events on page 238](#)

CHAPTER 24

Forcing Dynamic Reconfiguration of Clients From a DHCP Local Server

- [Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients on page 241](#)
- [Configuring Dynamic Client Reconfiguration of Extended Local Server Clients on page 244](#)
- [Configuring Dynamic Reconfiguration Attempts for DHCP Clients on page 246](#)
- [Configuring Deletion of the Client When Dynamic Reconfiguration Fails on page 247](#)
- [Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect on page 247](#)

Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients

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

Default Client/Server Interaction

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



NOTE: Technically, the DHCP client/server interactions are the same on routers and switches. However, the primary usage of this technology on the routers is for subscriber management. The switches are not used for subscriber management. Therefore, this topic provides two sample scenarios. The actions are the same, but the implementation details are different.

- On routers—Suppose a service provider restructures its addressing scheme or changes the server IP addresses that it provided to clients. Without dynamic reconfiguration, the service provider typically clears the DHCP server binding table, but cannot inform the DHCP clients that their bindings have been cleared. Consequently, the DHCP client operates as though its IP address is still valid, but it is now unable to communicate over the access network, resulting in an outage. The DHCP local server needs to wait for the client to send a message to renew its lease or rebind to the server. In response,

the server sends a NAK message to the client to force it to begin the DHCP connection process again. Alternatively, the provider can wait for customers to make a service call about the network failures and then instruct them to power cycle their customer premises equipment to reinitiate the connection. Neither of these actions is timely or convenient for customers.

- On switches—Suppose you restructure the addressing scheme or change the server IP addresses that the DHCP server provides to clients. Without dynamic reconfiguration, the network typically clears the DHCP server binding table, but cannot inform the DHCP clients that their bindings have been cleared. Consequently, the DHCP client operates as though its IP address is still valid, but it is now unable to communicate over the access network, resulting in an outage. The DHCP local server needs to wait for the client to send a message to renew its lease or rebind to the server. In response, the server sends a NAK message to the client to force it to begin the DHCP connection process again. Alternatively, you can wait for users to notify you of the network failures and then instruct them to power cycle their equipment to reinitiate the connection. Neither of these actions is timely or convenient for users.

Dynamic Client/Server Interaction for DHCPv4

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

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

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

Dynamic Client/Server Interaction for DHCPv6

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

DHCPv6 servers send reconfigure messages to DHCPv6 clients, initiating a message exchange. In response, DHCPv6 clients that support the reconfigure message transition

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

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

Manually Forcing the Local Server to Initiate the Reconfiguration Process

You can force the local server to initiate the reconfiguration process for clients by issuing the **request dhcp server reconfigure** command for DHCPv4 clients, and the **request dhcpv6 server reconfigure** command for DHCPv6 clients. Command options determine whether reconfiguration is then attempted for all clients or specified clients.

Action Taken for Events That Occur During a Reconfiguration

Events that take place while a reconfiguration is in process take precedence over the reconfiguration. [Table 37 on page 243](#) lists the actions taken in response to several different events.

Table 37: Action Taken for Events That Occur During a Reconfiguration

Event	Action
Server receives a discover (DHCPv4) or solicit (DHCPv6) message from the client.	Server drops packet and deletes client.
Server receives a request, renew, rebind, or init-reboot message from the client.	DHCPv4—Server sends NAK message and deletes client. DHCPv6—Server drops packet and deletes client. Server replies to renew message with lease time of zero (0).
Server receives a release or decline message from the client.	Server deletes client.
The client lease times out.	Server deletes client.
The clear dhcp server binding command is issued.	Server deletes client.
The request dhcp server reconfigure (DHCPv4) or request dhcpv6 server reconfigure (DHCPv6) command is issued.	Command is ignored.

Table 37: Action Taken for Events That Occur During a Reconfiguration (*continued*)

Event	Action
GRES or DHCP restart occurs.	Reconfiguration process is halted.

Related Documentation

- [Configuring Dynamic Client Reconfiguration of Extended Local Server Clients on page 244](#)

Configuring Dynamic Client Reconfiguration of Extended Local Server Clients

The DHCP local server can initiate reconfiguration of its clients to avoid extended outages because of server configuration changes. You can enable dynamic reconfiguration for all DHCP clients or only the DHCP clients serviced by a specified group of interfaces, and you can modify the behavior accordingly.

You can modify the behavior of the reconfiguration process by including the appropriate statements at the **[edit system services dhcp-local-server reconfigure]** hierarchy level for all DHCPv4 clients, and at the **[edit system services dhcp-local-server dhcpv6 reconfigure]** hierarchy level for all DHCPv6 clients. To override this global configuration for only the DHCP clients serviced by a specified group of interfaces, you can include the statements with different values at the **[edit system services dhcp-local-server group group-name reconfigure]** hierarchy level for DHCPv4 clients, and at the **[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]** hierarchy level for DHCPv6 clients.

To configure dynamic reconfiguration of DHCP clients:

1. Enable dynamic reconfiguration with default values for all clients.

For DHCPv4:

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

For DHCPv6:

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

2. (Optional) Enable dynamic reconfiguration for only the DHCP clients serviced by a group of interfaces.

For DHCPv4:

```
[edit system services dhcp-local-server group-name]
user@host# set reconfigure
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 group group-name]
user@host# set reconfigure
```


3. (Optional) Configure an authentication token. The DHCP local server then includes this token inside the authentication option when it sends `forcerenew` or `reconfigure` messages. If the service provider has previously configured the DHCP client with this token, then the client can compare that token against the newly received token, and reject the message if the tokens do not match. This functionality corresponds to RFC 3118, *Authentication for DHCP Messages*, section 4.

- a. For all clients:

For DHCPv4:

```
[edit system services dhcp-local-server reconfigure]
user@host# set token token-value
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set token token-value
```

- b. For only the DHCP clients serviced by a group of interfaces:

For DHCPv4:

```
[edit system services dhcp-local-server group-name reconfigure]
user@host# set token token-value
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]
user@host# set token token-value
```

4. For the DHCPv6 server only, you can include the `strict` statement. By default, the server accepts solicit messages from clients that do not support server-initiated reconfiguration. Including this statement causes the server to discard solicit messages from nonsupporting clients; consequently the server does not bind these clients.

For all DHCPv6 clients:

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set strict
```

For only the DHCPv6 clients serviced by a group of interfaces:

```
[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]
user@host# set strict
```

5. (Optional) Configure how the server attempts reconfiguration.
See [“Configuring Dynamic Reconfiguration Attempts for DHCP Clients” on page 246](#).
6. (Optional) Configure the response to a failed reconfiguration.
See [“Configuring Deletion of the Client When Dynamic Reconfiguration Fails” on page 247](#).
7. (Optional) Configure the behavior in response to a RADIUS-initiated disconnect.
See [“Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect” on page 247](#).
8. (Optional) Configure a token for rudimentary server authentication.

See [“Configuring a Token for DHCP Local Server Authentication”](#) on page 283.

9. (Optional) Initiate reconfiguration of some or all client bindings.

See [“Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings”](#) on page 307.

10. (Optional) Prevent DHCPv6 clients from binding if they do not support reconfigure messages.

See [“Preventing Binding of Clients That Do Not Support Reconfigure Messages”](#) on page 292.

Configuring Dynamic Reconfiguration Attempts for DHCP Clients

You can configure how many attempts the local server makes to initiate reconfiguration of the DHCP client by sending `forcerenew` or `reconfigure` messages. You can also specify how long the server waits between attempts. By default, eight attempts are made and the initial interval is two seconds.

Each successive attempt doubles the interval between attempts. For example, if the first value is 2, the first retry is attempted 2 seconds after the first attempt fails. The second retry is attempted 4 seconds after the first retry fails. The third retry is attempted 8 seconds after the second retry fails, and so on. A group configuration takes precedence over a DHCP local server configuration.

(Optional) To configure DHCP local server reconfiguration behavior for all DHCP clients:

1. Specify the number of reconfiguration attempts.

For DHCPv4:

```
[edit system services dhcp-local-server reconfigure]
user@host# set attempts 5
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set attempts 5
```

2. Specify the interval between reconfiguration attempts.

For DHCPv4:

```
[edit system services dhcp-local-server reconfigure]
user@host# set timeout 8
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set timeout 8
```

To override the global configuration for a particular group of clients, include the statements at the `[edit system services dhcp-local-server group group-name reconfigure]` hierarchy level or the `[edit system services dhcpv6 dhcp-local-server group group-name reconfigure]` hierarchy level.

- Related Documentation**
- [Configuring Dynamic Client Reconfiguration of Extended Local Server Clients on page 244](#)

Configuring Deletion of the Client When Dynamic Reconfiguration Fails

You can configure the local server to delete the client when the maximum number of reconfiguration attempts has been made without success. By default, the client's original configuration is restored.

(Optional) To configure the DHCP local server to delete the client when reconfiguration is not successful, for all clients:

- Specify the client deletion.

For DHCPv4:

```
[edit system services dhcp-local-server reconfigure]
user@host# set clear-on-abort
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set clear-on-abort
```

To override the global configuration for a particular group of clients, include the statement at the `[edit system services dhcp-local-server group group-name reconfigure]` hierarchy level or the `[edit system services dhcpv6 dhcp-local-server group group-name reconfigure]` hierarchy level.

- Related Documentation**
- [Configuring Dynamic Client Reconfiguration of Extended Local Server Clients on page 244](#)
 - [clear-on-abort on page 661](#)

Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect

You can configure the local server to reconfigure the client when the client receives a RADIUS-initiated disconnect. By default, the client is deleted when a RADIUS-initiated disconnect is received.

(Optional) To configure the DHCP local server to reconfigure the client instead of deleting the client when a RADIUS-initiated disconnect is received, for all clients:

- Specify the RADIUS-initiated disconnect trigger.

For DHCPv4:

```
[edit system services dhcp-local-server reconfigure trigger]
user@host# set radius-disconnect
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure trigger]
user@host# set radius-disconnect
```

To override the global configuration for a particular group of clients, include the statement at the `[edit system services dhcp-local-server group group-name reconfigure trigger]` hierarchy level or the `[edit system services dhcpv6 dhcp-local-server group group-name reconfigure trigger]` hierarchy level.

**Related
Documentation**

- [Configuring Dynamic Client Reconfiguration of Extended Local Server Clients on page 244](#)
- [radius-disconnect on page 874](#)
- [trigger on page 972](#)

CHAPTER 25

Conserving IP Addresses Using DHCP Auto Logout

- [DHCP Auto Logout Overview on page 249](#)
- [Automatically Logging Out DHCP Clients on page 251](#)
- [How DHCP Relay Agent Uses Option 82 for Auto Logout on page 252](#)

DHCP Auto Logout Overview

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

- [Auto Logout Overview on page 249](#)
- [How DHCP Identifies and Releases Clients on page 250](#)
- [Option 60 and Option 82 Requirements on page 251](#)

Auto Logout Overview

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

Auto logout is particularly useful when DHCP uses long lease times for IP address assignments and to help avoid allocating duplicate IP addresses for a single client.

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

How DHCP Identifies and Releases Clients

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

In order to explicitly identify clients, auto logout uses a secondary identification method when the primary identification method is unsuccessful—the primary method is considered unsuccessful if the MAC address or Client Identifier does not match that of an existing client. Subscriber management supports two secondary identification methods that you can configure.

- Incoming interface method—DHCP views a new client connection on the interface as if it comes from the same client. DHCP deletes the existing client binding before creating a binding for the newly connected device. This method allows only one client device to connect on the interface.



NOTE: The incoming interface method differs from the `overrides interface-client-limit 1` statement, which retains the existing binding and rejects the newly connected client.

- Option 60 and option 82 method—DHCP considers two clients as different if they have the same option 60 and option 82 information, but different subnets.

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

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

If the DHCP relay receives a Discover message from an existing client, the DHCP relay forwards the Discover message to the DHCP server. The DHCP relay preserves the binding if the client's existing IP address is returned by the DHCP server. This behavior is not applicable if the proxy-mode override or client-discover-match functionality are enabled.



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

Option 60 and Option 82 Requirements

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

DHCP relay agent requires that the received discover packet contain DHCP option 60. DHCP relay determines the option 82 value based on the guidelines provided in [“How DHCP Relay Agent Uses Option 82 for Auto Logout” on page 252](#).

Related Documentation

- [Automatically Logging Out DHCP Clients on page 251](#)
- [How DHCP Relay Agent Uses Option 82 for Auto Logout on page 252](#)
- [Allowing Only One DHCP Client Per Interface on page 234](#)
- [Clearing DHCP Bindings for Subscriber Access on page 308](#)

Automatically Logging Out DHCP Clients

You can configure the extended DHCP local server and extended DHCP relay to automatically log out DHCP clients. Auto logout immediately releases an existing client when DHCP receives a discover packet from a client whose identity matches an existing client. DHCP then releases the existing client IP address without waiting for the normal lease expiration.



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

To configure DHCP client auto logout:

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


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


```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```
2. Enable auto logout and specify the secondary identification method you want to use when the primary identification method is unsuccessful.
 - For example, to configure DHCP local server to use the incoming interface method:


```
[edit system services dhcp-local-server overrides]
user@host# set client-discover-match incoming-interface
```
 - For example, to configure DHCP relay agent to use the option 60 and option 82 method:

[edit forwarding-options dhcp-relay overrides]
 user@host# set **client-discover-match** option60-and-option82



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

Related Documentation

- [DHCP Auto Logout Overview on page 249](#)
- [How DHCP Relay Agent Uses Option 82 for Auto Logout on page 252](#)
- [Allowing Only One DHCP Client Per Interface on page 234](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 258](#)
- [Extended DHCP Local Server Overview on page 188](#)
- [Extended DHCP Relay Agent Overview on page 194](#)

How DHCP Relay Agent Uses Option 82 for Auto Logout

Table 38 on page 252 indicates how the DHCP relay agent determines the option 82 value used for the client auto logout feature. Depending on the configuration settings, DHCP relay agent takes the action indicated in the right column.

Table 38: DHCP Relay Agent Option 82 Value for Auto Logout

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

Table 38: DHCP Relay Agent Option 82 Value for Auto Logout (*continued*)

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

Related Documentation

- [DHCP Auto Logout Overview on page 249](#)
- [Automatically Logging Out DHCP Clients on page 251](#)

Overriding Default DHCP Local Server Configuration Settings

- [Overriding Default DHCP Local Server Configuration Settings on page 255](#)
- [Overriding the Default DHCP Relay Configuration Settings on page 256](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 258](#)

Overriding Default DHCP Local Server Configuration Settings

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

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

To override default DHCP local server configuration settings:

1. Specify that you want to configure override options.

Global override:

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

Group level override:

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

Per-interface override:

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

2. (Optional) Override the maximum number of DHCP clients allowed per interface.
See [“Specifying the Maximum Number of DHCP Clients Per Interface” on page 233.](#)
3. (Optional) Configure DHCP client auto logout.
See [“Automatically Logging Out DHCP Clients” on page 251.](#)
4. (Optional) Enable processing of information requests from clients.
See [“Enabling Processing of Client Information Requests” on page 214.](#)
5. (Optional, DHCPv6 only) Specify a delegated pool name to use for DHCPv6 multiple address assignment.
See [“Specifying the Delegated Address Pool for IPv6 Prefix Assignment” on page 290.](#)
6. (Optional, DHCPv6 only) Enable DHCPv6 rapid commit support.
See [“Enabling DHCPv6 Rapid Commit Support” on page 291.](#)
7. (Optional, DHCPv6 only) Specify that DHCPv6 local server return DNS server addresses as IA_NA or IA_PD suboptions rather than as a global DHCPv6 option..
See [“Overriding How the DNS Server Address Is Returned in a DHCPv6 Multiple Address Environment” on page 326.](#)
8. (Optional) Delete DHCP override settings.
See [“Deleting DHCP Local Server and DHCP Relay Override Settings” on page 258.](#)

**Related
Documentation**

- [Configuring Group-Specific DHCP Local Server Options on page 225](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 258](#)

Overriding the Default DHCP Relay Configuration Settings

You can override the default DHCP and DHCPv6 relay agent configuration settings at the global level, for a named group of interfaces, or for a specific interface within a named group.

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

- To override DHCP relay configuration options for a specific interface within a named group of interfaces, include the statements at the **[edit forwarding-options dhcp-relay group *group-name* interface]** hierarchy level.
- To configure overrides for DHCPv6 relay, use the supported statements at the **[edit forwarding-options dhcp-relay dhcpv6]** hierarchy level.

To override default DHCP relay agent configuration settings:

1. Specify that you want to configure override options.

Global override:

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

Group-level override:

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

Per-interface override:

```
[edit forwarding-options dhcp-relay]
user@host# edit group boston interface fe-1/0/1.2 overrides
```

2. (DHCPv4 only) Enable DHCP relay proxy mode.
See [“Enabling DHCP Relay Proxy Mode” on page 281](#).
3. (DHCPv4 only) Overwrite the giaddr in DHCP packets that the DHCP relay agent forwards.
See [“Changing the Gateway IP Address \(giaddr\) Field to the giaddr of the DHCP Relay Agent” on page 261](#).
4. (DHCPv4 only) Replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr).
See [“Replacing the DHCP Relay Request and Release Packet Source Address” on page 261](#).
5. (DHCPv4 only) Override the DHCP relay agent information option (option 82) in DHCP packets.
See [Overriding Option 82 Information](#).
6. (DHCPv4 only) Override the setting of the broadcast bit in DHCP request packets and use the Layer 2 unicast transmission method.
See [“Using Layer 2 Unicast Transmission for DHCP Packets” on page 263](#).
7. (DHCPv4 only) Trust DHCP client packets that have a giaddr of 0 and that contain option 82 information.
See [“Trusting Option 82 Information” on page 264](#).
8. (DHCPv4 and DHCPv6) Override the maximum number of DHCP clients allowed per interface.
See [“Specifying the Maximum Number of DHCP Clients Per Interface” on page 233](#).

9. (DHCPv4 only) Configure client auto logout.

See [“DHCP Auto Logout Overview” on page 249](#).

10. (DHCPv4 and DHCPv6) Enable or disable support for DHCP snooped clients on interfaces.

See *Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent*.

11. (DHCPv4 and DHCPv6) Delay authentication of subscribers until the DHCP client sends a Request packet.

See the [delay-authentication](#) statement.

12. (DHCPv4 and DHCPv6) Send release messages to the DHCP server when clients are deleted.

See [“Sending Release Messages When Clients Are Deleted” on page 264](#).

13. (DHCPv4 only) Disable the DHCP relay agent on specific interfaces.

See [“Disabling DHCP Relay” on page 280](#).

14. (DHCPv4 and DHCPv6) Disable automatic binding of stray DHCP requests.

See [“Disabling Automatic Binding of Stray DHCP Requests” on page 265](#).

**Related
Documentation**

- [Configuring Group-Specific DHCP Relay Options on page 226](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 258](#)

Deleting DHCP Local Server and DHCP Relay Override Settings

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

- To delete a specific DHCP override setting at a particular hierarchy level, include the **overrides** statement with the appropriate subordinate statements. For example, to delete the DHCP local server override **interface-client-limit** setting for a group named **marin20**:

```
[edit system services dhcp-local-server]
user@host# delete group marin20 overrides interface-client-limit
```

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

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

**Related
Documentation**

- [Overriding Default DHCP Local Server Configuration Settings on page 255](#)
- [Extended DHCP Local Server Overview on page 188](#)
- [Extended DHCP Relay Agent Overview on page 194](#)

CHAPTER 27

Applying a Common DHCP Relay Agent Configuration to Groups of DHCP Servers

- [Configuring Server Groups on page 259](#)
- [Configuring Active Server Groups on page 259](#)

Configuring Server Groups

You can configure a named group of DHCP servers for use by the extended DHCP relay agent on the router or switch.

You specify the name of the DHCP server group and the IP addresses of one or more DHCP servers that belong to this group. You can configure a maximum of five IP addresses per named server group.

To configure a named server group:

1. Specify the name of the server group.

```
[edit forwarding-options dhcp-relay]  
user@host# set server-group myServerGroup
```

2. Add the IP addresses of the DHCP servers belonging to the group.

```
[edit forwarding-options dhcp-relay server-group myServerGroup]  
user@host# set 192.168.100.50  
user@host# set 192.168.100.75
```

Related Documentation

- [Extended DHCP Relay Agent Overview on page 194](#)

Configuring Active Server Groups

You can configure an active server group. Using an active server group enables you to apply a common DHCP relay agent configuration to a named group of DHCP server addresses.

Use the statement at the `[edit ... dhcpv6]` hierarchy levels to configure DHCPv6 support.

To configure an active server group:

- Specify the name of the active server group.

```
[edit forwarding-options dhcp-relay]  
user@host# set active-server-group myServerGroup
```

To create an active server group as a global DHCP relay agent configuration option, include the **active-server-group** statement at the **[edit forwarding-options dhcp-relay]** hierarchy level. To have the group apply only to a named group of interfaces, include the **active-server-group** statement at the **[edit forwarding-options dhcp-relay group *group-name*]** hierarchy level.

Including the **active-server-group** statement at the **[edit forwarding-options dhcp-relay group *group-name*]** hierarchy level (as a group-specific option) overrides the effect of including the **active-server-group** statement at the **[edit forwarding-options dhcp-relay]** hierarchy level as a global option.

**Related
Documentation**

- [Extended DHCP Relay Agent Overview on page 194](#)
- [Grouping Interfaces with Common DHCP Configurations on page 223](#)

CHAPTER 28

Changing the Gateway IP Address (giaddr) Field and DHCP Relay Request and Release Packet Source Address

- [Changing the Gateway IP Address \(giaddr\) Field to the giaddr of the DHCP Relay Agent on page 261](#)
- [Replacing the DHCP Relay Request and Release Packet Source Address on page 261](#)

Changing the Gateway IP Address (giaddr) Field to the giaddr of the DHCP Relay Agent

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

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

1. Specify that you want to configure override options.

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

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

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

Related Documentation

- [Extended DHCP Relay Agent Overview on page 194](#)
- [Overriding the Default DHCP Relay Configuration Settings on page 256](#)

Replacing the DHCP Relay Request and Release Packet Source Address

You can configure the DHCP relay agent to replace request and release packets with the gateway IP address (giaddr) before forwarding the packet to the DHCP server.

To replace the source address with giaddr:

1. Specify that you want to configure override options.

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

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

2. Specify that you want to replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr).

```
[edit forwarding-options dhcp-relay overrides]  
user@host# set replace-ip-source-with giaddr
```

**Related
Documentation**

- [Extended DHCP Relay Agent Overview on page 194](#)
- [Overriding the Default DHCP Relay Configuration Settings on page 256](#)

CHAPTER 29

Configuring DHCP Relay Agent

- [Using Layer 2 Unicast Transmission for DHCP Packets on page 263](#)
- [Trusting Option 82 Information on page 264](#)
- [Sending Release Messages When Clients Are Deleted on page 264](#)
- [Disabling Automatic Binding of Stray DHCP Requests on page 265](#)
- [Using DHCP Relay Agent Option 82 Information on page 266](#)
- [Using DHCP Option Information to Selectively Process DHCP Client Traffic on page 273](#)
- [Example: Minimum DHCP Relay Agent Configuration on page 274](#)
- [Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings on page 275](#)
- [Example: DHCP Relay Agent Configuration with Multiple Clients and Servers on page 279](#)
- [Disabling DHCP Relay on page 280](#)

Using Layer 2 Unicast Transmission for DHCP Packets

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

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

1. Specify that you want to configure override options.

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

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

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

Related Documentation

- [Extended DHCP Relay Agent Overview on page 194](#)
- [Overriding the Default DHCP Relay Configuration Settings on page 256](#)

Trusting Option 82 Information

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

To configure DHCP relay agent to trust option 82 information:

1. Specify that you want to configure override options.

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

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

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

Related Documentation

- [Extended DHCP Relay Agent Overview on page 194](#)
- [Overriding the Default DHCP Relay Configuration Settings on page 256](#)

Sending Release Messages When Clients Are Deleted

By default, when DHCP relay and relay proxy delete a client, they do not send a release message to the DHCP server. You can override the default behavior and configure DHCP relay and relay proxy to send a release message whenever they delete a client. The release message sent by DHCP relay and relay proxy includes option 82 information.



NOTE: You must include the **send-release-on-delete** statement to configure DHCP relay and relay proxy to send the release message when the **client-discover-match** statement is included.

You can use the **[edit forwarding-options dhcp-relay dhcpv6]** hierarchy level to override the default behavior for DHCPv6 relay agent.

To send a release message:

1. Specify that you want to configure override options.

- For DHCP relay agent:

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

- For DHCPv6 relay agent:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit overrides
```

- Specify that you want DHCP relay and relay proxy (or DHCPv6 relay agent) to send a release message when clients are deleted.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set send-release-on-delete
```

**Related
Documentation**

- [Extended DHCP Relay Agent Overview on page 194](#)
- [Overriding the Default DHCP Relay Configuration Settings on page 256](#)

Disabling Automatic Binding of Stray DHCP Requests

DHCP requests that are received but have no entry in the database are known as stray requests. By default, DHCP relay, DHCP relay proxy, and DHCPv6 relay agent attempt to bind the requesting client by creating a database entry and forwarding the request to the DHCP server. If the server responds with an ACK, the client is bound and the ACK is forwarded to the client. If the server responds with a NAK, the database entry is deleted and the NAK is forwarded to the client. This behavior occurs regardless of whether authentication is configured.

You can override the default configuration at the global level, for a named group of interfaces, or for a specific interface within a named group. Overriding the default causes DHCP relay, DHCP relay proxy, and DHCPv6 relay agent to drop all stray requests instead of attempting to bind the clients.



NOTE: Automatic binding of stray requests is enabled by default.

- To disable automatic binding behavior, include the **no-bind-on-request** statement when you configure DHCP overrides at the global, group, or interface level.

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

- To override the default behavior for DHCPv6 relay agent, configure the override at the **[edit forwarding-options dhcp-relay dhcpv6]** hierarchy level.

```
[edit forwarding-options dhcp-relay dhcpv6 overrides]
user@host# set no-bind-on-request
```

The following two examples show a configuration that disables automatic binding of stray requests for a group of interfaces and a configuration that disables automatic binding on a specific interface.

To disable automatic binding of stray requests on a group of interfaces:

- Specify the named group.

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

- Specify that you want to configure overrides.

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

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

3. Disable automatic binding for the group.

```
[edit forwarding-options dhcp-relay group boston overrides]
user@host# set no-bind-on-request
```

To disable automatic binding of stray requests on a specific interface:

1. Specify the named group of which the interface is a member.

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

2. Specify the interface on which you want to disable automatic binding.

```
[edit forwarding-options dhcp-relay group boston]
user@host# edit interface fe-1/0/1.2
```

3. Specify that you want to configure overrides.

```
[edit forwarding-options dhcp-relay group boston interface fe-1/0/1.2]
user@host# edit overrides
```

4. Disable automatic binding on the interface.

```
[edit forwarding-options dhcp-relay group boston interface fe-1/0/1.2 overrides]
user@host# set no-bind-on-request
```

**Related
Documentation**

- [Extended DHCP Relay Agent Overview on page 194](#)
- [Overriding the Default DHCP Relay Configuration Settings on page 256](#)

Using DHCP Relay Agent Option 82 Information

Subscriber management enables you to configure the DHCP relay agent to include additional option 82 information in the DHCP packets that the relay agent receives from clients and forwards to a DHCP server. The DHCP server uses the additional information to determine the IP address to assign to the client. The server might also use the information for other purposes—for example, to determine which services to grant the client, or to provide additional security against threats such as address spoofing. The DHCP server sends its reply back to the DHCP relay agent, and the agent removes the option 82 information from the message and forwards the packet to the client.

To configure support for the DHCP relay agent information option 82, you use the **relay-option-82** statement. You can configure the DHCP relay agent to include the following suboptions in the packet the relay agent sends to the DHCP server:

- Agent Circuit ID (suboption 1)—An ASCII string that identifies the interface on which the client DHCP packet is received.
- Agent Remote ID (suboption 2)—An ASCII string assigned by the DHCP relay agent that securely identifies the client.

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

To restore the default behavior, in which option 82 information is not inserted into DHCP packets, you use the **delete relay-option-82** statement.



NOTE: The DHCPv6 relay agent provides similar Agent Circuit ID and Agent Remote ID support for DHCPv6 clients. For DHCPv6, subscriber management uses DHCPv6 option 18 to include the circuit ID in the packets that the relay agent sends to a DHCPv6 server, and option 37 to include the remote ID in the packets. See “[DHCPv6 Relay Agent Options](#)” on page 295.

The following sections describe the option 82 operations you can configure:

- [Configuring Option 82 Information on page 267](#)
- [Including a Prefix in DHCP Options on page 269](#)
- [Including a Textual Description in DHCP Options on page 271](#)

Configuring Option 82 Information

You use the **relay-option-82** statement to configure the DHCP relay agent to insert option 82 information in DHCP packets that the relay agent receives from clients and forwards to a DHCP server. When you configure option 82, you can include one of the suboption statements to specify the type of information you want to include in the DHCP packets. If you configure option 82 without including one of the suboption statements, the Agent Circuit ID option is included by default. Use the **circuit-id** statement to include the Agent Circuit ID (suboption 1) in the packets, or the **remote-id** statement to include the Agent Remote ID (suboption 2).

You can optionally configure DHCP relay agent to include a prefix or the interface description as part of the suboption information. If you specify the **circuit-id** or **remote-id** statement without including any of the optional **prefix**, **use-interface-description**, **use-vlan-id**, **include-irb-and-l2**, or **no-vlan-interface-name** statements, the format of the Agent Circuit ID or Agent Remote ID information for Fast Ethernet (fe), Gigabit Ethernet (ge), and integrated routing and bridging (irb) interfaces is one of the following, depending on your network configuration:



NOTE: Integrated routing and bridging (IRB) provides simultaneous support for Layer 2 bridging and Layer 3 IP routing on the same interface. IRB enables you to route local packets to another routed interface or to another bridging domain that has a Layer 3 protocol configured.

The interface to bridge domain relationship might be implicit (the interface is mapped to the bridge domain by the system based on the VLAN tag) or explicit (the interface is mapped to the bridge domain by configuring it in the bridge domain definition). For the explicit case, tagging might not be relevant for the mapping.

- For Fast Ethernet or Gigabit Ethernet interfaces that do not use VLANs, stacked VLANs (S-VLANs), or bridge domains:

(fe | ge)-fpc/pic/port.subunit



NOTE: For remote systems, the *subunit* is required and is used to differentiate an interface.

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

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

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

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

In the case of an IRB interface, the format displays the Layer 2 interface instead of the IRB interface along with the bridge domain name. For IRB interfaces (or other pseudo devices) the default format is as follows:

- IRB interfaces that use bridge domains but do not use VLANs or S-VLANs:

(fe | ge)-fpc/pic/port.subunit:bridge-domain-name

- IRB interfaces that use VLANs:

(fe | ge)-fpc/pic/port.subunit:vlan-name

To include the IRB interface name with the Layer 2 interface name, configure the **include-irb-and-l2** statement. The format is as follows:

- IRB interfaces that use bridge domains but do not use VLANs or S-VLANs:

(fe | ge)-fpc/pic/port:bridge-domain-name+irb.subunit

- IRB interfaces that use VLANs:

(fe | ge)-fpc/pic/port:vlan-name+irb.subunit

To include only the IRB interface name without the Layer 2 interface and bridge domain or VLAN, configure the **no-vlan-interface-name** statement. The format is as follows:

irb.subunit

To enable insertion of option 82 information:

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

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

2. Configure the DHCP relay agent to insert the Agent Circuit ID suboption, the Agent Remote ID suboption, or both.

- To insert the Agent Circuit ID:

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

- To insert the Agent Remote ID:

```
[edit forwarding-options dhcp-relay relay-option-82]
```


`user@host# set remote-id`

- To insert both, configure both set commands.
3. (Optional) Configure a prefix that is used in the option 82 information in the DHCP packets.
See [“Including a Prefix in DHCP Options” on page 269](#).
 4. (Optional) Configure the DHCP relay agent to include the interface’s textual description instead of the interface identifier in the option 82 information.
See [“Including a Textual Description in DHCP Options” on page 271](#).

Including a Prefix in DHCP Options

When you configure the DHCP relay agent to include DHCP options in the packets that the relay agent sends to a DHCP server, you can specify that the relay agent add a prefix to the DHCP option. You can add a prefix to the following DHCP options:

- DHCPv4 option 82 Agent Circuit ID (suboption 1)
- DHCPv4 option 82 Agent Remote ID (suboption 2)
- DHCPv6 option 18 Relay Agent Interface-ID
- DHCPv6 option 37 Relay Agent Remote-ID

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

host-name/logical-system-name;routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id

For Fast Ethernet or Gigabit Ethernet interfaces that use VLANs but not S-VLANs, only the *vlan-id* value appears in the DHCP option format.

(DHCPv4) To configure a prefix with the option 82 information:

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

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

2. Configure DHCP relay agent to insert the Agent Circuit ID, the Agent Remote ID, or both.

- To configure the Agent Circuit ID:

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

- To configure the Agent Remote ID:

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

3. Specify that the prefix be included in the option 82 information. In this example, the prefix includes the hostname and logical system name.

- To include the prefix with the Agent Circuit ID:

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

- To include the prefix with the Agent Remote ID:

```
[edit forwarding-options dhcp-relay relay-option-82 remote-id]
user@host# set prefix host-name logical-system-name
```

(DHCPv6) To use a prefix with the DHCPv6 option 18 or option 37 information:

1. Specify that you want to configure DHCPv6 relay agent support.

```
[edit forwarding-options dhcp-relay]
user@host# edit dhcpv6
```

2. Configure DHCPv6 relay agent to insert option 18 (Relay Agent Interface-ID), option 37 (Relay Agent Remote-ID), or both.

- To configure option 18:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-interface-id
```

- To configure option 37:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-interface-id
```

3. Specify that the prefix is included in the option information. In this example, the prefix includes the hostname and logical system name

- To include the prefix with option 18:

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set prefix host-name logical-system-name
```

- To include the prefix with option 37:

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id]
user@host# set prefix host-name logical-system-name
```

Including a Textual Description in DHCP Options

By default, when DHCP relay agent inserts option information in the packets sent to a DHCP server, the options include the interface identifier. However, you can configure the DHCP relay agent to include the textual description that is configured for the interface instead of the interface identifier. You can use the textual description for either the logical interface or the device interface.

You can include the textual interface description in the following DHCP options:

- DHCPv4 option 82 Agent Circuit ID (suboption 1)
- DHCPv4 option 82 Agent Remote ID (suboption 2)
- DHCPv6 option 18 Relay Agent Interface-ID
- DHCPv6 option 37 Relay Agent Remote-ID

The textual description is configured separately, using the **description** statement at the **[edit interfaces interface-name]** hierarchy level. If you specify that the textual description is used and no description is configured for the interface, DHCP relay defaults to using the Layer 2 interface name.

In the case of integrated routing and bridging (IRB) interfaces, the textual description of the Layer 2 interface is used instead of the textual description of the IRB interface. If there is no description configured, the Layer 2 logical interface name is used.



NOTE: For IRB interfaces, the option 82 field must be able to uniquely identify the incoming interface based on either the Agent Circuit ID or Agent Remote ID. You can modify the information in the textual interface description to match the raw IFD (physical interface without a subunit) name and configure the option 82 field to use the interface description.

You can use the textual description with the following DHCP options:

- DHCPv4 Option 82 Agent Circuit ID (suboption 1)
- DHCPv4 Option 82 Agent Remote ID (suboption 2)
- DHCPv6 Relay Agent Interface-ID (option 18)
- DHCPv6 Relay Agent Remote-ID (option 37)

(DHCPv4) To configure the DHCP relay option 82 suboption to include the textual interface description:

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

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

2. Configure DHCP relay agent to insert the Agent Circuit ID, Agent Remote ID, or both.

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

3. Specify that the textual description is included in the option 82 information. In this example, the option 82 information includes the description used for the device interface.

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

(DHCPv6) To configure the DHCPv6 option 18 or option 37 to include the textual interface description:

1. Specify that you want to configure DHCPv6 relay agent support.

```
[edit forwarding-options dhcp-relay]
user@host# edit dhcpv6
```

2. Configure DHCPv6 relay agent to insert option 18 (Relay Agent Interface-ID), option 37 (Relay Agent Remote-ID), or both.

- To configure option 18:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-interface-id
```

- To configure option 37:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-interface-id
```

- Specify that the textual description is included in the option information. In the following example, the option information includes the description used for the device interface.

- To include the textual description in option 18:

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set use-interface-description device
```

- To include the textual description in option 37:

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id]
user@host# set use-interface-description device
```

Using DHCP Option Information to Selectively Process DHCP Client Traffic

The following procedure describes the steps you use to configure DHCP relay agent to selectively process client traffic—selective processing uses DHCP or DHCPv6 option information to identify, filter, and process client traffic. To configure DHCPv6 support you use the procedure at the `[edit forwarding-options dhcp-relay dhcpv6]` hierarchy level.

To configure DHCP relay agent to use option information to selectively process DHCP client traffic:

- Specify that you want to configure DHCP relay agent support.

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

- Specify that you want to use the DHCP option feature to selectively process incoming DHCP traffic.

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

- Specify the DHCP or DHCPv6 option number DHCP relay uses to identify and process the client traffic. You can specify options 60 and 77 for DHCP relay agent, and options 15 and 16 for DHCPv6 relay agent.

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

For example, to identify traffic that has DHCP option 60 information:

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

- (Optional) Configure the default action that DHCP relay uses when the incoming client traffic does not satisfy any configured match or partial match criteria.

For example, to configure DHCP relay to drop traffic by default:

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

- (Optional) Configure an exact match condition that filters the client traffic and specifies the associated action for DHCP relay agent to take.

For example, to select traffic that has an option 60 (configured in the previous step) ASCII string of **video25**, and then forward that traffic to a named local server group:

```
[edit forwarding-options dhcp-relay relay-option]
user@host# set equals ascii video25 local-server-group servergroup-east-video
```

6. (Optional) Configure a partial match condition that filters the client traffic and specifies the associated action.

For example, to select traffic that has an option 60 hexadecimal string that starts with **766964656F** (left to right), and then forward that traffic without creating a new session:

```
[edit forwarding-options dhcp-relay relay-option]
user@host# edit starts-with hexadecimal 766964656F forward-only
```

Related Documentation

- [DHCP Options and Selective Traffic Processing Overview](#)
- [Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings on page 275](#)
- [Example: Configuring DHCP and DHCPv6 Relay Agent Group-Level Selective Traffic Processing on page 227](#)
- [Example: Configuring DHCP Message Exchange Between DHCP Server and Clients in Different Virtual Routing Instances to Increase Security of the DHCP Server](#)

Example: Minimum DHCP Relay Agent Configuration

This example shows the minimum configuration you need to use the extended DHCP relay agent on the router or switch:

```
[edit forwarding-options]
dhcp-relay {
  server-group {
    test 10.0.2.1;
  }
  active-server-group test;
  group all {
    interface fe-0/0/2.0;
  }
}
```



NOTE: The interface type in this topic is just an example. The **fe-** interface type is not supported by EX Series switches.

This example creates a server group and an active server group named **test** with IP address 10.0.2.1. The DHCP relay agent configuration is applied to a group named **all**. Within this group, the DHCP relay agent is enabled on interface fe-0/0/2.0.

Related Documentation

- [Extended DHCP Relay Agent Overview on page 194](#)

Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings

This example shows how to configure DHCP relay agent to use DHCP option strings to selectively identify, filter, and process client traffic.

- [Requirements on page 275](#)
- [Overview on page 275](#)
- [Configuration on page 276](#)
- [Verification on page 277](#)

Requirements

This example uses the following hardware and software components:

- MX Series 3D Universal Edge Routers or EX Series Switches

Before you configure DHCP relay agent selective processing support, be sure you:

- Configure DHCP relay agent.

See [“Extended DHCP Relay Agent Overview” on page 194](#).

- (Optional) Configure a named DHCP local server group if you want to forward client traffic to a server group.

See [“Grouping Interfaces with Common DHCP Configurations” on page 223](#).

Overview

In this example, you configure DHCP relay agent to use DHCP option strings in client packets to selectively identify, filter, and process client traffic. To configure selective processing, you perform the following procedures:

1. Identify the client traffic—Specify the DHCP option that DHCP relay agent uses to identify the client traffic you want to process. The option you specify matches the option in the client traffic.
2. Configure a default action—Specify the default processing action, which DHCP relay uses for identified client traffic that does not satisfy any configured match criteria.
3. Create match filters and associate an action with each filter—Specify match criteria that filter the client traffic. The criteria can be an exact match or a partial match with the option string in the client traffic. Associate a processing action with each match criterion.

Configuration

To configure DHCP relay agent selective processing based on DHCP option information, perform these tasks:

- [Configuring DHCP Relay Agent To Selectively Process Client Traffic Based on DHCP Option Strings on page 276](#)
- [Results on page 277](#)

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the command into the CLI at the **[edit]** hierarchy level.

```
set forwarding-options dhcp-relay relay-option option-number 60
set forwarding-options dhcp-relay relay-option equals ascii video-gold forward-only
set forwarding-options dhcp-relay relay-option equals ascii video-bronze local-server-group
  servergroup-15
set forwarding-options dhcp-relay relay-option starts-with hexadecimal ffff
  local-server-group servergroup-east
set forwarding-options dhcp-relay relay-option default-action drop
```

Configuring DHCP Relay Agent To Selectively Process Client Traffic Based on DHCP Option Strings

Step-by-Step Procedure

To configure DHCP relay selective processing:

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

```
[edit forwarding-options]
user@host# edit dhcp-relay
```
2. Specify the DHCP option that DHCP relay agent uses to identify incoming client traffic.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option option-number 60
```
3. Configure a default action, which DHCP relay agent uses when the incoming client traffic does not satisfy any configured match criteria.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option default-action drop
```
4. Configure an exact match condition and associated action that DHCP relay uses to process the identified client traffic.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option equals ascii video-gold forward-only
```
5. Configure a second exact match condition and associated action that DHCP relay uses to process client traffic.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option equals ascii video-bronze local-server-group
  servergroup-15
```


6. Configure a partial match criteria and associated action that DHCP relay uses to process client traffic.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option starts-with hexadecimal ffff local-server-group
servergroup-east
```

Results

From configuration mode, confirm the results of your configuration by issuing the **show** statement at the **[edit forwarding-options]** hierarchy level. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit forwarding-options]
user@host# show
dhcp-relay {
  relay-option {
    option-number 60;
    equals {
      ascii video-gold {
        forward-only;
      }
    }
    equals {
      ascii video-bronze {
        local-server-group servergroup-15;
      }
    }
    default-action {
      drop;
    }
    starts-with {
      hexadecimal ffff {
        local-server-group servergroup-east;
      }
    }
  }
}
```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To verify the status of DHCP relay agent selective traffic processing, perform this task:

- [Verifying the Status of DHCP Relay Agent Selective Traffic Processing on page 277](#)

Verifying the Status of DHCP Relay Agent Selective Traffic Processing

Purpose Verify the DHCP relay agent selective traffic processing status.

Action Display statistics for DHCP relay agent.

```
user@host> show dhcp relay statistics
Packets dropped:
    Total                30
    Bad hardware address  1
    Bad opcode            1
    Bad options           3
    Invalid server address 5
    No available addresses 1
    No interface match    2
    No routing instance match 9
    No valid local address 4
    Packet too short      2
    Read error            1
    Send error            1
    Option 60             1
    Option 82             2

Messages received:
    BOOTREQUEST          116
    DHCPDECLINE           0
    DHCPDISCOVER          11
    DHCPINFORM            0
    DHCPRELEASE           0
    DHCPREQUEST          105

Messages sent:
    BOOTREPLY             0
    DHCPOFFER             2
    DHCPACK               1
    DHCPNAK               0
    DHCPFORCERENEW        0

Packets forwarded:
    Total                4
    BOOTREQUEST           2
    BOOTREPLY             2
```

Meaning The **Packets forwarded** field in the **show dhcp relay statistics** command output displays the number of client packets that have been forwarded as a result of the selective traffic processing configuration. In this example, the output indicates the total number of packets that DHCP relay agent has forwarded, as well as a breakdown for the number of **BOOTREQUEST** and **BOOTREPLY** packets forwarded.

- Related Documentation**
- [Extended DHCP Relay Agent Overview on page 194](#)
 - [DHCP Options and Selective Traffic Processing Overview](#)
 - [Using DHCP Option Information to Selectively Process DHCP Client Traffic on page 273](#)
 - [Displaying a Count of DHCP Packets That Are Dropped or Forwarded During Selective Processing That Is Based on DHCP Option Strings on page 310](#)
 - [Example: Configuring DHCP and DHCPv6 Relay Agent Group-Level Selective Traffic Processing on page 227](#)

Example: DHCP Relay Agent Configuration with Multiple Clients and Servers

This example shows an extended DHCP relay agent configuration for a network that includes multiple DHCP clients and DHCP servers. Additional details follow the example.

```
[edit forwarding-options]
dhcp-relay {
  server-group {
    sp-1 {
      10.0.2.1;
      10.0.2.2;
    }
    sp-2 {
      10.33.2.1;
      10.33.2.2;
      10.33.2.3;
    }
  }
  active-server-group sp-1;
  overrides layer2-unicast-replies;
  group clients_a {
    relay-option-82 circuit-id;
    interface fe-1/0/1.1;
    interface fe-1/0/1.2;
    interface fe-1/0/1.3;
  }
  group clients_b {
    relay-option-82 {
      circuit-id {
        prefix routing-instance-name;
      }
    }
    interface fe-1/0/1.4;
    interface fe-1/0/1.5;
    interface fe-1/0/1.6;
  }
  group eth_dslam_relay {
    active-server-group sp-2;
    overrides {
      trust-option-82;
      layer2-unicast-replies;
    }
    interface fe-1/0/1.7;
    interface fe-1/0/1.8;
    interface fe-1/0/1.9;
  }
}
```

This example creates two server-groups: **sp-1**, which includes DHCP server addresses 10.0.2.1 and 10.0.2.2, and **sp-2**, which includes DHCP server addresses 10.33.2.1, 10.33.2.2, and 10.33.2.3. The active server group to which the DHCP relay agent configuration applies is **sp-1**. A global override is set that causes the DHCP relay agent to use Layer 2 unicast transmission to send DHCP reply packets from the DHCP server to DHCP clients during the discovery process.

The example also creates three groups of subscribers and their associated Fast Ethernet interfaces: **clients_a**, **clients_b**, and **eth_dslam_relay**. These groups are configured to meet different needs, as follows:

- The **clients_a** and **clients_b** groups consist of basic subscribers. The service provider for these groups inserts option 82 information in the DHCP packets that are destined for the DHCP server.
- The subscribers in **eth_dslam_relay** are connected to an Ethernet digital subscriber line access multiplexer (DSLAM) that functions as a Layer 2 DHCP relay agent. The active server group for **eth_dslam_relay** is **sp-2**. Overrides are set for the **eth_dslam_relay** group that enable the DHCP relay agent to trust option 82 information and to use Layer 2 unicast transmission to send DHCP reply packets to DHCP clients during discovery.

**Related
Documentation**

- [Extended DHCP Relay Agent Overview on page 194](#)

Disabling DHCP Relay

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

To disable DHCP relay agent:

1. Specify that you want to configure override options.

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

2. Disable the DHCP relay agent.

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

**Related
Documentation**

- [Extended DHCP Relay Agent Overview on page 194](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 258](#)

Configuring DHCP Relay Proxy Mode

- [Enabling DHCP Relay Proxy Mode on page 281](#)

Enabling DHCP Relay Proxy Mode

You can enable DHCP relay proxy mode on all interfaces or a group of interfaces.

To enable DHCP relay proxy mode:

1. Specify that you want to configure override options.

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

2. Enable DHCP relay proxy mode.

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

Related Documentation

- [DHCP Relay Proxy Overview on page 197](#)
- [Overriding the Default DHCP Relay Configuration Settings on page 256](#)

CHAPTER 31

Configuring DHCP Local Server Authentication

- [Configuring a Token for DHCP Local Server Authentication on page 283](#)

Configuring a Token for DHCP Local Server Authentication

You can configure the local server to include a constant, unencoded token in the DHCP `forcerenew` message as part of the authentication option it sends to clients. The client compares the received token with a token already configured on the client. If the tokens do not match, the DHCP client discards the `forcerenew` message. Use of the token provides rudimentary protection against inadvertently instantiated DHCP servers.

(Optional) To configure the DHCP local server to include a token in the `forcerenew` message sent to the client, for all clients:

- Specify the token.

For DHCPv4:

```
[edit system services dhcp-local-server reconfigure]
user@host# set token 8ysIU9E32k8r
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set token 8ysIU9E32k8r
```

To override the global configuration for a particular group of clients, include the statement at the `[edit system services dhcp-local-server group group-name reconfigure]` hierarchy level or the `[edit system services dhcpv6 dhcp-local-server group group-name reconfigure]` hierarchy level.

Related Documentation

- [Configuring Dynamic Client Reconfiguration of Extended Local Server Clients on page 244](#)
- [token on page 952](#)

Configuring a Minimum DHCP Local Server Configuration

- [Example: Minimum Extended DHCP Local Server Configuration on page 285](#)

Example: Minimum Extended DHCP Local Server Configuration

This example shows the minimum configuration you need to use for the extended DHCP local server on the router or switch:

```
[edit system services]
dhcp-local-server {
  group group_one {
    interface fe-0/0/2.0;
  }
}
```



NOTE: The interface type in this topic is just an example. The **fe-** interface type is not supported by EX Series switches.

This example creates the server group named **group_one**, and specifies that the DHCP local server is enabled on interface **fe-0/0/2.0** within the group. The DHCP local server uses the default pool match configuration of **ip-address-first**.



NOTE: If you delete the DHCP server configuration, DHCP server bindings might still remain. To ensure that DHCP bindings are removed, issue the **clear dhcp server binding** command before you delete the DHCP server configuration.

Related Documentation

- [Extended DHCP Local Server Overview on page 188](#)

Configuring DHCPv6 Local Server

- [DHCPv6 Local Server Overview on page 287](#)
- [Multiple Address Assignment for DHCPv6 Clients on page 289](#)
- [DHCPv6 Options in a DHCPv6 Multiple Address Environment on page 290](#)
- [Specifying the Delegated Address Pool for IPv6 Prefix Assignment on page 290](#)
- [Enabling DHCPv6 Rapid Commit Support on page 291](#)
- [Preventing Binding of Clients That Do Not Support Reconfigure Messages on page 292](#)
- [Example: Extended DHCPv6 Local Server Configuration on page 292](#)

DHCPv6 Local Server Overview

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

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

- Client username
- Client password



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

Based on the attributes that the DHCPv6 local server provides, RADIUS returns the information listed in [Table 39 on page 288](#) to configure the client:

Table 39: RADIUS Attributes and VSAs for DHCPv6 Local Server

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

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

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

- Configuration for a specific interface or for a group of interfaces
- Site-specific usernames and passwords
- Numbered Ethernet interfaces
- Statically configured CoS and filters
- AAA directed login
- Use of the IA_NA option to assign a specific address to a client

To configure the extended DHCPv6 local server on the router (or switch), you include the **dhcpv6** statement at the **[edit system services dhcp-local-server]** hierarchy level. See the “[edit system services dhcp-local-server] Hierarchy Level” on page 617 for the complete DHCP local server syntax, including the DHCPv6 syntax.

You can also include the **dhcpv6** statement at the following hierarchy levels:

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

Related Documentation

- [Extended DHCP Local Server Overview on page 188](#)
- [Using External AAA Authentication Services with DHCP on page 217](#)
- [Grouping Interfaces with Common DHCP Configurations on page 223](#)
- [Configuring Group-Specific DHCP Local Server Options on page 225](#)
- [Overriding Default DHCP Local Server Configuration Settings on page 255](#)
- [Configuring Passwords for Usernames on page 221](#)

- [Creating Unique Usernames for DHCP Clients on page 218](#)
- [Assign a Specific IP Address to a Client Using DHCP Option 50 and DHCPv6 IA_NA Option on page 204](#)
- [Verifying and Managing DHCPv6 Local Server Configuration on page 311](#)
- [Example: Extended DHCPv6 Local Server Configuration on page 292](#)

Multiple Address Assignment for DHCPv6 Clients

Subscriber management (on the routers) or DHCP management (on the switches) enables you to assign multiple addresses to a single DHCPv6 client. Multiple address support is enabled by default, and is activated when the DHCPv6 local server receives a DHCPv6 Solicit message from a subscriber (or DHCP client) that contains multiple addresses.

For example, if you are implementing this feature on the routers, you might use the multiple address assignment feature in a networking environment in which a customer premises equipment (CPE) device requires a host address and a delegated prefix. In such an environment, you can configure subscriber management to assign both a DHCPv6 IA_NA (Identity Association for Non-Temporary Addresses) and an IA_PD (Identity Association for Prefix Delegation) address to the client (the CPE device).

- [Multiple Address Assignment Using Local Address Pools or RADIUS on page 289](#)
- [Junos OS Predefined Variable for Multiple DHCPv6 Address Assignment on page 289](#)

Multiple Address Assignment Using Local Address Pools or RADIUS

You can use either local address pools or RADIUS when assigning multiple addresses to a DHCP client. When at least one address is successfully allocated, the router or switch creates a subscriber (or DHCP client) entry and binds the entry to the assigned address. If both addresses are successfully allocated, the router (or switch) creates a single subscriber (or DHCP client) entry and binds both addresses to that entry.

You can also configure a delegated address pool, which explicitly specifies the address pool that subscriber management (or DHCP management) uses to assign IPv6 prefixes for subscribers (or DHCP clients).

Junos OS Predefined Variable for Multiple DHCPv6 Address Assignment



NOTE: EX Series switches do not support demux.

(On the routers only) Subscriber management provides a predefined variable that you can use to dynamically configure DHCPv6 multiple address assignment. You apply the Junos OS predefined variable, `$junos-subscriber-ipv6-multi-address`, as a demux source address in a dynamic profile. When the dynamic profile is attached to a subscriber, the variable is expanded to include both the host and prefix addresses. You use this variable

instead of the `$junos-subscriber-ipv6-address` variable, which supports a single IPv6 address.

You include the `$junos-subscriber-ipv6-multi-address` variable at the `[edit dynamic-profile profile-name interfaces interface-name unit logical-unit-number family inet6 demux-source]` hierarchy level.

**Related
Documentation**

- [Specifying the Delegated Address Pool for IPv6 Prefix Assignment on page 290](#)
- [Junos OS Predefined Variables](#)

DHCPv6 Options in a DHCPv6 Multiple Address Environment

In a DHCPv6 environment, DHCPv6 clients can use a single DHCPv6 Solicit message to request multiple addresses (for example, IA_NA address, IA_PD address, or both), as well as the DNS server address (DHCPv6 attribute 23). When a client requests multiple addresses, DHCPv6 uses the following guidelines to determine how options are returned to the client.

- **DNS server address**—Whenever a client requests an IA_PD address (either alone or with an IA_NA address) and also requests a DNS server address, DHCPv6 returns a DNS address only when one is specified in the IA_PD pool. If the IA_PD pool does not include a DNS address, DHCPv6 ignores any DNS address configured in the IA_NA pool.

If the client requests an IA_NA address (but not an IA_PD address) and also a DNS server address, DHCPv6 returns a DNS address if one is configured in the IA_NA pool.
- **Lease time**—DHCPv6 returns the shortest value of the lease times configured in the IA_NA pool, the IA_PD pool, and **authd**. DHCPv6 uses this value to set the lifetimes and the Renew and Rebind timers.



NOTE: By default, DHCPv6 local server returns the DNS server address as a global DHCPv6 option. You can override the current default behavior if you want DHCPv6 to return the DNS server address at the suboption level.

**Related
Documentation**

- [Overriding How the DNS Server Address Is Returned in a DHCPv6 Multiple Address Environment on page 326](#)
- [Multiple Address Assignment for DHCPv6 Clients on page 289](#)

Specifying the Delegated Address Pool for IPv6 Prefix Assignment

You can explicitly specify a delegated address pool:

- **On routers**—Subscriber management uses the pool to assign IPv6 prefixes for subscribers. You can specify the delegated address pool globally, for a specific group of interfaces, or for a particular interface.

- On switches—DHCP management uses the pool to assign IPv6 prefixes for DHCP clients. You can specify the delegated address pool globally, for a specific group of interfaces, or for a particular interface.



NOTE: You can also use by Juniper Networks VSA 26-161 to specify the delegated address pool. The VSA-specified value always takes precedence over the **delegated-address** statement.

To configure the delegated address pool for DHCPv6 local server:

1. Specify that you want to configure override options.

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

2. Configure the delegated address pool.

```
[edit system services dhcp-local-server dhcpv6 overrides]
user@host# set delegated-pool paris-cable-12
```

Related Documentation

- [Overriding Default DHCP Local Server Configuration Settings on page 255](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 258](#)
- [Extended DHCP Local Server Overview on page 188](#)
- [Extended DHCP Relay Agent Overview on page 194](#)

Enabling DHCPv6 Rapid Commit Support

You can configure the extended DHCPv6 local server to support the DHCPv6 Rapid Commit option (DHCPv6 option 14). When rapid commit is enabled on the extended DHCPv6 local server, the server recognizes the Rapid Commit option in Solicit messages sent from the DHCPv6 client. (DHCPv6 clients are configured separately to include the DHCPv6 Rapid Commit option in the Solicit messages.) The server and client then use a two-message exchange (Solicit and Reply) to configure clients, rather than the default four-method exchange (Solicit, Advertise, Request, and Reply). The two-message exchange provides faster client configuration, and is beneficial in environments in which networks are under a heavy load.

You can configure the DHCPv6 local server to support the Rapid Commit option globally, for a specific group, or for a specific interface. By default, rapid commit support is disabled on the DHCPv6 local server.

To configure the DHCPv6 local server to support the DHCPv6 Rapid Commit option:

1. Specify that you want to configure the **overrides** options.

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

2. Enable rapid commit support.

```
[edit system services dhcp-local-server dhcpv6 overrides]
user@host# set rapid-commit
```

**Related
Documentation**

- [Overriding Default DHCP Local Server Configuration Settings on page 255](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 258](#)
- [Extended DHCP Local Server Overview on page 188](#)

Preventing Binding of Clients That Do Not Support Reconfigure Messages

The DHCPv6 client and server negotiate the use of reconfigure messages. When the client can accept reconfigure messages from the server, then the client includes the Reconfigure Accept option in both solicit and request messages sent to the server.

By default, the DHCPv6 server accepts solicit messages from clients regardless of whether they support reconfiguration. You can specify that the server require clients to accept reconfigure messages. In this case, the DHCPv6 server includes the Reconfigure Accept option in both advertise and reply messages when reconfiguration is configured for the client interface. Solicit messages from nonsupporting clients are discarded and the clients are not allowed to bind.

(Optional) To configure the DHCPv6 local server to require that all clients accept reconfiguration:

- Specify strict reconfiguration.

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set strict
```

To override the global configuration for a particular group of clients, include the statement at the `[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]` hierarchy level.

The `show dhcpv6 server statistics` command displays a count of solicit messages that the server has discarded.

**Related
Documentation**

- [Configuring Dynamic Client Reconfiguration of Extended Local Server Clients on page 244](#)
- [strict on page 935](#)

Example: Extended DHCPv6 Local Server Configuration

This example shows a sample extended DHCPv6 local server configuration. The second part of the example shows a sample RADIUS authentication configuration—authentication must be configured for DHCPv6 local server operations.

```
[edit system services]
dhcp-local-server {
  dhcpv6 {
    authentication {
      password v679M8vt;
```



```

        username-include {
            user-prefix wallybrown;
            domain-name isp55.com;
        }
    }
    group group_two {
        authentication {
            password P$55qw4$$;
            username-include {
                user-prefix south5;
                domain-name isp55.com;
            }
        }
    }
    interface ge-1/0/3.0;
}
}
}

```

The following is a sample RADIUS authentication configuration.

```

[edit access]
radius-server {
    192.168.1.250 {
        port 1812;
        secret &t!UEI*7688+;
    }
}
profile isp-bos-metro-fiber-basic {
    accounting-order radius;
    authentication-order radius;
    radius {
        authentication-server 192.168.1.250;
        accounting-server 192.168.1.250;
    }
    accounting {
        order radius;
        accounting-stop-on-failure;
        accounting-stop-on-access-deny;
        update-interval 10;
        statistics time;
    }
}
}

```

Related Documentation

- [DHCPv6 Local Server Overview on page 287](#)

Configuring DHCPv6 Relay Agent

- [DHCPv6 Relay Agent Options on page 295](#)
- [Configuring DHCPv6 Relay Agent Options on page 296](#)
- [Inserting DHCPv6 Interface-ID Option \(Option 18\) In DHCPv6 Packets on page 297](#)
- [Inserting DHCPv6 Remote-ID Option \(Option 37\) In DHCPv6 Packets on page 298](#)

DHCPv6 Relay Agent Options

Subscriber management enables you to configure DHCPv6 relay agent to include additional information in the client-originated DHCP packets that the relay forwards to a DHCPv6 server. This support is equivalent to the option 82 support provided by the DHCPv4 relay agent. The DHCPv6 server uses the additional information in the packets to determine the IPv6 address to assign to the client. The server might also use the information for other purposes; for example, to determine which services to grant the client, or to provide additional security against threats such as address spoofing. The DHCPv6 server sends its reply back to the DHCPv6 relay agent, and the agent removes the option information from the message, and then forwards the packet to the client.

You can configure the DHCPv6 relay agent to include the following options in the packet the relay sends to the DHCPv6 server:

- Relay Agent Interface-ID (option 18)—An ASCII string that identifies the interface on which the client DHCPv6 packet is received. This is the equivalent of the DHCPv4 relay agent option 82 Agent Circuit ID suboption (suboption 1).
- Relay Agent Remote-ID (option 37)—An ASCII string assigned by the DHCPv6 relay agent that securely identifies the client. This is the equivalent of the DHCPv4 relay agent option 82 Agent Remote ID suboption (suboption 2).

**Related
Documentation**

- [Configuring DHCPv6 Relay Agent Options on page 296](#)
- [Inserting DHCPv6 Interface-ID Option \(Option 18\) In DHCPv6 Packets on page 297](#)
- [Inserting DHCPv6 Remote-ID Option \(Option 37\) In DHCPv6 Packets on page 298](#)

Configuring DHCPv6 Relay Agent Options

You can configure DHCPv6 relay agent to insert optional information in the DHCPv6 packets that the relay receives from clients and forwards to a DHCPv6 server. To configure the optional information, you specify the type of information you want to include in the packets. You use the **relay-agent-interface-id** statement to include the Relay Agent Interface-ID (option 18) in the packets, or the **relay-agent-remote-id** statement to include the Relay Agent Remote-ID (option 37).

When you enable the DHCPv6 options support, you can optionally configure DHCPv6 relay agent to include a prefix, the interface description, or VLAN ID as part of the option information. If you configure the DHCPv6 options but do not include either the optional prefix or interface description, the format of the Relay Agent Interface-ID or Relay Agent Remote-ID information for Fast Ethernet (**fe**), Gigabit Ethernet (**ge**), or integrated routing and bridging (IRB) (**irb**) interfaces is one of the following, depending on your network configuration:



NOTE: IRB provides simultaneous support for Layer 2 bridging and Layer 3 IP routing on the same interface. IRB enables you to route local packets to another routed interface or to another bridging domain that has a Layer 3 protocol configured.

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

(fe | ge)-fpc/pic/port.subunit



NOTE: The *subunit* is required and used to differentiate the interface for remote systems.

- For IRB interfaces (or other pseudo devices) that do not use virtual local area networks (VLANs) or stacked VLANs (S-VLANs):

irb.subunit

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

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

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

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

To enable insertion of DHCPv6 options:

- Specify that you want to configure DHCPv6 relay agent support.

```
[edit forwarding-options dhcp-relay]
user@host# edit dhcpv6
```

2. Configure DHCPv6 relay agent to insert the Relay Agent Interface-ID option, the Relay Agent Remote-ID option, or both.

- To insert the Relay Agent Interface-ID (option 18):

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# set relay-agent-interface-id
```

- To insert the Relay Agent Remote-ID (option 37):

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# set relay-agent-remote-id
```

3. (Optional) Configure a prefix that is used in the DHCPv6 option information in the DHCPv6 packets

See [“Including a Prefix in DHCP Options” on page 269](#).

4. (Optional) Configure DHCPv6 relay agent to include the interface's textual description instead of interface identifier in the DHCPv6 option information.

See [“Including a Textual Description in DHCP Options” on page 271](#).

Related Documentation

- [Inserting DHCPv6 Interface-ID Option \(Option 18\) In DHCPv6 Packets on page 297](#)
- [Inserting DHCPv6 Remote-ID Option \(Option 37\) In DHCPv6 Packets on page 298](#)
- [Including a Prefix in DHCP Options on page 269](#)
- [Including a Textual Description in DHCP Options on page 271](#)

Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets

You can configure DHCPv6 relay agent to insert the DHCPv6 Interface-ID (option 18) in the packets that the relay sends to a DHCPv6 server. You can configure the option 18 support at either the DHCPv6 global or group level.

When you configure option 18 support, you can optionally include the following additional information:

- Prefix—Specify the **prefix** option to add a prefix to the interface identifier. The prefix can be any combination of hostname, logical system name, and routing instance name.
- Interface description—Specify the **use-interface-description** option to include the textual interface description instead of the interface identifier. You can include either the device interface description or the logical interface description.
- Option 82 Agent Circuit ID suboption (suboption 1)—Specify the **use-option-82** option to include the DHCPv4 Option 82 Agent Circuit ID suboption (suboption 1). This configuration is useful in a dual-stack environment, which has both DHCPv4 and DHCPv6 subscribers that reside over the same underlying logical interface. The router checks for the option 82 suboption 1 value and inserts it into the outgoing packets. If no DHCPv4 binding exists or if the binding does not have an option 82 suboption 1 value, the router sends the packets without adding an option 18.



NOTE: If you specify one of the optional configurations, and the specified information does not exist (for example, there is no interface description), DHCPv6 relay ignores the optional configuration and inserts the default interface identifier in the packets.

To insert the DHCPv6 Interface-ID option (option 18) in DHCPv6 packets:

1. Configure the DHCPv6 relay to include option 18.

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-interface-id
```

2. (Optional) Specify the prefix to include in option 18.

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set prefix prefix
```

3. (Optional) Specify that option 18 include the textual description of the interface. You can specify either the **logical** interface description or the **device** interface description.

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set use-interface-description (logical | device)
```

4. (Optional) Specify that option 18 use the DHCPv4 Option 82 Agent Circuit ID suboption (suboption 1) value.

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set use-option-82
```

Related Documentation

- [DHCPv6 Relay Agent Options on page 295](#)
- [Configuring DHCPv6 Relay Agent Options on page 296](#)
- [Including a Prefix in DHCP Options on page 269](#)
- [Including a Textual Description in DHCP Options on page 271](#)

Inserting DHCPv6 Remote-ID Option (Option 37) In DHCPv6 Packets

You can configure DHCPv6 relay agent to insert the DHCPv6 Remote-ID (option 37) in the packets that the relay sends to a DHCPv6 server. You can configure the option 37 support at either the DHCPv6 global or group level.

When you configure option 37 support, you can optionally include the following additional information:

- **Prefix**—Specify the **prefix** option to add a prefix to the interface identifier. The prefix can be any combination of hostname, logical system name, and routing instance name.
- **Interface description**—Specify the **use-interface-description** option to include the textual interface description instead of the interface identifier. You can include either the device interface description or the logical interface description.



NOTE: If you specify one of the optional configurations, and the specified information does not exist (for example, there is no interface description), DHCPv6 relay ignores the optional configuration and inserts the default interface identifier in the packets.

To insert the DHCPv6 Remote-ID option (option 37) in DHCPv6 packets:

1. Configure the DHCPv6 relay to include option 37.

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-remote-id
```

2. (Optional) Specify the prefix to include with the option 37 information.

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id]
user@host# set prefix prefix
```

3. (Optional) Specify that option 37 include the textual description of the interface. You can specify either the **logical** interface description or the **device** interface description.

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id]
user@host# set use-interface-description (logical | device)
```

Related Documentation

- [DHCPv6 Relay Agent Options on page 295](#)
- [Configuring DHCPv6 Relay Agent Options on page 296](#)

CHAPTER 35

Protecting the Routing Engine Using DHCP Firewall Filters

- [Example: Configuring a DHCP Firewall Filter to Protect the Routing Engine on page 301](#)
- [Port Number Requirements for DHCP Firewall Filters on page 305](#)

Example: Configuring a DHCP Firewall Filter to Protect the Routing Engine

This example shows how to configure a firewall filter to ensure that proper DHCP packets can reach the Routing Engine on MX Series routers.

- [Requirements on page 301](#)
- [Overview on page 301](#)
- [Configuration on page 302](#)
- [Verification on page 304](#)

Requirements

This configuration example applies only to routers where DHCP local server and DHCP relay agent services are provided by the `jdhcpd` process rather than the legacy `dhcpcd` process or `fud` (UDP forwarding) process. MX Series routers, M120 routers, and M320 routers use `jdhcpd`. For DHCP relay, that means the configuration is required only at the **[edit forwarding-options dhcp-relay]** hierarchy level and not at the **[edit forwarding-options helpers bootp]** hierarchy level.

No special configuration beyond device initialization is required before you can configure this feature.

Overview

Firewall filters that perform some action on DHCP packets at the Routing Engine, such as a filter to protect the Routing Engine by allowing only proper DHCP packets, require that both port 67 (bootps) and port 68 (bootpc) are configured as both source and destination ports.

DHCP packets received on the line cards are encapsulated by `jdhcpd` with a new UDP header where their source and destination addresses are set to port 68 before being forwarded to the Routing Engine. For DHCP relay and DHCP proxy, packets sent to the

DHCP server from the router have both the source and destination UDP ports set to 67. The DHCP server responds using the same ports. However, when the line card receives these DHCP response packets, it changes both port numbers from 67 to 68 before passing the packets to the Routing Engine. Consequently the filter needs to accept port 67 for packets relayed from the client to the server, and port 68 for packets relayed from the server to the client.

In this example, you configure two filter terms, **dhcp-client-accept** and **dhcp-server-accept**. The match conditions for **dhcp-client-accept** specify a source address and destination address for broadcast packets, the UDP protocol used for DHCP packets, and the bootpc (68) source port and bootps (67) destination port. Packets that match these conditions are counted and accepted.

The match conditions for **dhcp-server-accept** specify the UDP protocol used for DHCP packets, and both port 67 and 68 for both source port and destination port. Packets that match these conditions are counted and accepted.



NOTE: This example does not show all possible configuration choices, nor does it show how the filter is applied in your configuration. This example applies to both static application of the filter as well as dynamic application with a dynamic profile.

Configuration

CLI Quick Configuration

To quickly configure the sample Routing Engine DHCP filter, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

```
[edit]
edit firewall family inet filter RE-protect
edit term dhcp-client-accept
set from source-address 0.0.0.0/32
set from destination-address 255.255.255.255/32
set from protocol udp
set from source-port 68
set from destination-port 67
set then count dhcp-client-accept
set then accept
up
edit term dhcp-server-accept
set from protocol udp
set from source-port 67
set from source-port 68
set from destination-port 67
set from destination-port 68
set then count dhcp-server-accept
set then accept
top
```

Step-by-Step Procedure The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure a DHCP firewall filter to protect the Routing Engine:

1. Create or specify a firewall filter.

```
[edit firewall]
user@host# edit family inet filter RE-protect
```
2. Create a filter term for the client.

```
[edit firewall family inet filter RE-protect]
user@host# edit term dhcp-client-accept
```
3. Specify the match conditions for DHCP packets.

```
[edit firewall family inet filter RE-protect term dhcp-client-accept]
user@host# set from source-address 0.0.0.0/32
user@host# set from destination-address 255.255.255.255/32
user@host# set from protocol udp
user@host# set from source-port 68
user@host# set from destination-port 67
```
4. Specify the action to take for matched packets.

```
[edit firewall family inet filter RE-protect term dhcp-client-accept]
user@host# set then count dhcp-client-accept
user@host# set then accept
```
5. Create a filter term for the server.

```
[edit firewall family inet filter RE-protect]
user@host# edit term dhcp-server-accept
```
6. Specify the match conditions for DHCP packets.

```
[edit firewall family inet filter RE-protect term dhcp-server-accept]
user@host# set from protocol udp
user@host# set from source-port [67 68]
user@host# set from destination-port [67 68]
```
7. Specify the action to take for matched packets.

```
[edit firewall family inet filter RE-protect term dhcp-server-accept]
user@host# set then count dhcp-client-accept
user@host# set then accept
```

Results From configuration mode, confirm your configuration by entering the **show firewall** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show firewall
family inet {
  filter RE-protect {
    term dhcp-client-accept {
      from {
        source-address {
```

```

        0.0.0.0/32;
    }
    destination-address {
        255.255.255.255/32;
    }
    protocol udp;
    source-port 68;
    destination-port 67;
}
then {
    count dhcp-client-accept;
    accept;
}
}
term dhcp-server-accept {
    from {
        protocol udp;
        source-port [ 67 68 ];
        destination-port [ 67 68 ];
    }
    then {
        count dhcp-server-accept;
        accept;
    }
}
}
}
}

```

If you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the Routing Engine DHCP protection filter is properly passing DHCP packets, perform these tasks:

- [Verifying the DHCP Filter Operation on page 304](#)

Verifying the DHCP Filter Operation

Purpose Verify that both counters increment as DHCP traffic passes to the Routing Engine.

Action From operational mode, enter the **show firewall family inet filter RE-protect** command.

```
user@host> show firewall family inet filter RE-protect
```

```
Filter: RE-protect
```

```
Counters:
```

Name	Bytes	Packets
dhcp-client-accept	328	1
dhcp-server-accept	574	1

```
user@host> show firewall family inet filter RE-protect
```

```
Filter: RE-protect
```

```
Counters:
```

Name	Bytes	Packets
dhcp-client-accept	660	2
dhcp-server-accept	1152	2

Meaning The output lists both configured counters, dhcp-client-accept and dhcp-server-accept. By issuing the command more than once, you can see that the byte and packet fields both show that traffic is being accepted and counted.

- Related Documentation**
- [Port Number Requirements for DHCP Firewall Filters on page 305](#)
 - [Understanding Dynamic Firewall Filters](#)
 - [Firewall Filters Overview](#)
 - [Extended DHCP Local Server Overview on page 188](#)
 - [Extended DHCP Relay Agent Overview on page 194](#)

Port Number Requirements for DHCP Firewall Filters

When you configure a firewall filter to perform some action on DHCP packets at the Routing Engine, such as protecting the Routing Engine by allowing only proper DHCP packets, you must specify both port 67 (bootps) and port 68 (bootpc) for both the source and destination. The firewall filter acts at both the line cards and the Routing Engine.

This requirement applies to both DHCP local server and DHCP relay, but it applies only when DHCP is provided by the jdhcpd process. MX Series routers, M120 routers, and M320 routers use jdhcpd. For DHCP relay, that means the configuration is required only at the **[edit forwarding-options dhcp-relay]** hierarchy level and not at the **[edit forwarding-options helpers bootp]** hierarchy level.

DHCP packets received on the line cards are encapsulated by jdhcpd with a new UDP header where their source and destination addresses are set to port 68 before being forwarded to the Routing Engine.

For DHCP relay and DHCP proxy, packets sent to the DHCP server from the router have both the source and destination UDP ports set to 67. The DHCP server responds using the same ports. However, when the line card receives these DHCP response packets, it changes both port numbers from 67 to 68 before passing the packets to the Routing Engine. Consequently the filter needs to accept port 67 for packets relayed from the client to the server, and port 68 for packets relayed from the server to the client.

Failure to include both port 67 and port 68 as described here results in most DHCP packets not being accepted.

For information about firewall filters, see *Firewall Filters Overview*.

- Related Documentation**
- [Example: Configuring a DHCP Firewall Filter to Protect the Routing Engine on page 301](#)
 - [Extended DHCP Local Server Overview on page 188](#)
 - [Extended DHCP Relay Agent Overview on page 194](#)
 - [Understanding Dynamic Firewall Filters](#)

Monitoring and Managing DHCP

- [Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings on page 307](#)
- [Clearing DHCP Bindings for Subscriber Access on page 308](#)
- [Displaying a Count of DHCP Packets That Are Dropped or Forwarded During Selective Processing That Is Based on DHCP Option Strings on page 310](#)
- [Monitoring DHCP Relay Server Responsiveness on page 310](#)
- [Verifying and Managing DHCP Local Server Configuration on page 311](#)
- [Verifying and Managing DHCPv6 Local Server Configuration on page 311](#)
- [Verifying and Managing DHCP Relay Configuration on page 312](#)
- [Verifying and Managing DHCPv6 Relay Configuration on page 312](#)

Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings

You can request that the DHCP local server initiate reconfiguration of all of clients or only specified clients.

To request reconfiguration of all clients:

- Specify the **all** option.

For DHCPv4:

```
user@host> request dhcp server reconfigure all
```

For DHCPv6:

```
user@host> request dhcpv6 server reconfigure all
```

You can use any of the following methods to request reconfiguration of specific clients:

- Specify the IP address of the DHCP client.

For DHCPv4:

```
user@host> request dhcp server reconfigure 192.168.27.3
```

For DHCPv6:

```
user@host> request dhcpv6 server reconfigure 2001:bd8:1111:2222::
```

- Specify the client ID of a DHCPv6 client.

```
user@host> request dhcpv6 server reconfigure
LL_TIME0x1-0x2e159c0-00:10:94:00:00:02
```

- Specify the session ID of a DHCPv6 client.

```
user@host> request dhcpv6 server reconfigure 5
```

- Specify the MAC address of a DHCPv4 client.

```
user@host> request dhcp server reconfigure 12:23:34:45:56:67
```

- Specify an interface; reconfiguration is attempted for all clients on this interface.

```
user@host> request dhcp server reconfigure interface fe-0/0/0.100
```

- Specify a logical system; reconfiguration is attempted for all clients or the specified clients in this logical system.

```
user@host> request dhcp server reconfigure all logical-system ls-bldg5
```

- Specify a routing instance; reconfiguration is attempted for all clients or the specified clients in this routing instance.

```
user@host> request dhcp server reconfigure all routing-instance ri-boston
```

Related Documentation

- [Configuring Dynamic Client Reconfiguration of Extended Local Server Clients on page 244](#)
- [request dhcp server reconfigure on page 1036](#)

Clearing DHCP Bindings for Subscriber Access

This topic provides the procedure you use to display current DHCP bindings, clear selected bindings, and verify that the specified bindings are successfully cleared.

Subscriber management enables you to clear DHCP bindings at several different levels for DHCP local server and DHCP relay agent. For example, you can clear the DHCP bindings on all interfaces, a group of interfaces, or a specific interface. You can also clear DHCP bindings based on IP address, MAC address, session-ID, DHCPv6 prefix, DHCPv6 Client ID, FPC, PIC, port, VLAN, or stacked VLAN (S-VLAN).

This topic includes examples to show several variations of the clear DHCP binding feature. The examples use DHCP local server commands; however, the procedure and commands are similar for DHCP relay agent, DHCPv6 local server, and DHCPv6 relay agent.

To clear bindings and verify the results for a specific IP address:

1. Display current bindings. Issue the appropriate variation of the **show dhcp server binding** command.

```
user@host> show dhcp server binding
2 clients, (2 bound, 0 selecting, 0 renewing, 0 rebinding)
```

IP address	Hardware address	Type	Lease expires at
192.168.32.1	90:00:00:01:00:01	active	2011-10-17 11:38:47 PST
192.168.32.3	90:00:00:02:00:01	active	2011-00-17 11:38:41 PST

2. Clear the binding you want to remove.


```
user@host> clear dhcp server binding 192.168.32.1
```

3. Verify that the binding has been cleared.

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

```
1 clients, (1 bound, 0 selecting, 0 renewing, 0 rebinding)
```

IP address	Hardware address	Type	Lease expires at
192.168.32.3	90:00:00:02:00:01	active	2011-00-17 11:38:41 PST

The following examples show variations of the clear DHCP binding feature. The examples use the DHCP local server version of the commands.



NOTE: IP demux interfaces are not supported by the show and clear DHCP bindings commands for DHCP local server and DHCP relay agent.

To clear all bindings:

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

To clear bindings on a specific interface:

```
user@host> clear dhcp server binding interface fe-0/0/2
```

To clear all bindings over an interface. This example uses the wildcard option.

```
user@host> clear dhcp server binding ge-1/0/0.*
```

To clear bindings on top of a specific VLAN. This example clears all bindings on top of VLAN 100.

```
user@host> clear dhcp server binding ge-1/0/0:100
```

To clear bindings for a specific S-VLAN. This example clears bindings on S-VLAN 100-200.

```
user@host> clear dhcp server binding ge-1/0/0:100-200
```

To clear all bindings on top of all demux VLANs:

```
user@host> clear dhcp server binding demux0
```

To clear all bindings on top of an underlying interface. This example clears the bindings on all demux VLANs on top of interface ae0:

```
user@host> clear dhcp server binding ae0
```

To clear PPP bindings. This example uses the wildcard feature and clears the PPP bindings over interface pp0.100 and pp0.200.

```
user@host> clear dhcp server binding pp0.*
```

To clear all bindings on an FPC. This example uses the wildcard feature and clears all DHCP bindings on FPC 1.

```
user@host> clear dhcp server binding ge-1/*
```

To clear all bindings on a PIC. This example uses the wildcard feature and clears all DHCP bindings on FPC 1, PIC 0.

```
user@host> clear dhcp server binding ge-1/0/*
```

To clear all bindings on a port. This example uses the wildcard feature and clears all DHCP bindings on FPC 1, PIC 0, port 0.

```
user@host> clear dhcp server binding ge-1/0/0.*
```

**Related
Documentation**

- [DHCP Auto Logout Overview on page 249](#)
- [Automatically Logging Out DHCP Clients on page 251](#)

Displaying a Count of DHCP Packets That Are Dropped or Forwarded During Selective Processing That Is Based on DHCP Option Strings

To display the number of DHCP or DHCPv6 client packets that are dropped or forwarded during selective processing, use the following operational commands:

- [show dhcp relay statistics](#)
- [show dhcpv6 relay statistics](#)

**Related
Documentation**

- [DHCP Options and Selective Traffic Processing Overview](#)
- [Using DHCP Option Information to Selectively Process DHCP Client Traffic on page 273](#)
- [Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings on page 275](#)

Monitoring DHCP Relay Server Responsiveness

You can configure DHCP relay agent and DHCPv6 relay agent to enable the router to monitor DHCP server responsiveness. To monitor DHCP server responsiveness, you specify the length of time during which the router tracks how DHCP servers respond to relayed packets. If a configured DHCP server within the routing instance fails to respond to all relayed packets during the specified time period, the router generates the `DH_SVC_EXTERN_SERVER_STATE_CHG` system log message. When the DHCP server begins responding successfully, the router generates the log message again to indicate that responsiveness is restored. You can also use **show dhcp relay statistics** and **show dhcpv6 relay statistics** commands to display DHCP server responsiveness statistics.

The following procedure describes how to configure DHCP relay agent to enable the router to monitor DHCP server responsiveness. To configure DHCPv6 server responsiveness, include the **server-response-time** statement at the **[edit forwarding-options dhcp-relay]** hierarchy level.

To monitor DHCP server responsiveness:

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

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

2. `[edit forwarding-options dhcp-relay]`
`user@host# set server-response-time 86,400`

- Related Documentation**
- [Extended DHCP Relay Agent Overview on page 194](#)
 - [show dhcp relay statistics on page 1091](#)
 - [show dhcpv6 relay statistics on page 1108](#)

Verifying and Managing DHCP Local Server Configuration

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



NOTE: If you delete the DHCP server configuration, DHCP server bindings might still remain. To ensure that DHCP bindings are removed, issue the `clear dhcp server binding` command before you delete the DHCP server configuration.

- Action**
- To display the address bindings in the client table on the extended DHCP local server:
`user@host> show dhcp server binding routing-instance customer routing instance`
 - To display extended DHCP local server statistics:
`user@host> show dhcp server statistics routing-instance customer routing instance`
 - To clear the binding state of a DHCP client from the client table on the extended DHCP local server:
`user@host> clear dhcp server binding routing-instance customer routing instance`
 - To clear all extended DHCP local server statistics:
`user@host> clear dhcp server statistics routing-instance customer routing instance`

- Related Documentation**
- [CLI Explorer](#)

Verifying and Managing DHCPv6 Local Server Configuration

Purpose View or clear information about client address bindings and statistics for the DHCPv6 local server.

- Action**
- To display the address bindings in the client table on the DHCPv6 local server:
`user@host> show dhcpv6 server binding`
 - To display DHCPv6 local server statistics:
`user@host> show dhcpv6 server statistics`
 - To clear all DHCPv6 local server statistics:
`user@host> clear dhcpv6 server binding`

- To clear all DHCPv6 local server statistics:

user@host> [clear dhcpv6 server statistics](#)

Related Documentation • [CLI Explorer](#)

Verifying and Managing DHCP Relay Configuration

Purpose View or clear address bindings or statistics for extended DHCP relay agent clients:

- Action** • To display the address bindings for extended DHCP relay agent clients:

user@host> [show dhcp relay binding](#) routing-instance *customer routing instance*

- To display extended DHCP relay agent statistics:

user@host> [show dhcp relay statistics](#) routing-instance *customer routing instance*

- To clear the binding state of DHCP relay agent clients:

user@host> [clear dhcp relay binding](#) routing-instance *customer routing instance*

- To clear all extended DHCP relay agent statistics:

user@host> [clear dhcp relay statistics](#) routing-instance *customer routing instance*

Related Documentation • [CLI Explorer](#)

Verifying and Managing DHCPv6 Relay Configuration

Purpose View or clear address bindings or statistics for extended DHCPv6 relay agent clients:

- Action** • To display the address bindings for extended DHCPv6 relay agent clients:

user@host> [show dhcpv6 relay binding](#)

- To display extended DHCPv6 relay agent statistics:

user@host> [show dhcpv6 relay statistics](#)

- To clear the binding state of DHCPv6 relay agent clients:

user@host> [clear dhcpv6 relay binding](#)

- To clear all extended DHCPv6 relay agent statistics:

user@host> [clear dhcpv6 relay statistics](#)

Related Documentation • [CLI Explorer](#)

PART 3

Configuring Address-Assignment Pools for Subscriber Management

- [Configuring Address-Assignment Pools for Dynamic and Static Addresses on page 315](#)

CHAPTER 37

Configuring Address-Assignment Pools for Dynamic and Static Addresses

- [Address-Assignment Pools Overview on page 315](#)
- [Address-Assignment Pools Licensing Requirements on page 316](#)
- [Configuring Address-Assignment Pools on page 316](#)
- [Example: Configuring an Address-Assignment Pool on page 317](#)
- [Configuring an Address-Assignment Pool Name and Addresses on page 318](#)
- [Configuring a Named Address Range for Dynamic Address Assignment on page 319](#)
- [Configuring Address-Assignment Pool Usage Threshold Traps on page 320](#)
- [Configuring Address-Assignment Pool Linking on page 320](#)
- [Configuring Static Address Assignment on page 321](#)
- [Configuring Duplicate IPv4 Address Protection for AAA on page 322](#)

Address-Assignment Pools Overview

The address-assignment pool feature supports subscriber management and DHCP management functionality by enabling you to create centralized IPv4 and IPv6 address pools independently of the client applications that use the pools. The **authd** process manages the pools and the address allocation, whether the addresses come from local pools or from a RADIUS server. For example, multiple client applications, such as DHCP, can use the same address-assignment pool to provide addresses for their particular clients. Client applications can acquire addresses for either authenticated or unauthenticated clients.

Address-assignment pools support both dynamic and static address assignment. In dynamic address assignment, a client is automatically assigned an address from the address-assignment pool. In static address assignment, which is supported for IPv4 pools only, you reserve an address that is then always used by a particular client. Addresses that are reserved for static assignment are removed from the dynamic address pool and cannot be assigned to other clients.

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

address-assignment pools, you might create a named range that is based on a specific DHCP option 82 value. Then, when a DHCP client request matches the specified option 82 value, an address from the specified range is assigned to the client.

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

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

**Related
Documentation**

- [Configuring Address-Assignment Pools on page 316](#)
- [Address-Assignment Pools Licensing Requirements on page 316](#)
- [Example: Configuring an Address-Assignment Pool on page 317](#)

Address-Assignment Pools Licensing Requirements

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

**Related
Documentation**

- [Junos OS Feature Licenses](#)

Configuring Address-Assignment Pools

The address-assignment pool feature supports subscriber management functionality by enabling you to create address pools that can be shared by different client applications. An address-assignment pool can support either IPv4 address or IPv6 addresses. You cannot use the same pool for both types of address.



NOTE: Address-assignment pools are completely separate from services PIC-based L2TP LNS address pools, which you create with the `address-pool` statement at the `[edit access]` hierarchy level, and NAT pools, which you create with the `pool` statement at the `[edit services nat]` hierarchy level.

To configure an address-assignment pool:

1. Configure the address-assignment pool name and specify the addresses for the pool.
See [“Configuring an Address-Assignment Pool Name and Addresses” on page 318](#).
2. (Optional) Configure named ranges (subsets) of addresses.
See [“Configuring a Named Address Range for Dynamic Address Assignment” on page 319](#).
3. (Optional) Configure address-assignment pool linking and specify the secondary pool to use when the primary pool is fully allocated.

See [“Configuring Address-Assignment Pool Linking” on page 320](#).

4. (Optional) Create static address bindings (IPv4 only).

See [“Configuring Static Address Assignment” on page 321](#).

5. (Optional) Configure attributes for DHCP clients.

See [“Configuring DHCP Client-Specific Attributes Applied When Clients Obtain an Address” on page 205](#).

6. (Optional) Specify that the address-assignment pool is used for router advertisement.

See [Configuring an Address-Assignment Pool for Router Advertisement](#).

Related Documentation

- [Address-Assignment Pools Overview on page 315](#)
- [Address-Assignment Pools Licensing Requirements on page 316](#)
- [Example: Configuring an Address-Assignment Pool on page 317](#)

Example: Configuring an Address-Assignment Pool

This example shows an address-assignment pool configuration that creates two pools, one for IPv4 DHCP clients (**isp_1**), and a second pool (**chi-fiber-ra**) that is used for router advertisement.

```
[edit access]
address-assignment {
  network-discovery-router-advertisement chi-fiber-ra;
  pool isp_1 {
    family inet {
      network 192.168.0.0/16;
      range southeast {
        low 192.168.102.2 high 192.168.102.254;
      }
      range northeast {
        low 192.168.119.2 high 192.168.119.250;
      }
    }
    host svale6.boston.net {
      hardware-address 90:00:00:01:00:01;
      ip-address 192.168.44.12;
    }
    dhcp-attributes {
      option-match {
        option-82 {
          circuit-id fiber range northeast;
        }
        option-82 {
          circuit-id cable_net range southeast;
        }
      }
    }
    boot-file boot.client;
    boot-server 192.168.200.100;
    grace-period 3600;
    maximum-lease-time 18000;
  }
}
```

```
        netbios-node-type p-node;
        router 192.168.44.44 192.168.44.45;
    }
}
}
pool chi-fiber-ra {
    family inet6 {
        prefix 2008:2009:2010::/48;
        range fiber3 {
            low 2008:2009:2010::1/64;
            high 2008:2009:2010::5/64;
        }
    }
}
```

This example creates an IPv4 address-assignment pool named **isp-1**, which contains two named address ranges, **southeast** and **northeast**. The address-assignment pool also contains a static binding for client **host sval6.boston.net**. The **ISP_1** pool configuration also includes the **dhcp-attributes** statement, indicating that the pool is used for DHCP clients. If the option 82 **circuit-id** entry matches the string **fiber**, then DHCP assigns the client an address from the **northeast** range. If the option 82 **circuit-id** matches the string **cable_net**, DHCP assigns an address from the **southeast** range.

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

- Related Documentation**
- [Address-Assignment Pools Overview on page 315](#)
 - [Configuring Address-Assignment Pools on page 316](#)

Configuring an Address-Assignment Pool Name and Addresses

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

To configure an IPv4 address-assignment pool:

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

[edit access]

user@host# edit **address-assignment pool** isp_1 family inet

2. Configure the network address and the prefix length of the addresses in the pool.

[edit access address-assignment pool isp_1 family inet]

user@host# set **network** 192.168.0.0/16

To configure an IPv6 address-assignment pool:

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

[edit access]

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

2. Configure the IPv6 network prefix for the address pool. The prefix specification is required when you configure an IPv6 address-assignment pool.

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

**Related
Documentation**

- [Address-Assignment Pools Overview on page 315](#)
- [Configuring Address-Assignment Pools on page 316](#)

Configuring a Named Address Range for Dynamic Address Assignment

You can optionally configure multiple named ranges, or subsets, of addresses within an address-assignment pool. During dynamic address assignment, a client can be assigned an address from a specific named range. To create a named range, you specify a name for the range and define the address range.

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

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

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

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

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

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

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

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

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

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

**Related
Documentation**

- [Address-Assignment Pools Overview on page 315](#)
- [Configuring Address-Assignment Pools on page 316](#)

Configuring Address-Assignment Pool Usage Threshold Traps

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

To set the usage for threshold traps:

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

[edit access]

user@host# edit address-assignment high-utilization 95

To set the abated value for the trap:

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

[edit access]

user@host# edit address-assignment abated-utilization 80

Related Documentation

- [Address-Assignment Pools Overview on page 315](#)

Configuring Address-Assignment Pool Linking

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

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

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

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

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

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

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

**Related
Documentation**

- [Address-Assignment Pools Overview on page 315](#)
- [Address-Assignment Pools Licensing Requirements on page 316](#)

Configuring Static Address Assignment

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

To configure a static binding for an IPv4 address:

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

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

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

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

**Related
Documentation**

- [Address-Assignment Pools Overview on page 315](#)
- [Configuring Address-Assignment Pools on page 316](#)

Configuring Duplicate IPv4 Address Protection for AAA

If you are using AAA to supply IPv4 addresses, you can enable duplicate address protection to prevent addresses from being used more than once. If enabled, the following attributes received from external servers are checked:

- *Framed-IP-Address*
- *Framed-Pool*

The router then takes one of the following actions:

- If an address matches an address in an address pool, the address is taken from the pool, provided it is available.
- If the address is already in use, it is rejected as unavailable.

To configure duplicate address protection:

1. Enter the **access** configuration.

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

2. Enable duplicate address protection.

```
[edit access]  
user@host# address-protection
```

Related Documentation

- *Configuring Duplicate Prefix Protection for Router Advertisement*

PART 4

Configuring DNS Addresses for Subscriber Management

- [Configuring DNS Address Assignments and Session Options on page 325](#)

Configuring DNS Address Assignments and Session Options

- [Configuring DNS Name Server Addresses for Subscriber Management on page 325](#)
- [Overriding How the DNS Server Address Is Returned in a DHCPv6 Multiple Address Environment on page 326](#)

Configuring DNS Name Server Addresses for Subscriber Management

This topic describes the procedure for configuring DNS name server addresses at the access profile and routing instance levels. For information about configuring addresses in DHCP address pools, see the DHCP topics referenced in the *Related Documentation* section. For information about configuring addresses on your RADIUS server, refer to your RADIUS software documentation. The order in which the name server configurations at different levels are preferred is described in *DNS Name Server Address Overview*.



BEST PRACTICE: In practice, choose either the `domain-name-server` statement or the `domain-name-server-inet` statement for IPv4 addresses. They both have the same effect and there is no need to use both statements. If you do use both statements, addresses configured with `domain-name-server-inet` are preferred over addresses configured with `domain-name-server`.

To configure DNS name server addresses globally:

1. Configure an IPv4 address.

```
[edit access]
user@host# set domain-name-server-inet dns-address
```

Alternatively, you can use a different statement to configure an IPv4 address.

```
[edit access]
user@host# set domain-name-server dns-address
```

2. Configure an IPv6 address.

```
[edit access]
user@host# set domain-name-server-inet6 dns-address
```

For example, to configure multiple addresses of each type:

```
[edit access]
user@host# set domain-name-server-inet 172.16.25.31
user@host# set domain-name-server-inet 172.16.25.100
user@host# set domain-name-server-inet6 2001:db8:85a3::8a2e:370:81ca
user@host# set domain-name-server-inet6 2001:db8:85a3::8a2e:370:7334
```

To configure DNS name server addresses in an access profile:

1. Configure an IPv4 address.

```
[edit access profile profile-name]
user@host# set domain-name-server-inet dns-address
```

Alternatively, you can use a different statement to configure an IPv4 address.

```
[edit access profile profile-name]
user@host# set domain-name-server dns-address
```

2. Configure an IPv6 address.

```
[edit access profile profile-name]
user@host# set domain-name-server-inet6 dns-address
```

For example, to configure multiple addresses of each type:

```
[edit access profile vrf-s-access]
user@host# set domain-name-server-inet 172.20.10.01
user@host# set domain-name-server-inet 172.20.100.100
user@host# set domain-name-server-inet6 2001:db8:85a3::8a2e:370:ac81
user@host# set domain-name-server-inet6 2001:db8:85a3::8a2e:370:71bfd
```

Related Documentation

- [DNS Name Server Address Overview](#)
- [DHCP Attributes for Address-Assignment Pools on page 201](#)
- [Configuring DHCP Client-Specific Attributes Applied When Clients Obtain an Address on page 205](#)

Overriding How the DNS Server Address Is Returned in a DHCPv6 Multiple Address Environment

In a DHCPv6 environment, DHCPv6 clients can use a single Solicit message to request multiple addresses (an IA_NA address, an IA_PD address, or both), as well as the DNS server address (DHCPv6 attribute 23). By default, the DHCPv6 local server returns the DNS server address as a global DHCPv6 option.

You can override the default behavior and specify that the DHCPv6 local server returns DNS server addresses as their respective IA_NA and IA_PD suboptions. You can configure the DHCPv6 local server to support the override globally, for a specific group, or for a specific interface.



CAUTION: Some customer premises equipment (CPE) cannot recognize the DNS server address when the address is returned as an IA_NA or IA_PD suboption, which can create interoperability issues.

To configure the DHCPv6 local server to return the DNS server address as an IA_NA or IA_PD suboption.

1. Specify that you want to configure DHCPv6 override options.

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

2. Override the default behavior. DHCPv6 local server now returns DNS server addresses as the respective IA_PD or IA_NA suboption.

```
[edit system services dhcp-local-server dhcpv6 overrides]  
user@host# set multi-address-embedded-option-response
```

**Related
Documentation**

- [DHCPv6 Options in a DHCPv6 Multiple Address Environment on page 290](#)
- [Multiple Address Assignment for DHCPv6 Clients on page 289](#)
- [Overriding Default DHCP Local Server Configuration Settings on page 255](#)

PART 5

Configuring CLI-Based Subscriber Services

- [Configuring CLI-Activated Subscriber Services on page 331](#)
- [Configuring Subscriber Services with Multiple Instances on page 339](#)
- [Monitoring and Managing Subscriber Services on page 347](#)

Configuring CLI-Activated Subscriber Services

- [CLI-Activated Subscriber Services on page 331](#)
- [Activating and Deactivating Subscriber Services Locally with the CLI on page 332](#)
- [Using the CLI to Modify Traffic-Control Profiles That Are Currently Applied to Subscribers on page 335](#)

CLI-Activated Subscriber Services

Subscriber management enables you to use the Junos OS CLI to locally activate and deactivate dynamic subscriber services. CLI-based activation and deactivation provides local control for dynamic subscriber services that is similar to subscriber management's change of authorization (CoA) feature. CoA is considered a remote activation method because the commands, or triggers, are received from a remote server, such as a RADIUS or provisioning server. Both the CoA and CLI-based methods enable you to manage services for subscribers who are currently logged in to the network—you can activate a new service for the subscriber or deactivate a current service.

The CLI-based feature activates the specified service—you cannot use it to modify a subscriber's dynamic profile instantiation or to modify user-defined variables in a dynamic profile. You can, however, include variables that are defined for the service in the dynamic profile.

Subscriber management does not support accounting for CLI-activated subscriber services. Accounting for any service is disabled by default. Therefore when you use the CLI to activate a service, it is activated with accounting disabled, and there is no way to explicitly enable accounting for the service. CLI deactivation of a service previously activated (such as by RADIUS) has no effect on accounting for that service.

CLI-based activation and deactivation is useful in service provider networks that do not use provisioning servers or RADIUS servers to activate and deactivate subscriber services. The local control provided by the CLI-based operations enables service providers to add and remove services for existing subscribers without requiring that the subscriber log out and then log in again to complete the change. For example, a service provider might allow subscribers to log in and initially use the default service, which provides basic features. After the default service is established, the provider might then use CLI-activation to upgrade qualified subscribers to an advanced service, in addition to retaining the initial

service. Later, the provider can use CLI-deactivation to terminate the subscriber's advanced service session. The subscriber retains the initial service until the service is deactivated.

CLI-based activation or deactivation of a subscriber service fails if any of the following conditions exist:

- A RADIUS CoA operation or a previous CLI-based activation or deactivation is currently in progress for the subscriber. Only one dynamic request can be active for the subscriber.
- A unified in-service software upgrade (unified ISSU) operation is active.
- The specified service could not be activated or deactivated.

A CLI-based activation or deactivation of a subscriber service also fails if a PCRF has successfully activated any services for the subscriber. You must override the PCRF provisioning to be able to activate or deactivate services for such a subscriber. For more information, see [“Disabling PCRF Control of a Subscriber Session” on page 581](#).

Related Documentation

- [Activating and Deactivating Subscriber Services Locally with the CLI on page 332](#)
- [Using the CLI to Modify Traffic-Control Profiles That Are Currently Applied to Subscribers on page 335](#)
- [Default Subscriber Service Overview on page 199](#)

Activating and Deactivating Subscriber Services Locally with the CLI

Subscriber management enables you to use the Junos OS CLI to locally activate or deactivate dynamic subscriber services for subscribers who are currently logged in to the network. You can activate an initial service for the subscriber, provide an additional service, or deactivate the subscriber's current service.



NOTE:

A CLI-based activation or deactivation of a subscriber service fails if any of the following conditions exist:

- A RADIUS CoA operation or a previous CLI-based activation or deactivation is active for the subscriber.
- A unified in-service software upgrade (unified ISSU) operation is active.
- The specified service could not be activated or deactivated.

A CLI-based activation or deactivation of a subscriber service also fails if a PCRF has successfully activated any services for the subscriber. You must override the PCRF provisioning to be able to activate or deactivate services for such a subscriber. For more information, see [“Disabling PCRF Control of a Subscriber Session” on page 581](#).

To use the CLI to activate a subscriber service:

1. (Optional) Verify the subscriber's ID, and ensure that provisioning is not enabled. To display the session IDs of all current subscribers, use the **show subscribers detail** or **show network-access aaa subscribers** command.

```
user@host> show network-access aaa subscribers session-id 55 detail
Type: dhcp
Username: larry@isp5.net
Stripped username: larry
AAA Logical system/Routing instance: default:default
Target Logical system/Routing instance: default:retail-onlinecompany-ca
Access-profile:retailer-onlinecompany-sjc
Session ID: 55
Accounting Session ID: 55
Multi Accounting Session ID: 0
IP Address: 192.168.44.104
Authentication State: AuthStateActive
Accounting State: Acc-Start-Send
Provisioning-type: none
Service name: basic-service
Service State: SvcActive
Session ID: 56
Session uptime: 00:01:45
```

2. Activate the service for the subscriber.

```
user@host> request network-access aaa subscriber add session-id 55 service-profile
gold-service
```

3. (Optional) Verify that the new service is activated for the subscriber. (The initial **basic-service** is also listed because it has not been deactivated.)

```
user@host> show network-access aaa subscribers session-id 55 detail
Type: dhcp
Username: larry@isp5.net
Stripped username: larry
AAA Logical system/Routing instance: default:default
Target Logical system/Routing instance: default:retail-onlinecompany-ca
Access-profile:retailer-onlinecompany-sjc
Session ID: 55
Accounting Session ID: 55
Multi Accounting Session ID: 0
IP Address: 192.168.44.104
Authentication State: AuthStateActive
Accounting State: Acc-Start-Send
Provisioning-type: none
Service name: basic-service
Service State: SvcActive
Session ID: 56
Session uptime: 00:02:15
Service name: gold-service
Service State: SvcActive
Session ID: 57
Session uptime: 00:00:30
```

To use the CLI to deactivate a subscriber service:

1. Display the active services for the specified subscriber. The following example shows that the **basic-service** and **gold-service** are active.

```
user@host> show network-access aaa subscribers session-id 55 detail
Type: dhcp
Username: larry@isp5.net
Stripped username: larry
AAA Logical system/Routing instance: default:default
Target Logical system/Routing instance: default:retail-onlinecompany-ca
Access-profile:retailer-onlinecompany-sjc
Session ID: 55
Accounting Session ID: 55
Multi Accounting Session ID: 0
IP Address: 192.168.44.104
Authentication State: AuthStateActive
Accounting State: Acc-Start-Send
Provisioning-type: none
Service name: basic-service
  Service State: SvcActive
  Session ID: 56
  Session uptime: 00:02:15
Service name: gold-service
  Service State: SvcActive
  Session ID: 57
  Session uptime: 00:00:30
```

2. Deactivate the service for the subscriber. The following example deletes the subscriber's **basic-service** service.

```
user@host> request network-access aaa subscriber delete session-id 55 service-profile
basic-service
```

3. (Optional) Verify that the deleted service is no longer active for the subscriber. (The **gold-service** is still listed because it has not been deactivated.)

```
user@host> show network-access aaa subscribers session-id 55 detail
Type: dhcp
Username: larry@isp5.net
Stripped username: larry
AAA Logical system/Routing instance: default:default
Target Logical system/Routing instance: default:retail-onlinecompany-ca
Access-profile:retailer-onlinecompany-sjc
Session ID: 55
Accounting Session ID: 55
Multi Accounting Session ID: 0
IP Address: 192.168.44.104
Authentication State: AuthStateActive
Accounting State: Acc-Start-Send
Provisioning-type: none
Service name: gold-service
  Service State: SvcActive
  Session ID: 57
  Session uptime: 00:00:30
```

Related Documentation

- [CLI-Activated Subscriber Services on page 331](#)
- [Using the CLI to Modify Traffic-Control Profiles That Are Currently Applied to Subscribers on page 335](#)
- [Default Subscriber Service Overview on page 199](#)

Using the CLI to Modify Traffic-Control Profiles That Are Currently Applied to Subscribers

Subscriber management enables you to use the CLI to modify a traffic-control profile that is currently applied to existing subscribers. This feature allows you to update subscribers who are initially assigned the default traffic-control profile, which might have limited features.



TIP: You specify the default traffic-control profile with the **predefined-variable-defaults** statement and the **cos-traffic-control-profile** variable at the **[edit dynamic-profiles *profile-name* class-of-service]** hierarchy level.

There are two methods you can use to modify an traffic-control profile that is in use—global and per-subscriber. The global method modifies the traffic-control profile for all subscribers currently using the traffic-control profile. The per-subscriber method modifies the traffic-control profile for a particular subscriber—all other subscribers currently using the traffic-control profile remain unaffected.

The global and per-subscriber methods share the following characteristics:

- They modify traffic-control profiles that are currently applied to active subscribers.
- Neither method creates new traffic-control profiles; they modify existing traffic-control profiles that have been previously created using the **traffic-control-profiles** statement at the **[edit dynamic-profiles *profile-name* class-of-service]** hierarchy level.
- Modifications are transparent to the active subscribers who are using the modified profile. The modified traffic-control profile is assigned without requiring any action by the subscriber.
- Both methods are useful when updating subscribers who are initially assigned the default traffic-control profile, which might have limited features. You specify the default traffic-control profile with the **predefined-variable-defaults** statement and the **cos-traffic-control-profile** variable at the **[edit dynamic-profiles *profile-name* class-of-service]** hierarchy level.



NOTE: To support CLI modification of traffic-control profiles in an IPv4/IPv6 dual-stack environment, you must have the `aggregate-clients replace` statement enabled at the `[edit system services dhcp-local-server group group-name dynamic-profile profile-name]` hierarchy

This topic includes the following tasks:

- [Using the CLI to Globally Modify a Traffic-Control Profile Currently Applied to Multiple Subscribers on page 336](#)
- [Using the CLI to Modify a Traffic-Control Profile for a Specific Current Subscriber on page 336](#)

Using the CLI to Globally Modify a Traffic-Control Profile Currently Applied to Multiple Subscribers

To make a global modification for all current subscribers assigned a particular traffic-control profile, you change one or more parameters for the traffic-control profile and **commit** the changes.

In this example, the statement changes the shaping rate for the existing traffic-control profile named **TCP-silver**. After the change, the new shaping rate applies to all subscribers currently using **TCP-silver**.

1. Access the traffic-control profile you want to modify.

```
[edit dynamic-profiles business-profile class-of-service]
user@host# edit traffic-control-profiles TCP-silver
```

2. Specify the parameters that you want to modify in the traffic-control profile.

```
[edit dynamic-profiles business-profile class-of-service traffic-control-profiles
TCP-silver]
user@host# set shaping-rate 20m
```

3. Commit the configuration change to update the traffic-control profile. All current subscribers using **TCP-silver** now have the new **shaping-rate**.

Using the CLI to Modify a Traffic-Control Profile for a Specific Current Subscriber

To make a per-subscriber modification for a specific subscriber that is currently assigned a traffic-control profile, you specify the name of the new traffic-control profile to use.

In this example, the command replaces the existing traffic-control profile with the profile named **TCP-gold**. The new traffic-control profile applies only to the subscriber identified by session ID **2551**.

- Request that the traffic-control profile named **TCP-gold** be applied to session ID 2551.

```
user@host> request network-access aaa subscriber modify session-id 2551
junos-cos-traffic-control-profile TCP-gold
```

The system then displays the status message, **Successful completion**, indicating that the modification is successful. The subscriber identified by session ID 2551 now uses the **TCP-gold** traffic-control profile.

CHAPTER 40

Configuring Subscriber Services with Multiple Instances

- [Subscriber Services with Multiple Instances Overview on page 339](#)
- [Deactivating a Single Instance of a Subscriber Service with Multiple Instances on page 341](#)
- [Deactivating All Instances of a Subscriber Service with Multiple Instances on page 343](#)

Subscriber Services with Multiple Instances Overview

Services are activated for subscribers either at login, or by using Change of Authorization (CoA) RADIUS messages or command-line interface (CLI) requests. A subscriber can have multiple instances of the same named service, provided that each instance of the subscriber service has a different set of parameters. Support for multiple instances of a subscriber service enables you to use service parameters to customize the same service to meet different needs for a particular subscriber.

- [Subscriber Service Instances and Service Parameters on page 339](#)
- [CLI Deactivation of Subscriber Services with Multiple Instances on page 340](#)
- [Subscriber Services with Multiple Instances in RADIUS Accounting Messages on page 340](#)

Subscriber Service Instances and Service Parameters

In a subscriber access network, each subscriber has its own set of services. You can configure a specific *service instance* for a particular subscriber by specifying a *service name*, also referred to as a *service profile*, and unique service parameters for that service instance. *Service parameters* can include a combination of policy lists, filters, rate-limit profiles, class of service (CoS) profiles, and interface profiles.

For example, `filter-service(up-filter,down-filter)` and `filter-service(upstream-filter,downstream-filter)` are considered two different instances of the same service (`filter-service`) because their parameters, enclosed in parentheses after the service name, are different.

Each service instance is uniquely identified by the combination of its service name and service parameters. In CoA messages, the router identifies a subscriber service by its complete activation string, which consists of the service name and, if configured, one or more service parameters in the order specified.

CLI Deactivation of Subscriber Services with Multiple Instances

You can use the Junos OS CLI to deactivate subscriber services with multiple instances in either of the following ways:

- Deactivate a single instance of a subscriber service by specifying the name and parameters of the service to be deactivated.

With this feature, you can deactivate a particular instance of a subscriber service while other instances of that same service remain active. For example, assume that a subscriber identified by a particular session ID has two instances of filter-service activated: filter-service(up-filter,down-filter) and filter-service(upstream-filter,downstream-filter). If you specify “filter-service(up-filter,down-filter)” in the **request network-access aaa subscriber delete session-id** command, the router deactivates only filter-service(up-filter,down-filter); filter-service(upstream-filter,downstream-filter) remains active.

The ability to use both service names and service parameters to identify the particular service instance to be deactivated is analogous to the subscriber service deactivation feature in use on Juniper Networks E Series Broadband Services Routers that run JunosE Software.

- Deactivate all instances of a subscriber service by specifying only the name of the service to be deactivated, with no service parameters.

With this feature, you can deactivate all instances of the same subscriber service with a single operational command. Using the same subscriber service example, if you specify “filter-service” in the **request network-access aaa subscriber delete session-id** command, the router deactivates both filter-service(up-filter,down-filter) and filter-service(upstream-filter,downstream-filter).

Subscriber Services with Multiple Instances in RADIUS Accounting Messages

RADIUS Acct-Start, Interim-Acct, and Acct-Stop accounting messages include the subscriber service name and, if configured, service parameters. If RADIUS logging is enabled, the router logs all subscriber service attributes, including service names and parameters, in messages sent to and received from the RADIUS authentication server.

For example, assume that the router receives the following RADIUS Access-Accept message from the RADIUS server:

```
Jul 13 12:37:02 radius-access-accept: Activate-Service (Juniper-ERX-VSA) received:  
Tag (1) filter-service(up-filter,down-filter)
```

Table 40 on page 341 shows sample logged RADIUS Acct-Start, Interim-Acct, and Acct-Stop messages that the router sends to the RADIUS server in response to the Access-Accept message. In each of these accounting messages, the Activate-Service-Session-Name is the full activation string that includes both the service name (filter-service) and service parameters (up-filter,down-filter) to identify the service instance.

Table 40: Subscriber Services and Service Parameters in RADIUS Accounting Messages

RADIUS Accounting Message Type	RADIUS Accounting Message Text
Acct-Start	Jul 13 12:37:02 radius-acct-start: Activate-Service-Session-Name (Juniper-ERX-VSA) added: filter-service(up-filter,down-filter)
Interim-Acct	Jul 13 12:47:00 radius-acct-interim: Activate-Service-Session-Name (Juniper-ERX-VSA) added: filter-service(up-filter,down-filter)
Acct-Stop	Jul 13 12:53:59 radius-acct-stop: Activate-Service-Session-Name (Juniper-ERX-VSA) added: filter-service(up-filter,down-filter)

Related Documentation

- [Deactivating a Single Instance of a Subscriber Service with Multiple Instances on page 341](#)
- [Deactivating All Instances of a Subscriber Service with Multiple Instances on page 343](#)
- [Verifying and Managing Subscriber Services with Multiple Instances on page 347](#)

Deactivating a Single Instance of a Subscriber Service with Multiple Instances

For subscriber services that have multiple instances, you can use the Junos OS CLI to deactivate a service in either of the following ways:

- Deactivate a single instance of a service by specifying the name and parameters of the service to be deactivated.
- Deactivate all instances of a service by specifying only the name of the service to be deactivated.

This topic describes how to deactivate a single instance of a subscriber service.

To use the Junos OS CLI to deactivate a single instance of a subscriber service with multiple instances:

1. Display the active services for the subscriber identified by the specified session ID.

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

For example, the following command displays the active services for the DHCP subscriber identified by session ID 6. In this example, two instances of economy-service are active: **economy-service(up-filter,down-filter)** and **economy-service(upstrm-filter,dwnstrm-filter)**. A single instance of premium-service named **premium-service(up-filter,down-filter)** is also active.

```
user@host> show network-access aaa subscribers session-id 6 detail
Type: dhcp
Stripped username: fran2
AAA Logical system/Routing instance: default:default
Target Logical system/Routing instance: default:default
```

```

Access-profile: attr_test_profile1
Session ID: 6
Accounting Session ID: 6
Multi Accounting Session ID: 0
IP Address: 100.20.0.10
Authentication State: AuthStateActive
Accounting State: Acc-Interim-Sent
Provisioning Type: None
Service name: economy-service(up-filter,down-filter)
  Service State: SvcActive
  Service Family: inet
  Service Activation Source: Radius
  Session ID: 7
  Session uptime: 00:04:36
  Accounting status: on/volume+time
  Service accounting session ID: 6:7-1354811427
  Service accounting state: Acc-Start-Sent
  Accounting interim interval: 600
Service name: economy-service(upstrm-filter,dwnstrm-filter)
  Service State: SvcActive
  Service Family: inet
  Service Activation Source: Radius
  Session ID: 8
  Session uptime: 00:04:36
  Accounting status: on/volume+time
  Service accounting session ID: 6:8-1354811427
  Service accounting state: Acc-Start-Sent
  Accounting interim interval: 600
Service name: premium-service(up-filter,down-filter)
  Service State: SvcActive
  Service Family: inet
  Service Activation Source: Radius
  Session ID: 9
  Session uptime: 00:04:36
  Accounting status: on/volume+time
  Service accounting session ID: 6:9-1354811427
  Service accounting state: Acc-Start-Sent
  Accounting interim interval: 600

```

2. Deactivate the specified instance of a subscriber service by specifying its service name and parameters.

```

user@host> request network-access aaa subscriber delete session-id subscriber-session-id
service-profile "profile-name(parameters)"

```

For example, the following command deactivates only the instance of economy-service named economy-service(up-filter,down-filter).

```

user@host> request network-access aaa subscriber delete session-id 6 service-profile
"economy-service(up-filter,down-filter)"

```

3. (Optional) Verify that the deactivated service instance is no longer active for the subscriber.

```

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

```

For example, the following command displays the services still active for the DHCP subscriber identified by session ID 6. In this example, **economy-service(up-filter,down-filter)** is no longer listed because it was deactivated, but **economy-service(upstrm-filter,dwnstrm-filter)** and **premium-service(up-filter,down-filter)** are still active.

```

user@host> show network-access aaa subscribers session-id 6 detail

```

```

Type: dhcp
Stripped username: fran2
AAA Logical system/Routing instance: default:default
Target Logical system/Routing instance: default:default
Access-profile: attr_test_profile1
Session ID: 6
Accounting Session ID: 6
Multi Accounting Session ID: 0
IP Address: 100.20.0.10
Authentication State: AuthStateActive
Accounting State: Acc-Interim-Sent
Provisioning Type: None
Service name: economy-service(upstrm-filter,dwnstrm-filter)
  Service State: SvcActive
  Service Family: inet
  Service Activation Source: Radius
  Session ID: 8
  Session uptime: 00:04:36
  Accounting status: on/volume+time
  Service accounting session ID: 6:8-1354811427
  Service accounting state: Acc-Start-Sent
  Accounting interim interval: 600
Service name: premium-service(up-filter,down-filter)
  Service State: SvcActive
  Service Family: inet
  Service Activation Source: Radius
  Session ID: 9
  Session uptime: 00:04:36
  Accounting status: on/volume+time
  Service accounting session ID: 6:9-1354811427
  Service accounting state: Acc-Start-Sent
  Accounting interim interval: 600

```

- Related Documentation**
- [Deactivating All Instances of a Subscriber Service with Multiple Instances on page 343](#)
 - [Verifying and Managing Subscriber Services with Multiple Instances on page 347](#)
 - [Subscriber Services with Multiple Instances Overview on page 339](#)

Deactivating All Instances of a Subscriber Service with Multiple Instances

For subscriber services that have multiple instances, you can use the Junos OS CLI to deactivate a service in either of the following ways:

- Deactivate a single instance of a service by specifying the name and parameters of the service to be deactivated.
- Deactivate all instances of a service by specifying only the name of the service to be deactivated.

This topic describes how to deactivate all instances of a subscriber service.

To use the Junos OS CLI to deactivate all instances of a subscriber service with multiple instances:

1. Display the active services for the subscriber identified by the specified session ID.

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

For example, the following command displays the active services for the DHCP subscriber identified by session ID 6. In this example, two instances of economy-service are active: **economy-service(up-filter,down-filter)** and **economy-service(upstrm-filter,dwnstrm-filter)**. A single instance of premium-service named **premium-service(up-filter,down-filter)** is also active.

```
user@host> show network-access aaa subscribers session-id 6 detail
```

```
Type: dhcp
Stripped username: fran2
AAA Logical system/Routing instance: default:default
Target Logical system/Routing instance: default:default
Access-profile: attr_test_profile1
Session ID: 6
Accounting Session ID: 6
Multi Accounting Session ID: 0
IP Address: 100.20.0.10
Authentication State: AuthStateActive
Accounting State: Acc-Interim-Sent
Provisioning Type: None
Service name: economy-service(up-filter,down-filter)
  Service State: SvcActive
  Service Family: inet
  Service Activation Source: Radius
  Session ID: 7
  Session uptime: 00:04:36
  Accounting status: on/volume+time
  Service accounting session ID: 6:7-1354811427
  Service accounting state: Acc-Start-Sent
  Accounting interim interval: 600
Service name: economy-service(upstrm-filter,dwnstrm-filter)
  Service State: SvcActive
  Service Family: inet
  Service Activation Source: Radius
  Session ID: 8
  Session uptime: 00:04:36
  Accounting status: on/volume+time
  Service accounting session ID: 6:8-1354811427
  Service accounting state: Acc-Start-Sent
  Accounting interim interval: 600
Service name: premium-service(up-filter,down-filter)
  Service State: SvcActive
  Service Family: inet
  Service Activation Source: Radius
  Session ID: 9
  Session uptime: 00:04:36
  Accounting status: on/volume+time
  Service accounting session ID: 6:9-1354811427
  Service accounting state: Acc-Start-Sent
  Accounting interim interval: 600
```

2. Deactivate all instances of the specified service by specifying the service name without parameters.

```
user@host> request network-access aaa subscriber delete session-id subscriber-session-id
service-profile "profile-name"
```

For example, the following command deactivates both instances of economy-service.

```
user@host> request network-access aaa subscriber delete session-id 6 service-profile
"economy-service"
```

3. (Optional) Verify that all instances of the deactivated service are no longer active for the subscriber.

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

In the following example, only **premium-service(up-filter,down-filter)** is still active. Neither **economy-service(up-filter,down-filter)** nor **economy-service(upstrm-filter,dwnstrm-filter)** is listed because all instances of economy-service were deactivated.

```
user@host> show network-access aaa subscribers session-id 6 detail
```

```
Type: dhcp
Stripped username: fran2
AAA Logical system/Routing instance: default:default
Target Logical system/Routing instance: default:default
Access-profile: attr_test_profile1
Session ID: 6
Accounting Session ID: 6
Multi Accounting Session ID: 0
IP Address: 100.20.0.10
Authentication State: AuthStateActive
Accounting State: Acc-Interim-Sent
Provisioning Type: None
Service name: premium-service(up-filter,down-filter)
  Service State: SvcActive
  Service Family: inet
  Service Activation Source: Radius
  Session ID: 9
  Session uptime: 00:04:36
  Accounting status: on/volume+time
  Service accounting session ID: 6:9-1354811427
  Service accounting state: Acc-Start-Sent
  Accounting interim interval: 600
```

- Related Documentation**
- [Deactivating a Single Instance of a Subscriber Service with Multiple Instances on page 341](#)
 - [Verifying and Managing Subscriber Services with Multiple Instances on page 347](#)
 - [Subscriber Services with Multiple Instances Overview on page 339](#)

Monitoring and Managing Subscriber Services

- [Verifying and Managing Subscriber Services with Multiple Instances on page 347](#)

Verifying and Managing Subscriber Services with Multiple Instances

Purpose Display information about the active services for a subscriber identified by the specified session ID.

Action The following example displays information about the active services for the DHCP subscriber identified by session ID 6.

```
user@host> show network-access aaa subscribers session-id 6 detail
```

```
Type: dhcp
```

```
Stripped username: fms2
```

```
AAA Logical system/Routing instance: default:default
```

```
Target Logical system/Routing instance: default:default
```

```
Access-profile: attr_test_profile1
```

```
Session ID: 6
```

```
Accounting Session ID: 6
```

```
Multi Accounting Session ID: 0
```

```
IP Address: 100.20.0.10
```

```
Authentication State: AuthStateActive
```

```
Accounting State: Acc-Interim-Sent
```

```
Provisioning Type: None
```

```
Service name: economy-service(up-filter,down-filter)
```

```
Service State: SvcActive
```

```
Service Family: inet
```

```
Service Activation Source: Radius
```

```
Session ID: 7
```

```
Session uptime: 00:04:36
```

```
Accounting status: on/volume+time
```

```
Service accounting session ID: 6:7-1354811427
```

```
Service accounting state: Acc-Start-Sent
```

```
Accounting interim interval: 600
```

```
Service name: economy-service(upstrm-filter,dwnstrm-filter)
```

```
Service State: SvcActive
```

```
Service Family: inet
```

```
Service Activation Source: Radius
```

```
Session ID: 8
```

```
Session uptime: 00:04:36
```

```
Accounting status: on/volume+time
```

```
Service accounting session ID: 6:8-1354811427
```

```
Service accounting state: Acc-Start-Sent
```

```
Accounting interim interval: 600
Service name: premium-service
Service State: SvcActive
Service Family: inet
Service Activation Source: Radius
Session ID: 9
Session uptime: 00:04:36
Accounting status: on/volume+time
Service accounting session ID: 6:9-1354811427
Service accounting state: Acc-Start-Sent
Accounting interim interval: 600
```

Meaning If parameters are configured when a subscriber service with multiple instances is activated, the **Service name** field in the **show network-access aaa subscribers session-id** command displays both the service name and, in parentheses following the service name, the service parameters. If parameters are not configured for a particular service, the **show network-access aaa subscribers session-id** command displays only the service name. The value **SvcActive** in the **Service State** field indicates that the service is active.

In this example, two instances of economy-service are active: **economy-service(up-filter,down-filter)** and **economy-service(upstrm-filter,dwnstrm-filter)**. For **premium-service**, which is also active, the command output displays only the service name, indicating that no parameters were configured for this service.

- Related Documentation**
- [Deactivating a Single Instance of a Subscriber Service with Multiple Instances on page 341](#)
 - [Deactivating All Instances of a Subscriber Service with Multiple Instances on page 343](#)

PART 6

Configuring ANCP and the ANCP Agent for Subscribers

- [Configuring ANCP Agent Neighbors and Operations on page 351](#)
- [Configuring the ANCP Agent Traffic and CoS on page 395](#)
- [Configuring the ANCP Agent and AAA on page 403](#)
- [Monitoring and Managing ANCP for Subscriber Access on page 411](#)

Configuring ANCP Agent Neighbors and Operations

- [ANCP and the ANCP Agent Overview on page 351](#)
- [ANCP Operations in Different Network Configurations on page 358](#)
- [Configuring the ANCP Agent on page 368](#)
- [Configuring ANCP Neighbors on page 369](#)
- [Associating an Access Node with Subscribers for ANCP Agent Operations on page 370](#)
- [Specifying the Interval Between ANCP Adjacency Messages on page 371](#)
- [Specifying the Maximum Number of Discovery Table Entries on page 371](#)
- [Configuring the ANCP Agent for Backward Compatibility on page 372](#)
- [Specifying How Long Processes Wait for the ANCP Agent Restart to Complete on page 373](#)
- [Configuring the ANCP Agent to Learn ANCP Partition IDs on page 373](#)
- [Example: Configuring an ANCP Network with Interface Sets and N:1 Static Demux VLANs over Aggregated Ethernet on page 374](#)

ANCP and the ANCP Agent Overview

This topic describes the Access Node Control Protocol (ANCP) and the *ANCP agent*. The ANCP agent is the Junos OS process that manages subscriber access lines with ANCP. The agent monitors subscriber access lines, reports subscriber traffic rates on the access lines between the subscribers and the access nodes, and modifies the traffic rates, all in support of CoS traffic shaping.

- [Overview on page 352](#)
- [Topology Discovery on page 352](#)
- [Subscriber Services on page 353](#)
- [ANCP Interfaces and Access Loop Circuit Identifiers on page 353](#)
- [ANCP Neighbors on page 354](#)
- [Partitions on page 356](#)
- [Generic Response Messages and Result Codes on page 357](#)

Overview

ANCP acts as a control plane between a service-oriented Layer 3 edge device and a Layer 2 access node. The access nodes—ANCP *neighbors*—are network devices that terminate access loops from subscribers; for DSL access loops, the access node is a DSL access multiplexer (DSLAM). Queuing and scheduling mechanisms for subscriber traffic must avoid congestion within the access network while contending with multiple flows and distinct CoS requirements. These mechanisms require the edge device—a router acting as a broadband network gateway (BNG), often also called a network access server (NAS)—to provide information about the access network and subscriber traffic.

The ANCP agent can map an access line to an interface or interface set either statically or dynamically. The agent provides that information to both CoS and AAA. The agent passes on to both CoS and AAA the traffic shaping attributes for each subscriber access line that the access node sent to the ANCP agent. In addition, the agent sends to AAA all DSL Forum attributes that were sent by the access node. AAA can use these attributes during RADIUS accounting and authentication for both DHCP IP demux and PPPoE subscriber sessions. The traffic rates can also be used for shaping L2TP tunnel traffic.

You can monitor ANCP agent events and operations by including the **traceoptions** statement at the **[edit protocols ancp]** hierarchy level.

Junos OS supports the following interface types for ANCP:

- Static VLAN interfaces
- Static VLAN demux interfaces
- Static interface sets
- Dynamic interface sets
- Dynamic VLAN-tagged interface sets
- Dynamic agent circuit identifier (ACI) interface sets, also known as ACI sets or ACI VLANs
- Dynamic PPPoE and DHCP IP demux subscriber interfaces

ANCP was developed as an extension of *RFC 3292, General Switch Management Protocol (GSMP) V3*, but is now defined in *RFC 6320, Protocol for Access Node Control Mechanism in Broadband Networks*.

Topology Discovery

The router uses topology discovery to collect information from the access node. The information includes the following:

- Topology of the access network
- DSL line state
- Actual upstream and downstream net data rates of a synchronized DSL link

- Maximum attainable upstream and downstream net data rates
- Interleaving delay

Subscriber Services

The router receives the service profile for the subscribers from a RADIUS server. Most of the services are enforced by the router itself. The router shapes the aggregate egress traffic to subscribers based on the local loop throughput reported by the DSLAM. This traffic shaping optimizes traffic flow while avoiding traffic drops in the access node.

Some service attributes, such as interleaving delay and multicast channel information, are enforced at the access node. The ANCP agent provides the line configuration mechanism that the edge device can use to pass the line configuration to the access nodes. Typically, multiple profiles are provisioned on the access node. The router instructs the access node which profile to use for a given subscriber.

Subscribers typically receive some combination of voice, data, and video services. Each service can be provisioned on a VLAN. A subscriber might receive only a single service over a single VLAN configured on a logical interface. A group of VLANs carrying services to a subscriber is an *interface set*.

Subscribers have operational states, but they do not have administrative states because they cannot be configured in the CLI.

Subscribers have one of the following operational states which represent the DSL line state as it is reported in the ANCP Port Up and Port Down messages sent by an access node:

- Idle—Ports are not configured and the subscriber cannot log in.
- Silent—Ports are configured and the subscriber is connected, but the DSL modem is not ready to transfer data.
- Showtime—Ports are configured, the subscriber is connected, and the DSL modem is online and ready to transfer data.

ANCP Interfaces and Access Loop Circuit Identifiers

The access loop or access line in an ANCP topology consists of the physical elements between the subscriber device (CPE) and the access node. An identifier associated with the access loop serves to identify the subscriber as well. This identifier is an alphanumeric string that actually identifies the interface on the DSLAM from which subscriber requests originate. It can be referred to by various names.

- In ANCP messages, a TLV carries the access loop circuit ID, also referred to as the access line identifier, access loop circuit identifier, or access identifier.
- DHCP discovery packets can identify the line with the Agent Circuit ID suboption in the Option 82 field.
- PPPoE discovery packets can identify the line with the Agent-Circuit-ID subattribute in the DSL Forum vendor-specific tag.

Each of these identifiers is abbreviated as ACI. When the ANCP agent receives a port management message from an access node, it uses the access loop circuit identifier contained in the message to determine which logical interface or interface set corresponds to the subscriber.

You can associate an identifier with an ANCP access line by static configuration. When you configure a logical interface by specifying the interface name at the **[edit protocols ancp interfaces]** hierarchy level, include the **access-identifier** statement to associate the access loop circuit identifier with the interface. When you configure an interface set by including the **interface-set** statement at the **[edit protocols ancp interfaces]** hierarchy level, associate the access loop circuit identifier with the interface set by including the **access-identifier** statement at the **[edit protocols ancp interfaces interface-set interface-set-name]** hierarchy level.

When the DHCP or PPPoE discovery packet includes an ACI, the ANCP agent can dynamically map the ACI to the subscriber interface or interface set. VLANs for the subscribers are created according to a dynamic profile; these are called agent circuit identifier-based or ACI-based dynamic VLANs.

ANCP agent support for RADIUS authentication and accounting requires that both static and dynamic ACIs must be unique across the network. No two interfaces across multiple neighbors (access nodes) can share the same identifier. The DHCP and PPPoE processes do not have information about the access node IP addresses and consequently cannot distinguish between duplicate identifiers. This situation prevents the AAA services framework from correlating a DHCP or PPPoE client session with an access line for RADIUS authentication and accounting.

ANCP Neighbors

The ANCP agent can report traffic only for access nodes that are configured as ANCP neighbors (also referred to as ANCP peers). Neighbors can establish TCP connections with the router. Include the **neighbor** statement at the **[edit protocols ancp]** hierarchy level to configure an access node as an ANCP neighbor.

The ANCP agent exchanges adjacency messages with neighbors. If an adjacency message is not received from a neighbor within the expected period, then the neighbor is considered to be down and is disconnected. You can adjust how long the ANCP agent waits for adjacency messages from all neighbors by including the **adjacency-timer** statement at the **[edit protocols ancp]** hierarchy level. The interval between adjacency messages is negotiated between router and the neighbor during adjacency establishment. The larger of two timer values—either the value received in the ANCP SYN message or the configured value—is selected. Loss of synchronization between the router and a neighbor is declared when no valid messages are received for a period of time that exceeds three times the negotiated value.

**NOTE:**

The ANCP TCP connection is not established and consequently ANCP neighbors do not come up in either of the following circumstances:

- When the neighbor address (numbered or unnumbered) has a /32 mask.
- When the unnumbered local address for ANCP dynamic logical interfaces is configured to use a preferred source address.

ANCP neighbors have one of the following administrative states, which simply represent the configuration of the neighbor:

- **enabled**—The neighbor is configured in the CLI.
- **disabled**—The neighbor is not configured, meaning either that it has never been configured or that the configuration has been deleted.

ANCP neighbors in the enabled state have one of the following operational states, which represent the state of adjacency negotiations:

- **Configured**—The neighbor has been configured, but has never established an adjacency.
- **Establishing**—Adjacency negotiations are in progress.
- **Established**—Adjacency negotiations have succeeded and an ANCP session has been established.
- **Not Established**—The neighbor has lost a previously established adjacency, but is ready to begin negotiations.

You can also configure parameters for a specific neighbor that override global or default configurations by including any of the following statements at the **[edit protocols ancp neighbor ip-address]** hierarchy level:

- **adjacency-timer**—Adjust the interval between adjacency messages exchanged with this neighbor.
- **ietf-mode**—Prevent the ANCP agent from operating in a backward-compatible mode for this neighbor; for neighbors that use the current IETF implementation of ANCP.
- **maximum-discovery-table-entries**—Specify how many discovery table entries are accepted from this neighbor. Include this statement at the **[edit protocols ancp]** hierarchy level to set the number of entries globally for all neighbors.
- **pre-ietf-mode**—Enable the ANCP agent to operate in a backward-compatible mode for this neighbor; for neighbors that use the original IETF implementation of ANCP (GSMPv2) rather than the current implementation. Include this statement at the **[edit protocols ancp]** hierarchy level to operate in backward-compatible mode globally for all neighbors.

RFC 6320, Protocol for Access Node Control Mechanism in Broadband Networks, defines ANCP Version 1. ANCP was originally implemented based on General Switch Management Protocol (GSMP) version 3, sub-version 1. However, the Internet community has made

so many extensions and modifications to GSMPv3 in the course of developing ANCP that ANCP is no longer interoperable with GSMPv3. Consequently, ANCP neighbors must be able to dynamically detect the version that each peer supports. A joint registry codifies the GSMP and ANCP version numbers.

When an ANCP neighbor opens adjacency negotiations, it indicates the highest version of ANCP that it supports, either 0x31 for GSMPv3 or 0x32 for ANCP Version 1. (Version 1 may also be called Version 50, referring to the decimal conversion from the hexadecimal value.) If the receiving neighbor supports that version of ANCP, it returns that value when it responds to the sending neighbors. If it does not support that version, the receiving neighbor simply drops the message.

The ANCP agent stores information about active ANCP subscribers in the Junos shared database, including DSL attributes for the access lines. This storage is persistent and is removed from the database only when you delete the interface or interface set for the access line or issue one of the following commands:

- `clear ancp neighbor`
- `clear ancp subscriber`

The persistence of the storage enables PPPoE and DHCP IP demux subscribers to be properly managed by RADIUS for authentication and accounting, with their DSL attributes, even when the ANCP connection has been temporarily terminated.

Partitions

ANCP supports the division of an access node into logical partitions. Each partition creates an adjacency with a router; each partition on an access node can form adjacencies with different routers.

Each partition has an identifier carried in ANCP messages. A partition type field in ANCP messages indicates whether the access node is partitioned and how the partition identifier is negotiated. The field has one of the following values negotiated during the formation of the adjacency:

- 0—The access node is not partitioned or does not support partitions.
- 1—The number of partitions is fixed and the router requests the access node to use the identifier it places in the partition identifier field.
- 2—The number of partitions is fixed and the access node has assigned the partition identifier.

ANCP messages include a partition ID field that indicates one of the following scenarios for ANCP agent support of the neighbor:

- Zero partition ID—The ANCP agent supports each neighbor on an IP address over a single TCP session with a partition ID of zero. This is the default support case.
- Single nonzero partition ID—The ANCP agent supports each neighbor on an IP address over a single TCP session with a nonzero partition ID. This case requires partition ID learning to be enabled with the `gsmp-syn-wait` statement at the `[edit protocols ancp]` hierarchy level.

Generic Response Messages and Result Codes

ANCP neighbors and the router can reply to messages either with a specific response message or a generic response message. A generic response message is typically sent when no information needs to be sent to the peer other than a success or failure result. If the response is about a failure, then a result code is included that specifies the kind of failure; a limited amount of diagnostic data can also be included. A generic response message can also be sent independently of a request if the adjacency is being shut down because of the failure. In this case, the sender of the message zeros out the Transaction ID field in the message header and the Message Type field in the Status-Info TLV.

[Table 41 on page 357](#) describes the result codes that can be included in a generic response message.

Table 41: ANCP Failure Result Codes

Code Value	Description	Detected By
0x02	Although the request message is properly formed, it is invalid because it violates the protocol, either because of timing issues such as a race condition or the direction in which the message was transmitted.	ANCP agent
0x06	One or more of the specified ports is down because of a state mismatch between the router and an ANCP control application.	Control applications (none yet available)
0x13	ANCP is out of resources. This result code is sent only by the access node; the problem is probably not related to the access lines, but can be related to a specific request.	ANCP protocol layer or control applications (none yet available)
0x51	The type of request message is not implemented because of a mismatch in protocol versions or capability state between the peers, or possibly because the message type is optional for an ANCP capability.	ANCP agent
0x53	The message is malformed either because it was corrupted in transit or an implementation error occurred at one end of the connection.	ANCP agent
0x54	One or more mandatory TLVs is missing from the request.	ANCP agent
0x55	The contents of one or more TLVs in the request are invalid because they do not match the TLV specification.	ANCP agent

Table 41: ANCP Failure Result Codes (*continued*)

Code Value	Description	Detected By
0x500	One or more of the ports specified in a request does not exist, possibly because of a configuration mismatch between the access node and the router or AAA.	Control applications (none yet available)



NOTE: Although Junos OS supports both sending and receiving generic response messages, currently the ANCP agent only receives these messages. When one of these messages is received, the router generates a system log, increments the generic message counters, and increments the result code counters. When the ANCP agent receives an incorrect or unexpected generic response message from an ANCP neighbor, it immediately drops the packet, generates a system log notice message, and takes no further action.

Generic response messages usually include the Status-Info TLV, which includes supplemental information about a warning or error condition. The Status-Info TLV is required when the result code indicates any of the following: a port is down or does not exist, a mandatory TLV is missing, or a TLV is invalid. The Status-Info TLV can also be included in other ANCP message types.

Related Documentation

- [Traffic Rate Reporting and Adjustment by the ANCP Agent on page 395](#)
- [Configuring the ANCP Agent on page 368](#)
- [Triggering ANCP OAM to Test the Local Loop on page 411](#)
- [Agent Circuit Identifier-Based Dynamic VLANs Overview](#)

ANCP Operations in Different Network Configurations

This topic describes different types of supported network configurations and the sequence of events for ANCP operations in representative sample network topologies.

You can configure the ANCP agent for any of the following interface types:

- Static VLAN interfaces
- Static VLAN demux interfaces
- Static interface sets
- Dynamic interface sets
- Dynamic VLAN-tagged interface sets
- Dynamic agent circuit identifier (ACI) interface sets, also known as ACI sets or ACI VLANs
- Dynamic PPPoE and DHCP IP demux subscriber interfaces

Subscriber sessions are dynamically created as needed for each of the devices in a household. Each household can include multiple CPE devices that access the Internet. In all cases, each household is identified by a unique ACI that is assigned by the access node. Additional identifiers are used in some configurations.

The 1:1 and N:1 configuration models determine how VLANs are correlated with households. A network can include one or both of the models:

- **1:1 model**—A household has only one PPPoE or DHCP IP demux subscriber session. One or more such households can exist on a single VLAN or VLAN demux interface. In the case of a single household, either the subscriber interface or its underlying VLAN or VLAN demux interface can represent the household. In the case of multiple households, the corresponding subscriber interfaces represent the households. In either case, the interface representing a household must be mapped to the ACI for its access line.

[Table 42 on page 359](#) describes the types of interfaces supported for the ANCP 1:1 access model when interface sets are not involved, and whether the PPPoE or DHCP IP demux discovery packets must include the ACI for the subscriber access lines.

Table 42: ACI Mapping by Interface Type for the ANCP 1:1 Model

Interface Type	Description	Presence of ACI in Discovery Packets
Dynamic PPPoE or DHCP IP demux interface	When ACI is present in discovery packets, the ANCP agent maps the ACI to the subscriber interface. The name of the interface is automatically generated and nondeterministic.	Required.
Static VLAN or VLAN demux interface	The name of the interface is statically configured. The ANCP agent configuration must include the access-identifier statement to statically map the ACI to the interface.	Not present.

- **N:1 model**—A household can have more than one PPPoE or DHCP IP demux subscriber session. The household can have more than one VLAN or VLAN demux interface. In either case, all the interfaces must be grouped into an interface set. The interface set in turn must be mapped to the ACI for the household's access line.

An interface set groups the dynamic PPPoE or DHCP IP demux sessions for a household. The subscribers are placed into interface sets by one several methods.

[Table 43 on page 360](#) describes the types of interface sets supported in the ANCP N:1 access model, how they are created, and how the ACI is mapped to the interface set.

Table 43: ACI Mapping by Interface Set Type for the ANCP N:1 Access Model

Type of Interface Set	Description	Interface Type	Presence of ACI in Discovery Packets
ACI-based VLAN interface sets	<p>When the router receives a DHCP or PPPoE discovery packet that includes an ACI embedded within the DSL Forum vendor-specific tag, it dynamically creates the VLAN and the interface set. The router generates a nondeterministic name for the interface set, such as aci-1003-ge-1/0/0.1073741832.</p> <p>The ANCP agent automatically maps the ACI from the discovery packet to the dynamically created interface set.</p> <p>All DHCP IP demux or PPPoE sessions that have the same ACI are mapped to the same interface set.</p>	Dynamic VLAN and VLAN demux interfaces.	Required.
Dynamic interface sets	<p>A dynamic profile dynamically creates the interface set and places interfaces in the set. The profile can either have the name of the interface set explicitly configured or a variable that represents the interface set name. If a variable is used, then the interface set name is provided by RADIUS when it returns an Access-Accept message for the subscriber.</p> <p>The ANCP agent configuration must include the access-identifier statement to statically map the ACI to the interface set.</p> <p>All DHCP IP demux and PPPoE sessions are mapped to an interface set according to the rules of the dynamic profile.</p>	DHCP IP demux subscriber interfaces, PPPoE subscriber interfaces, or VLAN interfaces.	Irrelevant.
Static interface sets	<p>The interface set and set name are statically configured and include multiple static interfaces.</p> <p>The ANCP agent configuration must include the access-identifier statement to statically map the ACI to the interface set.</p>	Static VLAN and VLAN demux interfaces.	Irrelevant.
VLAN-tagged interface sets	<p>When the router receives a DHCP or PPPoE discovery packet that includes a VLAN ID, it dynamically creates the VLAN and the interface set. The interface set is given a deterministic name consisting of the physical interface name and the VLAN tags, for example, ge-1/0/0-101.</p> <p>The ANCP agent configuration must include the access-identifier statement to statically map the ACI to the interface set.</p> <p>All DHCP IP demux or PPPoE sessions that have the same VLAN ID tag are mapped to the same interface set.</p>	Dynamic VLAN and VLAN demux interfaces.	Irrelevant.

CoS traffic shaping is based on the subscriber downstream traffic rate that the ANCP agent receives from the access node and then passes to CoS. CoS can shape subscriber traffic at the level of the household or the session:

- Household shaping—Only aggregate traffic to the household is shaped. Household shaping results from applying a CoS traffic-control profile to the static VLAN or VLAN demux interface or to the interface set.

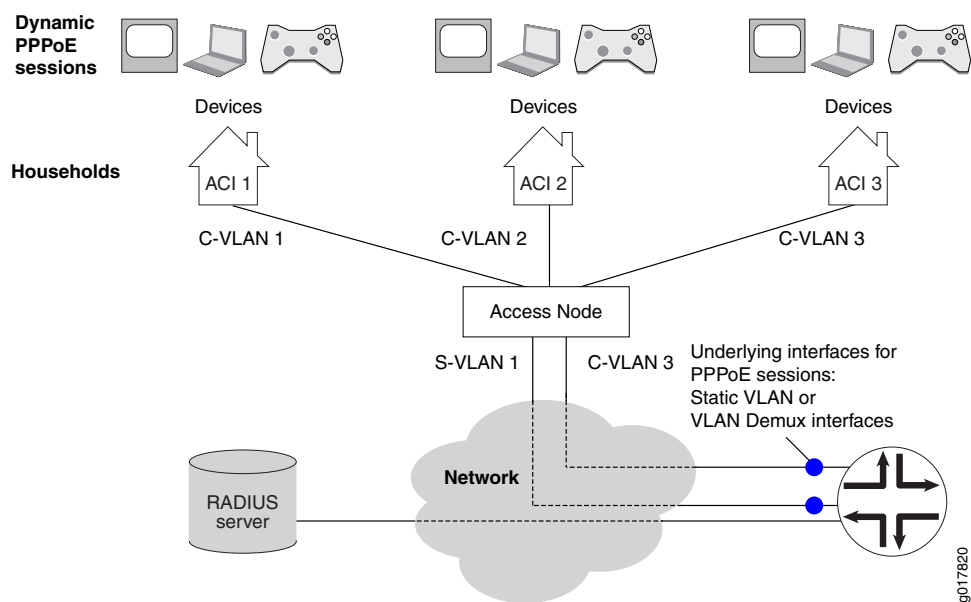
- Session shaping—The traffic rate to individual devices in the household is shaped. Session shaping results from specifying a CoS traffic-control profile in the dynamic PPPoE profile that creates the subscriber session. Depending on the network configuration, session shaping may employ shared priority queues to shape all sessions identically or individual priority queues to shape the sessions separately.

The following sections illustrate several possible configurations and lists the sequence of events for the ANCP operations in each case. Not every possible configuration is presented.

ANCP Network Using N:1 and 1:1 Configuration Models without Interface Sets

In this sample topology, two households are configured for one underlying static VLAN or VLAN demux interface (N:1; dual-tagged VLAN) and a single household is configured for another underlying interface (1:1; single-tagged VLAN) (Figure 3 on page 362). In addition to the unique ACI assigned by the access node, each household is further identified by the VLAN, which is mapped to the identifier in the ANCP agent configuration. CoS traffic shaping for sessions can employ only shared priority queues to shape all sessions identically; individual priority queues to shape the sessions separately are not supported.

Figure 3: Sample ANCP Topology Without Interface Sets (1:1 and N:1 Model)



Sequence of ANCP Events: Static VLAN or VLAN Demux Interfaces over Ethernet Without Interface Sets

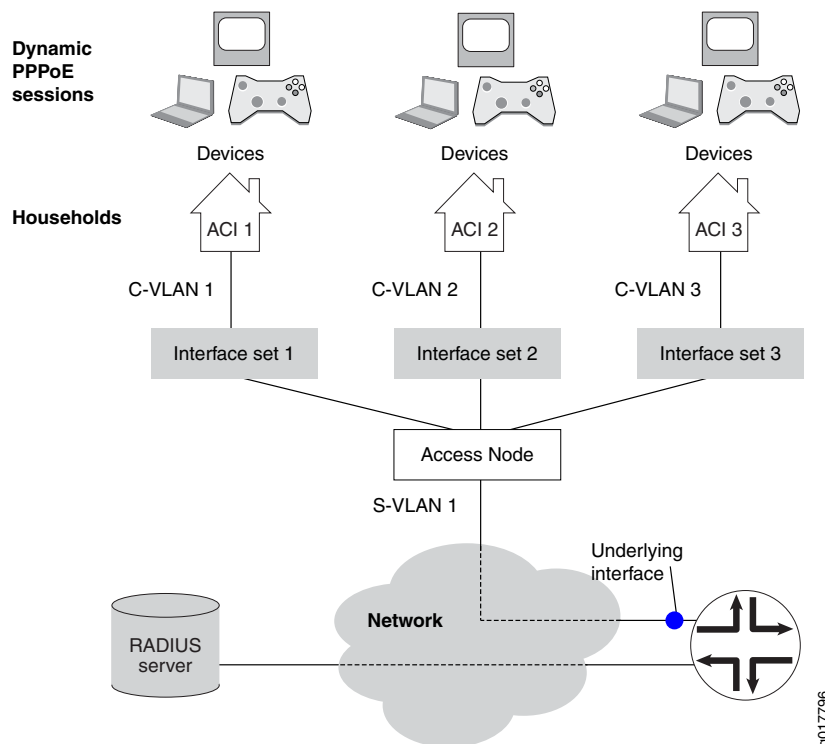
The following sequence of events is for the topology in [Figure 3 on page 362](#) with static VLAN interfaces over Ethernet without interface sets.

1. A network device in the household initiates PPPoE discovery.
2. PPPoE creates a dynamic PPPoE session on the underlying static VLAN or VLAN demux interface and applies the advisory options configured on the VLAN to the session.
3. The access node independently provides the ANCP agent with the ANCP DSL attributes for an access line identified by an ACI.
4. The ANCP agent sends CoS the adjusted downstream data rate for the static VLAN or demux VLAN mapped to the ACI. The ANCP agent stores all DSL attributes, including the adjusted upstream data rate, in the router's shared database.
5. AAA correlates the dynamic PPPoE session with the access line by matching the underlying interface of the session to the static VLAN or VLAN demux interface associated with the ACI in the ANCP agent configuration.
6. AAA retrieves the ANCP DSL attributes for the access line from the router's shared database and maps them to the Juniper Networks DSL VSAs in the RADIUS Access-Request and Accounting-Request messages. If the DSL attributes are unavailable, the session's advisory upstream and downstream data rates are mapped to the Upstream-Calculated-Qos-Rate VSA (26-142) and Downstream-Calculated-Qos-Rate (26-141) VSAs, respectively. These VSAs are then included in the RADIUS messages.

ANCP Network Using N:1 Configuration Model with Interface Sets

In this topology, multiple households are configured for each underlying static VLAN or VLAN demux interface (Figure 4 on page 364). The VLANs are dual-tagged. Each household includes several CPE devices that access the Internet. In addition to the unique ACI assigned by the access node, the household is further identified by the interface set. The interface set groups the dynamic PPPoE sessions for the individual subscriber devices. It is either explicitly configured in the dynamic PPPoE profile or specified in the RADIUS Access-Accept message during PPPoE session authentication. Session shaping can employ shared priority queues to shape all sessions identically or individual queues to shape the sessions separately.

Figure 4: Sample ANCP Topology with Interface Sets (N:1 Model)



In this N:1 model with interface sets, the access node must add the DSL Forum VSA to the PPPoE PADI and PADR discovery packets that it passes to the router during the establishment of dynamic PPPoE sessions. The VSA includes the ACI for the household. This inclusion enables AAA to correlate the PPPoE sessions with their respective subscriber access lines and DSL attributes during RADIUS authentication and accounting. If the ACI is not present, AAA cannot make the correlation and subsequently reports only the advisory upstream and downstream data rates to RADIUS Authentication and Accounting.

When the dynamic PPPoE profile is configured with the **\$junos-interface-set-name** predefined variable, the configuration of the access node, router, and RADIUS server must be synchronized with regard to the ACI and interface set:

- The RADIUS Access-Accept message must contain the Juniper Networks Qos-Interface-Set-Name VSA (26-130).
- The CoS Layer 2 configuration must explicitly identify the interface set that is named in the Qos-Interface-Set-Name VSA (26-130).
- The ANCP agent configuration must map an ACI to the interface set that is named in the Qos-Interface-Set-Name VSA (26-130).

Sequence of ANCP Events: Static VLAN Interfaces over Ethernet with Interface Sets

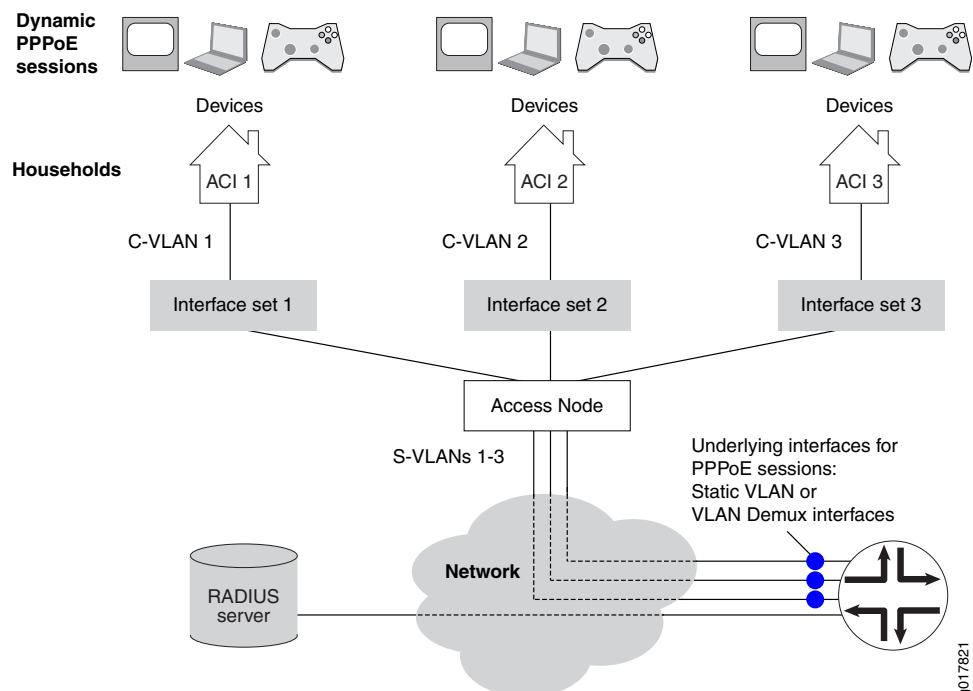
The following sequence of events is for the topology in [Figure 4 on page 364](#) with static VLAN interfaces over Ethernet with interface sets.

1. A network device in the household initiates PPPoE discovery.
2. The access node adds the DSL Forum VSA tag with the ACI for the household to the PPPoE PADI and PADR discovery packets. (The identifier is known to PPPoE as the agent circuit identifier.)
3. PPPoE creates a dynamic PPPoE session with the provided ACI on the underlying static VLAN and applies the advisory options configured on the VLAN to the session.
4. The access node independently provides the ANCP agent with the ANCP DSL attributes for an access line identified by an ACI.
5. The ANCP agent provides CoS with the adjusted downstream data rate for the interface set mapped to the ACI. The ANCP agent stores all ANCP DSL attributes, including the adjusted upstream and downstream data rates, in the router's shared database.
6. AAA correlates the dynamic PPPoE session with the access line by matching the session identifier received in the DSL Forum VSA to the ACI configured for the interface set in the ANCP agent configuration.
7. AAA retrieves the ANCP DSL attributes for the access line from the router's shared database and maps them to the Juniper Networks DSL VSAs in the RADIUS Access-Request and Accounting-Request messages. If the DSL attributes are unavailable, the session's advisory upstream and downstream data rates are mapped to the Upstream-Calculated-Qos-Rate VSA (26-142) and Downstream-Calculated-Qos-Rate (26-141) VSAs, respectively. These VSAs are then included in the RADIUS messages.
8. When authentication is completed, the dynamic PPPoE session is placed into the interface set configured in the dynamic PPPoE profile. The profile specifies a named interface set or the **\$junos-interface-set-name** predefined variable, which indicates that the interface set is named in the RADIUS Access-Accept message.

ANCP Network Using 1:1 Configuration Model with Interface Sets

In this topology, a single household is configured for each underlying static VLAN or VLAN demux interface (Figure 5 on page 366). The VLANs are dual-tagged. Each household includes several CPE devices that access the Internet. In addition to the unique ACI assigned by the access node, the household is further identified by the interface set. The interface set is either explicitly configured in the dynamic PPPoE profile or specified in the RADIUS Access-Accept message during PPPoE session authentication. Session shaping can employ shared priority queues to shape all sessions identically or individual queues to shape the sessions separately.

Figure 5: Sample ANCP Topology with Interface Sets (1:1 Model)



In this 1:1 model with interface sets, the ANCP agent configuration must map the underlying interface for the PPPoE sessions in an interface set to both the ACI and the interface set. This configuration enables AAA to correlate the PPPoE sessions with their respective subscriber access lines and DSL attributes during RADIUS authentication and accounting.

When the dynamic PPPoE profile is configured with the `$junos-interface-set-name` predefined variable, the configuration of the access node, router, and RADIUS server must be synchronized with regard to the ACI and interface set:

- The RADIUS Access-Accept message must contain the Juniper Networks Qos-Interface-Set-Name VSA (26-130).
- The CoS Layer 2 configuration must explicitly identify the interface set that is named in the Qos-Interface-Set-Name VSA (26-130).
- The ANCP agent configuration must map an ACI to the interface set that is named in the Qos-Interface-Set-Name VSA (26-130).

Sequence of ANCP Events: Static VLAN Demux Interfaces over Aggregated Ethernet with Interface Sets

The following sequence of events is for the topology in [Figure 5 on page 366](#) with static VLAN demux interfaces over aggregated Ethernet with interface sets.

1. A network device in the household initiates PPPoE discovery.
2. PPPoE creates a dynamic PPPoE session with the provided ACI on the underlying static VLAN demux interface and applies the advisory options configured on the VLAN to the session.
3. The access node independently provides the ANCP agent with the ANCP DSL attributes for an access line identified by an ACI.
4. The ANCP agent provides CoS with the adjusted downstream data rate for the interface set mapped to the ACI. The ANCP agent stores all ANCP DSL attributes, including the adjusted upstream and downstream data rates, in the router's shared database.
5. AAA correlates the dynamic PPPoE session with the access line by matching the underlying interface of the session to the underlying interface configured for the interface set in the ANCP agent configuration.
6. AAA retrieves the ANCP DSL attributes for the access line from the router's shared database and maps them to the Juniper Networks DSL VSAs in the RADIUS Access-Request and Accounting-Request messages. If the DSL attributes are unavailable, the session's advisory upstream and downstream data rates are mapped to the Upstream-Calculated-Qos-Rate VSA (26-142) and Downstream-Calculated-Qos-Rate (26-141) VSAs, respectively. These VSAs are then included in the RADIUS messages.
7. When authentication is completed, the dynamic PPPoE session is placed into the interface set configured in the dynamic PPPoE profile. The profile specifies a named interface set or the `$junos-interface-set-name` predefined variable, which indicates that the interface set is named in the RADIUS Access-Accept message.

Related Documentation

- [ANCP and the ANCP Agent Overview on page 351](#)
- [Configuring the ANCP Agent on page 368](#)
- [Example: Configuring an ANCP Network with Interface Sets and N:1 Static Demux VLANs over Aggregated Ethernet on page 374](#)

Configuring the ANCP Agent

You can configure the ANCP agent to enable a service-oriented Layer 3 edge device to discover information about the topology of a connected access network. The ANCP agent can also provide details about subscriber traffic and enable the adjustment of QoS traffic shaping for subscribers.

To configure the ANCP agent:

1. Specify each ANCP neighboring access node to be monitored and optionally configure neighbor parameters.
[See “Configuring ANCP Neighbors” on page 369.](#)
2. Specify the subscribers reached by a VLAN or a set of VLANs through a particular access node.
[See “Associating an Access Node with Subscribers for ANCP Agent Operations” on page 370.](#)
3. (Optional) Configure the adjacency timer.
[See “Specifying the Interval Between ANCP Adjacency Messages” on page 371.](#)
4. (Optional) Specify the maximum number of discovery table entries that are accepted.
[See “Specifying the Maximum Number of Discovery Table Entries” on page 371](#)
5. (Optional) Configure the ANCP agent to work with an early IETF draft.
[See “Configuring the ANCP Agent for Backward Compatibility” on page 372.](#)
6. (Optional) Configure the graceful restart timer.
[See “Specifying How Long Processes Wait for the ANCP Agent Restart to Complete” on page 373.](#)
7. (Optional) Configure the ANCP agent to learn partition IDs from neighbors.
[See “Configuring the ANCP Agent to Learn ANCP Partition IDs” on page 373.](#)
8. (Optional) Configure an adjustment factor per DSL line type for the downstream and upstream data rates that the ANCP agent reports to AAA.
[See “Setting a Global Adjustment Factor per DSL Subscriber Line for ANCP Agent-Reported Traffic Rates” on page 402.](#)
9. (Optional) Configure the ANCP agent to report unadjusted downstream traffic rates to CoS.
[See “Configuring the ANCP Agent to Report Traffic Rates to CoS” on page 399.](#)
10. (Optional) Specify a recommended shaping rate to be applied by RADIUS to downstream or upstream traffic per ANCP interface.
[See “Setting a Recommended Shaping Rate for Traffic on ANCP Interfaces” on page 400.](#)
11. (Optional) Configure AAA to Include or Exclude Juniper Networks DSL VSAs in RADIUS authentication and accounting messages.

See [“Configuring AAA to Include Juniper Networks DSL VSAs in RADIUS Messages”](#) on page 407.

12. (Optional) Configure AAA to send an immediate interim accounting update to the RADIUS server when AAA receives a rate change notification from the ANCP agent on the router.

See [“Configuring Immediate Interim Accounting Updates to RADIUS in Response to ANCP Notifications”](#) on page 408.

13. (Optional) Configure trace options for troubleshooting the configuration.

See [“Tracing ANCP Agent Operations for Subscriber Access”](#) on page 553.

Related Documentation

- [ANCP and the ANCP Agent Overview](#) on page 351
- [Triggering ANCP OAM to Test the Local Loop](#) on page 411

Configuring ANCP Neighbors

You must configure each neighboring access node that you want the ANCP agent to monitor and potentially shape traffic for. Some neighbor settings override globally configured values.

To configure an ANCP neighbor:

1. Specify the IP address of the neighbor.

```
[edit protocols ancp]
user@host# set neighbor 10.2.3.4
```

2. (Optional) Configure the neighbor to operate in a backward-compatible mode when it does not support the current IETF standard and the backward-compatible mode is not configured globally.

```
[edit protocols ancp neighbor 10.2.3.4]
user@host# set pre-ietf-mode
```

3. (Optional) Override the globally configured backward-compatible mode when the neighbor supports the current IETF standard.

```
[edit protocols ancp neighbor 10.2.3.4]
user@host# set ietf-mode
```

4. (Optional) Configure the interval in seconds between ANCP adjacency messages exchanged with this neighbor.

```
[edit protocols ancp neighbor 10.2.3.4]
user@host# set adjacency-timer 20
```

5. (Optional) Specify the maximum number of discovery table entries that are accepted from this neighbor.

```
[edit protocols ancp neighbor 10.2.3.4]
user@host# set maximum-discovery-table-entries 10000
```

**Related
Documentation**

- [Configuring the ANCP Agent on page 368](#)
- [Configuring the ANCP Agent for Backward Compatibility on page 372](#)
- [Specifying the Interval Between ANCP Adjacency Messages on page 371](#)
- [Specifying the Maximum Number of Discovery Table Entries on page 371](#)

Associating an Access Node with Subscribers for ANCP Agent Operations

The ANCP agent on the router uses the access loop circuit identifier (ACI) to distinguish individual ANCP subscribers. Because the agent uses the ACI to associate (map) each subscriber to an interface or interface set, each ACI must be unique across all ANCP neighbors connected to the router.



NOTE: We recommend that the ACIs be unique across your ANCP network.

The ACIs can be statically or dynamically configured. When the subscriber's DHCP or PPPoE discovery packets contain the ACI, then the agent can dynamically map it to the interface or interface set. Otherwise, the ACI must be statically configured. A static configuration overrides dynamic mapping of ACIs—and therefore subscribers—to interfaces or sets.

To associate an ACI with a set of VLAN interfaces for subscribers:

- Specify the name of the interface set and the unique ACI for the access node.

```
[edit protocols ancp interfaces]
user@host# set interface-set vlan5 access-identifier "dslam port 2/3"
```

To associate an ACI with a single VLAN:

- Specify the logical interface and the unique ACI for the access node.

```
[edit protocols ancp interfaces]
user@host# set ge-1/0/4.12 access-identifier "dslam port-2-10"
```

To associate an ACI with a static VLAN demux interface:

- Specify the logical interface and the unique ACI for the access node.

```
[edit protocols ancp interfaces]
user@host# set demux0.100 access-identifier aci_100_1_0
```

**Related
Documentation**

- [Configuring the ANCP Agent on page 368](#)
- [interfaces on page 772](#)

Specifying the Interval Between ANCP Adjacency Messages

When the ANCP agent and a neighbor negotiate to establish an adjacency, each proposes a value for the interval between the adjacency messages that they exchange after it is established. The larger of the values proposed by the agent and the neighbor is selected for the interval between subsequent adjacency messages exchanged by the agent and the neighbor. You can specify the interval value that the ANCP agent proposes for either all neighbors or a specific neighbor.

To configure the proposed interval between ANCP adjacency messages for all neighbors:

- Specify the time in seconds.


```
[edit protocols ancp]
user@host# set adjacency-timer 20
```

To configure the proposed interval between ANCP adjacency messages for a specific neighbor:

- Specify the time in seconds.


```
[edit protocols ancp neighbor 10.2.3.4]
user@host# set adjacency-timer 20
```

Related Documentation

- [Configuring the ANCP Agent on page 368](#)
- [Configuring ANCP Neighbors on page 369](#)

Specifying the Maximum Number of Discovery Table Entries

You can specify the maximum number of discovery table entries accepted from all neighbors or from a particular neighbor.

To configure the maximum number of entries for all neighbors:

- Specify the number of entries.


```
[edit protocols ancp]
user@host# set maximum-discovery-table-entries 5000
```

To configure the maximum number of entries for a specific neighbor:

- Specify the number of entries.


```
[edit protocols ancp neighbor 10.2.3.4]
user@host# set maximum-discovery-table-entries 5000
```

Related Documentation

- [Configuring the ANCP Agent on page 368](#)
- [Configuring ANCP Neighbors on page 369](#)

Configuring the ANCP Agent for Backward Compatibility

You can configure the ANCP agent to operate in a mode compatible with the protocol as it was initially proposed to operate. This backward-compatible or pre-IETF mode is compatible with Internet draft draft-wadhwa-gsmp-l2control-configuration-00.txt, *GSMP extensions for layer2 control (L2C)*. Setting this backward-compatible mode enables interoperability with devices that are not compatible with the later ANCP Internet drafts or RFC 6320, *Protocol for Access Node Control Mechanism in Broadband Networks*.

When this mode is configured globally for all neighbors, you can override it for a particular neighbor that supports the IETF draft or standard.

To configure the ANCP agent to operate in a backward-compatible mode for all neighbors:

- Specify the pre-IETF mode.

```
[edit protocols ancp]
user@host# set pre-ietf-mode
```

To configure the ANCP agent to operate in a backward-compatible mode for a specific neighbor:

- Specify the pre-IETF mode.

```
[edit protocols ancp neighbor 10.2.3.4]
user@host# set pre-ietf-mode
```

- To override the globally configured backward-compatible mode for a specific neighbor:

Specify the IETF mode.

```
[edit protocols ancp neighbor 10.2.3.4]
user@host# set ietf-mode
```

Related Documentation

- [Configuring the ANCP Agent on page 368](#)
- [Configuring ANCP Neighbors on page 369](#)

Specifying How Long Processes Wait for the ANCP Agent Restart to Complete

You can specify how long other processes wait for the ANCP agent to restart. The ANCP agent sends a keepalive message to CoS at intervals equal to one-third the value of the maximum helper restart time. For example, when you configure the maximum restart time to 120 seconds, the ANCP agent sends a keepalive message every 40 seconds.

If CoS does not receive a keepalive message within the maximum helper restart time, it considers the ANCP agent to be down and immediately reverts any traffic shaping updates that were implemented as a result of ANCP agent monitoring to the configured values. Consequently, traffic to the subscribers is not effectively shaped, potentially resulting in traffic drops in the DSLAMs. The configured values are maintained until the ANCP agent comes back up and sends fresh traffic shaping updates to CoS.

To configure how long other processes wait for the ANCP agent to restart:

- Specify the time in seconds.

```
[edit protocols ancp]
user@host# set maximum-helper-restart-time 150
```

Related Documentation

- [Configuring the ANCP Agent on page 368](#)
- [Configuring the ANCP Agent to Report Traffic Rates to CoS on page 399](#)

Configuring the ANCP Agent to Learn ANCP Partition IDs

By default, the ANCP agent expects ANCP partition IDs to be zero, meaning that the access node is not divided into logical partitions that can each form adjacencies with routers. You can configure the ANCP agent to support nonzero partition IDs. When you do so, the agent waits a configurable period to receive a SYN message from a neighbor during adjacency initiation. When the agent receives such a message, it uses the partition information contained in the Partition ID, PType, and PFlag fields to generate in turn a SYN message that it sends to the neighbor to continue adjacency negotiation.

To configure the ANCP agent to learn partition ID information from neighbors:

1. Enable partition ID learning.

```
[edit protocols ancp]
user@host# set gsmp-syn-wait
```

2. (Optional) Specify the maximum time the ANCP agent waits to receive a SYN message from a neighbor during the formation of an adjacency.

```
[edit protocols ancp]
user@host# set gsmp-syn-timeout seconds
```

For example, to enable partition ID learning and force the ANCP agent to wait 45 seconds for a SYN message:

```
[edit protocols ancp]
```

```
user@host# set gsmp-syn-wait
user@host# set gsmp-syn-timeout 45
```

**Related
Documentation**

- [Configuring the ANCP Agent on page 368](#)
- [ANCP and the ANCP Agent Overview on page 351](#)

Example: Configuring an ANCP Network with Interface Sets and N:1 Static Demux VLANs over Aggregated Ethernet

This example describes how to configure an ANCP network topology that manages subscriber access for several households by grouping individual devices into interface sets, providing access and services through one dedicated C-VLAN per household, and shaping traffic on a per-household basis. In this N:1 configuration, dual-tagged VLANs are configured over a single, underlying, static VLAN demux interfaces over aggregated Ethernet.

- [Requirements on page 374](#)
- [Overview on page 374](#)
- [Configuration on page 379](#)
- [Verification on page 391](#)

Requirements

This example uses the following hardware and software components:

- MX Series 3D Universal Edge Router with only MPCs installed for VLAN demux support
- RADIUS server
- DSLAM access node

Before you begin configuring the example, be sure you have:

- Thoroughly read and understood the following topics:
 - [ANCP and the ANCP Agent Overview on page 351](#)
 - [ANCP Operations in Different Network Configurations on page 358](#)
- Configured your access node.
- Configured your RADIUS server.

Overview

ANCP provides a means to configure, maintain, and monitor local access lines between access nodes (DSLAMs) and subscribers. Associated CoS configurations shape the downstream subscriber traffic. ANCP can enable more accurate traffic shaping by adjusting net data rates to discount the packet overhead of the access lines and then providing these adjusted rates to CoS.

The network topology in this example includes a dual-tagged (C-VLAN/S-VLAN) VLAN configuration over a static VLAN demux interface that is in turn configured over aggregated Ethernet for redundancy. This topology is an N:1 configuration model because—although each C-VLAN corresponds to one subscriber household—all the C-VLANs are configured over the same underlying VLAN demux interface. Multiple end-user devices in each household—or rather the dynamic PPPoE sessions established by each device—are grouped by household into interface sets. The grouping is accomplished by a separate dynamic profile configured for each C-VLAN. The ANCP agent configuration maps the ACI for the household's access line to an interface set. CoS applies a traffic-control profile to each interface set to shape the subscriber-directed traffic on a per-household basis. The CoS shaping rate is dynamically updated based upon the DSL attributes provided by the access node for each household's access line.

Figure 6 on page 375 shows S-VLAN 103, configured on demux0, servicing the access node. C-VLANs 1, 2, and 3 each service a single household (subscriber). The respective households are identified by unique ACIs. The dynamic PPPoE sessions for devices in each household are grouped for monitoring and traffic shaping into interface sets 10301, 10302, and 10303.

Figure 6: N:1 ANCP Topology with Interface Sets and VLAN Demux Interface over Aggregated Ethernet

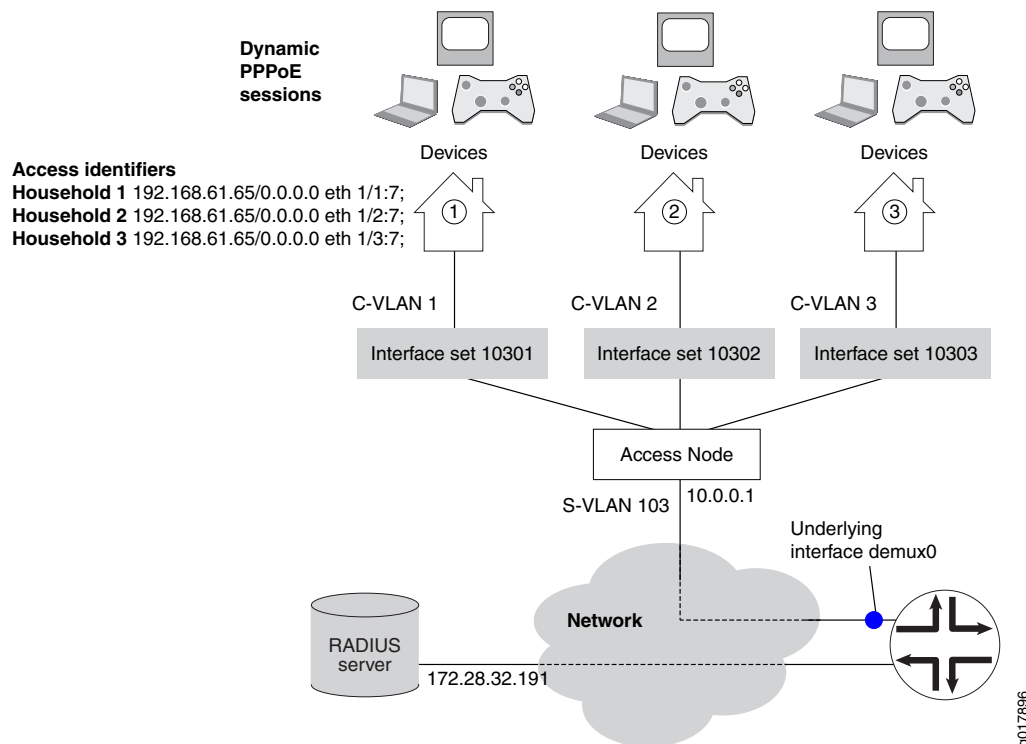


Table 44 on page 376 describes the configuration components used in this example.

Table 44: Configuration Components used in ANCP N:1 Topology Example with Interface Sets

Configuration Component or Property	Component Name or Setting	Description
Dynamic profiles	ancp-10301	<p>Each profile defines the dynamic PPPoE session created when any of the devices for a particular subscriber household accesses the network.</p> <p>Each profile specifies the following:</p> <ul style="list-style-type: none"> • A set of interfaces in which the sessions are created. • Dynamic instantiation of both the logical interfaces for the sessions and the underlying PPPoE logical interfaces on which the subscribers log in. • CHAP and PAP authentication for the sessions. • The interval between successive PPP keepalive messages. • The loopback address for the dynamic PPPoE logical interfaces.
	ancp-10302	
	ancp-10303	
Predefined variables	\$junos-interface-unit	Instantiates the logical interface for each PPPoE session.
	\$junos-underlying-interface	Instantiates the logical underlying PPP interface on which each dynamic PPPoE logical interface is created when a subscriber logs in.

Table 44: Configuration Components used in ANCP N:1 Topology Example with Interface Sets (*continued*)

Configuration Component or Property	Component Name or Setting	Description
Interfaces	ae0	<p>Aggregated Ethernet interface that is the underlying interface for the VLAN demux interfaces.</p> <p>The interface includes the following configuration:</p> <ul style="list-style-type: none"> • CoS hierarchical scheduling. • Stacked VLAN tagging for all logical interfaces on top of ae0. • Link protection.
	demux0	VLAN demux interface that runs over the underlying aggregated Ethernet interface.
	demux0.10301	<p>VLAN demux logical interfaces that correspond to the C-VLANs for individual subscriber households.</p> <p>Each logical interface includes the following configuration:</p> <ul style="list-style-type: none"> • Inner (C-VLAN) and outer VLAN (S-VLAN) tags. • The underlying physical interface, ae0. • The dynamic profile that creates PPPoE sessions on the C-VLAN. • Downstream and upstream advisory traffic rates. • Proxy ARP and protection against duplicate sessions on the interface.
	demux0.10302	
	demux0.10303	
	ge-1/0/1	Primary member link in the aggregated Ethernet bundle.
	ge-1/0/2	Backup member link in the aggregated Ethernet bundle.
	lo0.0	Loopback interface for use in the access network. The loopback interface is automatically used for unnumbered interfaces.
	pp0	PPP interface on which the PPPoE subscriber logical interfaces are created.

Table 44: Configuration Components used in ANCP N:1 Topology Example with Interface Sets (continued)

Configuration Component or Property	Component Name or Setting	Description
Interface sets	10301	Set of interfaces in which the sessions for the devices in a particular household are created. Each interface set is specified in a dynamic profile for that household. ANCP associates each interface set with an ACI and a VLAN demux logical interface (C-VLAN). CoS applies a traffic-control profile to each interface set.
	10302	
	10303	
Advisory traffic rates	downstream-rate	Recommended rate for downstream traffic in the absence of traffic rate information from the access node.
	upstream-rate	Recommended rate for upstream traffic in the absence of traffic rate information from the access node.
Traffic-control profile	tcp1	CoS profile that shapes the downstream subscriber traffic rate; in this example, shaping is adjusted for ATM packet overhead. The profile is applied to the interface sets.
IP addresses	10.0.0.1	Address of the ANCP access node that monitors the subscriber households.
	10.50.0.1/28	Address of the loopback interface, lo0.
	172.28.32.191	Address of the RADIUS accounting server and authentication server.
Access circuit loop identifiers	192.168.61.65/0.0.0.0 eth 1/1:7;	Identifier for the local access circuit from the access node to the subscriber household. It identifies the household. ANCP associates each identifier with an interface set.
	192.168.61.65/0.0.0.0 eth 1/2:7;	
	192.168.61.65/0.0.0.0 eth 1/3:7;	

The ANCP agent configuration includes the following elements:

- The IP address for the access node (DSLAM) is specified as 10.0.0.1. The interval between ANCP adjacency messages sent between neighbors is set to 5 seconds.
- The ANCP agent is enabled to report adjusted data rates to CoS to improve the accuracy of downstream traffic shaping. The ANCP agent adjusts the net data rates for ADSL lines by ninety percent and for ADSL2 lines by ninety-five percent.
- Each interface set is associated with both the ACI unique to the subscriber household and the relevant underlying VLAN demux interface.

The RADIUS configuration on the router includes the following elements:

- The IP address (172.28.32.191) for the authentication and accounting server, as well as the secret password for accessing the server.
- The subscriber access profile, radius-profile, specifies that RADIUS is used for authentication.
- Juniper Networks DSL VSAs are included in RADIUS request messages, but the DSL Forum VSA attributes are excluded from RADIUS messages
- Accounting sessions are configured to be recognized in decimal format.

Configuration

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode*.

To configure an ANCP network with static N:1 demux VLANs to the subscriber households, perform these tasks:

- [Configuring the Dynamic PPPoE Profiles on page 381](#)
- [Configuring the Static VLAN Demux Interface over Aggregated Ethernet on page 383](#)
- [Configuring Class of Service on page 387](#)
- [Configuring ANCP on page 388](#)
- [Configuring RADIUS Authentication and Accounting on page 389](#)

CLI Quick Configuration

To quickly configure the ANCP network described in this example, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

```
# Dynamic Profiles
edit dynamic-profiles ancp-10301
set interfaces interface-set 10301 interface pp0 unit "$junos-interface-unit"
edit interfaces pp0 unit "$junos-interface-unit"
set ppp-options chap
set ppp-options pap
set pppoe-options underlying-interface "$junos-underlying-interface"
set keepalives interval 30
set family inet unnumbered-address lo0.0
top
edit dynamic-profiles ancp-10302
set interfaces interface-set 10302 interface pp0 unit "$junos-interface-unit"
edit interfaces pp0 unit "$junos-interface-unit"
set ppp-options chap
set ppp-options pap
set pppoe-options underlying-interface "$junos-underlying-interface"
set keepalives interval 30
set family inet unnumbered-address lo0.0
top
edit dynamic-profiles ancp-10303
set interfaces interface-set 10303 interface pp0 unit "$junos-interface-unit"
edit interfaces pp0 unit "$junos-interface-unit"
```

```
set ppp-options chap
set ppp-options pap
set pppoe-options underlying-interface "$junos-underlying-interface"
set keepalives interval 30
set family inet unnumbered-address lo0.0
top
#
# Aggregated Ethernet Interfaces and VLAN Demux Interfaces
set interfaces ge-1/0/1 hierarchical-scheduler
set interfaces ge-1/0/1 gigether-options 802.3ad ae0
set interfaces ge-1/0/1 gigether-options 802.3ad primary
set interfaces ge-1/0/2 hierarchical-scheduler
set interfaces ge-1/0/2 gigether-options 802.3ad ae0
set interfaces ge-1/0/2 gigether-options 802.3ad backup
set interfaces ae0 hierarchical-scheduler
set interfaces ae0 stacked-vlan-tagging
set interfaces ae0 aggregated-ether-options link-protection
set interfaces demux0 unit 10301 proxy-arp
set interfaces demux0 unit 10301 vlan-tags outer 103
set interfaces demux0 unit 10301 vlan-tags inner 1
set interfaces demux0 unit 10301 demux-options underlying-interface ae0
set interfaces demux0 unit 10301 family pppoe duplicate-protection
set interfaces demux0 unit 10301 family pppoe dynamic-profile ancp-10301
set interfaces demux0 unit 10301 advisory-options downstream-rate 16m
set interfaces demux0 unit 10301 advisory-options upstream-rate 1m
set interfaces demux0 unit 10302 proxy-arp
set interfaces demux0 unit 10302 vlan-tags outer 103
set interfaces demux0 unit 10302 vlan-tags inner 2
set interfaces demux0 unit 10302 demux-options underlying-interface ae0
set interfaces demux0 unit 10302 family pppoe duplicate-protection
set interfaces demux0 unit 10302 family pppoe dynamic-profile ancp-10302
set interfaces demux0 unit 10302 advisory-options downstream-rate 16m
set interfaces demux0 unit 10302 advisory-options upstream-rate 1m
set interfaces demux0 unit 10303 proxy-arp
set interfaces demux0 unit 10303 vlan-tags outer 103
set interfaces demux0 unit 10303 vlan-tags inner 3
set interfaces demux0 unit 10303 demux-options underlying-interface ae0
set interfaces demux0 unit 10303 family pppoe duplicate-protection
set interfaces demux0 unit 10303 family pppoe dynamic-profile ancp-10303
set interfaces demux0 unit 10303 advisory-options downstream-rate 16m
set interfaces demux0 unit 10303 advisory-options upstream-rate 1m
set interfaces lo0 unit 0 family inet address 10.50.0.1/28
top
#
# Class of Service
edit class-of-service
set traffic-control-profiles tcp1 shaping-rate 16m
set traffic-control-profiles tcp1 overhead-accounting cell-mode
set interfaces interface-set 10301 output-traffic-control-profile tcp1
set interfaces interface-set 10302 output-traffic-control-profile tcp1
set interfaces interface-set 10303 output-traffic-control-profile tcp1
top
#
# ANCP
edit protocols ancp
set traceoptions file ancpd
```



```

set traceoptions file size 512m
set traceoptions flag config
set traceoptions flag cos
set qos-adjust
set adjacency-timer 5
set maximum-helper-restart-time 90
set qos-adjust-adsl 90
set qos-adjust-adsl2 95
set interfaces interface-set 10301 access-identifier "192.168.61.65/0.0.0.0 eth 1/1:7;"
set interfaces interface-set 10302 access-identifier "192.168.61.65/0.0.0.0 eth 1/2:7;"
set interfaces interface-set 10303 access-identifier "192.168.61.65/0.0.0.0 eth 1/3:7;"
set interfaces interface-set 10301 underlying-interface demux0.10301
set interfaces interface-set 10302 underlying-interface demux0.10302
set interfaces interface-set 10303 underlying-interface demux0.10303
set neighbor 10.0.0.1
top
#
# RADIUS
edit access
set radius-server 172.28.32.191 secret "$9$MUeL7VgoGqmTwYmTz3tpWLx"
edit access profile radius-profile
set authentication-order radius
set radius authentication-server 172.28.32.191
set radius accounting-server 172.28.32.191
set radius options accounting-session-id-format decimal
set radius options juniper-dsl-attributes
set radius attributes exclude dsl-forum-attributes access-request
set radius attributes exclude dsl-forum-attributes accounting-start
set radius attributes exclude dsl-forum-attributes accounting-stop
top

```

Configuring the Dynamic PPPoE Profiles

- Step-by-Step Procedure**
- In this procedure, you configure a dynamic profile for each C-VLAN: ancp-10301, ancp-10302, and ancp-10303.
1. Configure the interface set that the PPPoE sessions on this C-VLAN are placed in.


```

[edit dynamic-profiles ancp-10301]
user@host1# edit interfaces interface-set 10301

```
 2. Configure the logical interfaces to be dynamically instantiated for the interface set.


```

[edit dynamic-profiles ancp-10301 interfaces interface-set 10301]
user@host1# set interface pp0 unit "$junos-interface-unit"

```
 3. Configure CHAP and PAP authentication as properties of the dynamic PPPoE logical interfaces.


```

[edit dynamic-profiles ancp-10301 interfaces pp0 unit "$junos-interface-unit"]
user@host1# set ppp-options chap
user@host1# set ppp-options pap

```
 4. Configure the logical underlying interface on which the router creates the dynamic PPPoE logical interface; this is the interface on which the subscriber logs in.


```

[edit dynamic-profiles ancp-10301 interfaces pp0 unit "$junos-interface-unit"]
user@host1# set pppoe-options underlying-interface "$junos-underlying-interface"

```

5. Specify the interval between successive keepalive requests.

```
[edit dynamic-profiles ancp-10301 interfaces pp0 unit "$junos-interface-unit"]
user@host1# set keepalives interval 30
```

6. Configure the IPv4 protocol family and that the local (unnumbered) address can be derived from the loopback address for the dynamic PPPoE logical interfaces.

```
[edit dynamic-profiles ancp-10301 interfaces pp0 unit "$junos-interface-unit"]
user@host1# set family inet unnumbered-address lo0.0
```

7. Repeat Steps 1 through 6 for the second dynamic profile, ancp-10302, and the third dynamic profile, ancp-10303.

Results From configuration mode, confirm the dynamic profile configuration by entering the **show dynamic-profiles** command.

```
[edit]
user@host# show dynamic-profiles
ancp-10301 {
  interfaces {
    interface-set 10301 {
      interface pp0 {
        unit "$junos-interface-unit";
      }
    }
  }
  pp0 {
    unit "$junos-interface-unit" {
      ppp-options {
        chap;
        pap;
      }
      pppoe-options {
        underlying-interface "$junos-underlying-interface";
      }
      keepalives interval 30;
      family inet {
        unnumbered-address lo0.0;
      }
    }
  }
}
ancp-10302 {
  interfaces {
    interface-set 10302 {
      interface pp0 {
        unit "$junos-interface-unit";
      }
    }
  }
  pp0 {
    unit "$junos-interface-unit" {
      ppp-options {
        chap;
        pap;
      }
    }
  }
}
```

When you are done configuring the device, enter **commit** from configuration mode.

1. Enable hierarchical scheduling on this interface.
[edit interfaces ge-1/0/1]
user@host1# **set hierarchical-scheduler**
2. Specify this interface as the primary member of the aggregated Ethernet bundle.
[edit interfaces ge-1/0/1]
user@host1# **set gigether-options 802.3ad ae0 primary**
3. Enable hierarchical scheduling on a second interface.
[edit interfaces ge-1/0/2]
user@host1# **set hierarchical-scheduler**
4. Specify this interface as the backup member of the aggregated Ethernet bundle.
[edit interfaces ge-1/0/2]

```
user@host1# set gigether-options 802.3ad ae0 backup
```

5. Enable hierarchical scheduling on the aggregated Ethernet interface.

```
[edit interfaces ae0]  
user@host1# set hierarchical-scheduler
```

6. Enable stacked VLAN tagging for all logical interfaces on the aggregated Ethernet interface.

```
[edit interfaces ae0]  
user@host1# set stacked-vlan-tagging
```

7. Enable link protection as a property of the aggregated Ethernet interface.

```
[edit interfaces ae0]  
user@host1# set aggregated-ether-options link-protection
```

8. Configure VLAN demux interface demux0.10301.

- a. Configure the router to respond to ARP requests on the interface.

```
[edit interfaces demux0 unit 10301]  
user@host1# set proxy-arp
```

- b. Configure the outer VLAN tag to identify the access node (S-VLAN) and the inner VLAN tag to identify the subscriber port on the access node (C-VLAN).

```
[edit interfaces demux0 unit 10301]  
user@host1# set vlan tags outer 103 inner 1
```

- c. Specify that the VLAN demux interface runs on the underlying aggregated Ethernet interface.

```
[edit interfaces demux0 unit 10301]  
user@host1# set demux-options underlying-interface ae0
```

- d. Prevent multiple PPPoE sessions from being created for the same PPPoE subscriber on this VLAN demux interface.

```
[edit interfaces demux0 unit 10301]  
user@host1# set family pppoe duplicate-protection
```

- e. Configure the dynamic profile that is instantiated on the VLAN demux interface.

```
[edit interfaces demux0 unit 10301]  
user@host1# set family pppoe dynamic-profile ancp-10301
```

- f. Configure the recommended upstream and downstream traffic rates.

```
[edit interfaces demux0 unit 10301]  
user@host1# set advisory-options upstream-rate 1m  
user@host1# set advisory-options downstream-rate 16m
```

9. Configure VLAN demux interface demux0.10302.

- a. Configure the router to respond to ARP requests on the interface.

```
[edit interfaces demux0 unit 10302]  
user@host1# set proxy-arp
```

- b. Configure the outer VLAN tag to identify the access node (S-VLAN) and the inner VLAN tag to identify the subscriber port on the access node (C-VLAN).

```
[edit interfaces demux0 unit 10302]
user@host1# set vlan tags outer 103 inner 2
```

- c. Specify that the VLAN demux interface runs on the underlying aggregated Ethernet interface.

```
[edit interfaces demux0 unit 10302]
user@host1# set demux-options underlying-interface ae0
```

- d. Prevent multiple PPPoE sessions from being created for the same PPPoE subscriber on this VLAN demux interface.

```
[edit interfaces demux0 unit 10302]
user@host1# set family pppoe duplicate-protection
```

- e. Configure the dynamic profile that is instantiated on the VLAN demux interface.

```
[edit interfaces demux0 unit 10302]
user@host1# set family pppoe dynamic-profile ancp-10302
```

- f. Configure the recommended upstream and downstream traffic rates.

```
[edit interfaces demux0 unit 10302]
user@host1# set advisory-options upstream-rate 1m
user@host1# set advisory-options downstream-rate 16m
```

10. Configure VLAN demux interface demux0.10303.

- a. Configure the router to respond to ARP requests on the interface.

```
[edit interfaces demux0 unit 10303]
user@host1# set proxy-arp
```

- b. Configure the outer VLAN tag to identify the access node (S-VLAN) and the inner VLAN tag to identify the subscriber port on the access node (C-VLAN).

```
[edit interfaces demux0 unit 10303]
user@host1# set vlan tags outer 103 inner 3
```

- c. Specify that the VLAN demux interface runs on the underlying aggregated Ethernet interface.

```
[edit interfaces demux0 unit 10303]
user@host1# set demux-options underlying-interface ae0
```

- d. Prevent multiple PPPoE sessions from being created for the same PPPoE subscriber on this VLAN demux interface.

```
[edit interfaces demux0 unit 10303]
user@host1# set family pppoe duplicate-protection
```

- e. Configure the dynamic profile that is instantiated on the VLAN demux interface.

```
[edit interfaces demux0 unit 10303]
user@host1# set family pppoe dynamic-profile ancp-10303
```

- f. Configure the recommended upstream and downstream traffic rates.

```
[edit interfaces demux0 unit 10303]
user@host1# set advisory-options upstream-rate 1m
user@host1# set advisory-options downstream-rate 16m
```

11. Configure the IPv4 protocol family and the address of the loopback interface.

```
[edit interfaces lo0]
user@host1# set unit 0 family inet address 10.50.0.1/28
```

Results From configuration mode, confirm the static VLAN demux configuration by entering the **show interfaces** command.

```
[edit]
user@host# show interfaces
ge-1/0/1 {
  hierarchical-scheduler;
  gigether-options {
    802.3ad {
      ae0;
      primary;
    }
  }
}
ge-1/0/2 {
  hierarchical-scheduler;
  gigether-options {
    802.3ad {
      ae0;
      backup;
    }
  }
}
ae0 {
  hierarchical-scheduler;
  stacked-vlan-tagging;
  aggregated-ether-options {
    link-protection;
  }
}
demux0 {
  unit 10301 {
    proxy-arp;
    vlan-tags outer 103 inner 1;
    demux-options {
      underlying-interface ae0;
    }
    family pppoe {
      duplicate-protection;
      dynamic-profile ancp-10301;
    }
    advisory-options {
      downstream-rate 16m;
      upstream-rate 1m;
    }
  }
  unit 10302 {
    proxy-arp;
    vlan-tags outer 103 inner 2;
    demux-options {
      underlying-interface ae0;
    }
  }
}
```

```

family pppoe {
    duplicate-protection;
    dynamic-profile ancp-10302;
}
advisory-options {
    downstream-rate 16m;
    upstream-rate 1m;
}
}
unit 10303 {
    proxy-arp;
    vlan-tags outer 103 inner 3;
    demux-options {
        underlying-interface ae0;
    }
    family pppoe {
        duplicate-protection;
        dynamic-profile ancp-10303;
    }
    advisory-options {
        downstream-rate 16m;
        upstream-rate 1m;
    }
}
lo0 {
    unit 0 {
        family inet {
            address 10.50.0.1/28
        }
    }
}
}

```

When you are done configuring the device, enter **commit** from configuration mode.

Configuring Class of Service

- | | |
|-------------------------------|---|
| Step-by-Step Procedure | <ol style="list-style-type: none"> Configure the traffic-control profile with the shaping rate and specify the overhead accounting mode to account for ATM cell encapsulation.

 <pre> [edit class-of-service] user@host1# set traffic-control-profiles tcp1 shaping-rate 16m user@host1# set traffic-control-profiles tcp1 overhead-accounting cell-mode </pre> Apply the traffic-control profile to the interface sets.

 <pre> [edit class-of-service] user@host1# set interfaces interface-set 10301 output-traffic-control-profile tcp1 user@host1# set interfaces interface-set 10302 output-traffic-control-profile tcp1 user@host1# set interfaces interface-set 10303 output-traffic-control-profile tcp1 </pre> |
| Results | <p>From configuration mode, confirm the class of service configuration by entering the show class-of-service command.</p> <pre> [edit] user@host# show class-of-service </pre> |

```
traffic-control-profiles {
  tcp1 {
    shaping-rate 16m;
    overhead-accounting cell-mode;
  }
}
interfaces {
  interface-set 10301 {
    output-traffic-control-profile tcp1;
  }
  interface-set 10302 {
    output-traffic-control-profile tcp1;
  }
  interface-set 10303 {
    output-traffic-control-profile tcp1;
  }
}
```

When you are done configuring the device, enter **commit** from configuration mode.

Configuring ANCP

Step-by-Step Procedure

1. Configure the access node address.

```
[edit protocols ancp]
user@host1# set neighbor 10.0.0.1
```
2. Configure the ANCP agent to report adjusted downstream traffic rates to CoS.

```
[edit protocols ancp]
user@host1# set qos-adjust
```
3. Specify an overhead adjustment of the traffic on ADSL and ADSL2 lines to 90 percent and 95 percent, respectively, of the net data rate.

```
[edit protocols ancp]
user@host1# set qos-adjust-adsl 90
user@host1# set qos-adjust-adsl2 95
```
4. Specify an interval of 5 seconds between adjacency messages sent to all ANCP neighbors.

```
[edit protocols ancp]
user@host1# set adjacency-timer 5
```
5. Associate the ACI with the interface sets for each C-VLAN.

```
[edit protocols ancp]
user@host1# set interfaces interface-set 10301 access-identifier
"192.168.61.65/0.0.0.0 eth 1/1:7;"
user@host1# set interfaces interface-set 10302 access-identifier
"192.168.61.65/0.0.0.0 eth 1/2:7;"
user@host1# set interfaces interface-set 10303 access-identifier
"192.168.61.65/0.0.0.0 eth 1/3:7;"
```
6. Specify the underlying interface for the interface sets.

```
[edit protocols ancp]
user@host1# set interfaces interface-set 10301 underlying-interface demux0.10301
```



```

user@host1# set interfaces interface-set 10302 underlying-interface demux0.10302
user@host1# set interfaces interface-set 10303 underlying-interface demux0.10303

```

7. Configure the size of the ANCP trace log files.

```

[edit protocols ancp traceoptions]
user@host1# set file ancpd size 512m

```

8. Configure flags for tracing ANCP configuration and CoS operations.

```

[edit protocols ancp traceoptions]
user@host1# set flag config
user@host1# set flag cos

```

Results From configuration mode, confirm the ANCP agent configuration by entering the **show ancp** command.

```

[edit]
user@host# show ancp
traceoptions {
  file ancpd size 512m;
  flag config;
  flag cos;
}
qos-adjust;
adjacency-timer 5;
qos-adjust-adsl 90;
qos-adjust-adsl2 95;
interfaces {
  interface-set {
    10301 {
      access-identifier "192.168.61.65/0.0.0.0 eth 1/1:7;";
      underlying-interface demux0.10301;
    }
    10302 {
      access-identifier "192.168.61.65/0.0.0.0 eth 1/2:7;";
      underlying-interface demux0.10302;
    }
    10303 {
      access-identifier "192.168.61.65/0.0.0.0 eth 1/3:7;";
      underlying-interface demux0.10303;
    }
  }
}
neighbor 10.0.0.1;

```

When you are done configuring the device, enter **commit** from configuration mode.

Configuring RADIUS Authentication and Accounting

Step-by-Step Procedure

1. Configure the password for the RADIUS server.

```

[edit access]
user@host1# set radius-server 172.28.32.191 secret
"$9$MUeL7VgoGqmTwYmTz3tpWLx"

```

2. Specify that RADIUS is used to authenticate subscribers.

```
[edit access]
user@host1# set profile radius-profile authentication-order radius
```

3. Configure the RADIUS authentication and accounting server.

```
[edit access]
user@host1# set profile radius-profile radius authentication-server 172.28.32.191
user@host1# set profile radius-profile radius accounting-server 172.28.32.191
```

4. Configure options for the RADIUS server: The format used to identify the accounting session and that Juniper Networks DSL VSAs are added to RADIUS request messages.

```
[edit access]
user@host1# set profile radius-profile radius options accounting-session-id-format decimal
user@host1# set profile radius-profile radius options juniper-dsl-attributes
```

5. Exclude DSL Forum VSA attributes from being included in RADIUS messages.

```
[edit access]
user@host1# set profile radius-profile radius attribute exclude dsl-forum-attributes access-request
user@host1# set profile radius-profile radius attribute exclude dsl-forum-attributes accounting-start
user@host1# set profile radius-profile radius attribute exclude dsl-forum-attributes accounting-stop
```

Results From configuration mode, confirm the RADIUS configuration by entering the **show access** command.

```
[edit]
user@host# show access
radius-server {
  172.28.32.191 secret "$9$MUeL7VgoGqmTwYmTz3tpWLx"; ## SECRET-DATA
}
profile radius-profile {
  radius {
    authentication-server 172.28.32.191;
    accounting-server 172.28.32.191;
    options {
      accounting-session-id-format decimal;
      juniper-dsl-attributes;
    }
    attributes {
      exclude {
        dsl-forum-attributes [ access-request accounting-start accounting-stop ];
      }
    }
  }
}
```

When you are done configuring the device, enter **commit** from configuration mode.

Verification

To confirm that the configuration is working properly, perform these tasks:

- [Verifying the Aggregated Ethernet Interface Configuration on page 391](#)
- [Verifying the Traffic Scheduling and Shaping Parameters for the Interface Set on page 391](#)
- [Verifying the demux0 Interface Configuration on page 392](#)
- [Verifying the pp0 Interface Configuration on page 392](#)
- [Verifying the ANCP Agent Configuration on page 393](#)

Verifying the Aggregated Ethernet Interface Configuration

Purpose Verify that the interface values match your configuration, the link is up, and traffic is flowing.

Action From operational mode, enter the **show interfaces redundancy** command.

```
user@host> show interfaces redundancy
Interface  State           Last change  Primary    Secondary  Current status
ae0        On primary          ge-1/0/1    ge-1/0/2   both up
```

From operational mode, enter the **show interfaces ae0** command.

```
user@host> show interfaces ae0
Physical interface: ae0, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 606
  Link-level type: Ethernet, MTU: 1522, Speed: 1Gbps, BPDU Error: None,
  MAC-REWRITE Error: None, Loopback: Disabled, Source filtering: Disabled,
  Flow control: Disabled, Minimum links needed: 1, Minimum bandwidth needed: 0
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Current address: 00:1f:12:b8:ef:c0, Hardware address: 00:1f:12:b8:ef:c0
  Last flapped   : 2012-03-11 13:24:18 PST (2d 03:34 ago)
  Input rate     : 1984 bps (2 pps)
  Output rate    : 0 bps (0 pps)

Logical interface ae0.32767 (Index 69) (SNMP ifIndex 709)
  Flags: SNMP-Traps 0x4004000 VLAN-Tag [ 0x0000.0 ] Encapsulation: ENET2
  Statistics          Packets      pps      Bytes      bps
  Bundle:
    Input :           371259          2    46036116    1984
    Output:              0          0         0         0
  Protocol multiservice, MTU: Unlimited
  Flags: Is-Primary
```

Meaning The **show interfaces redundancy** output shows the redundant link configuration and that both link interfaces are up. The **show interfaces ae0** output shows that the aggregated Ethernet interface is up and that traffic is being received on the logical interface.

Verifying the Traffic Scheduling and Shaping Parameters for the Interface Set

Purpose Verify that the traffic scheduling and shaping parameters are configured and applied properly.

Action user@host> **show class-of-service**

Verifying the demux0 Interface Configuration

Purpose Verify that the VLAN demux interface displays the configured PPPoE family attributes and the member links in the aggregated Ethernet bundle.

Action From operational mode, enter the **show interfaces demux0** command for each VLAN.

```
user@host> show interfaces demux0.10301
Logical interface demux0.10301 (Index 76) (SNMP ifIndex 61160)
  Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.100 ]
  Encapsulation: ENET2
  Demux:
    Underlying interface: ae0 (Index 199)
  Link:
    ge-1/0/1
    ge-1/0/2
  Input packets : 2
  Output packets: 18575
  Protocol pppoe
    Dynamic Profile: ancp-10301,
    Service Name Table: None,
    Max Sessions: 16000, Duplicate Protection: On,
    AC Name: pppoe-server-1
```

Alternatively, you can enter **show pppoe underlying-interfaces detail** to display the state and PPPoE family configuration for all configured underlying interfaces.

Meaning The output shows the name of the underlying interface, the member links of the aggregated bundle, and the PPPoE family configuration. The output shows packet counts when traffic is present on the logical interface.

Verifying the pp0 Interface Configuration

Purpose Verify that the interface values match your configuration.

Action From operational mode, enter the **show interfaces pp0** command.

```
user@host> show interfaces pp0.100
Logical interface pp0.100 (Index 71) (SNMP ifIndex 710)
  Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPPoE
  PPPoE:
    State: SessionUp, Session ID: 1,
    Session AC name: pppoe-server-1, Remote MAC address: 00:90:1a:00:18:34,
    Underlying interface: demux0.10301 (Index 70)
  Link:
    ge-5/0/3.32767
    ge-5/1/2.32767
  Input packets : 18572
  Output packets: 18572
  Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
  Keepalive: Input: 0 (never), Output: 18566 (00:00:02 ago)
  LCP state: Opened
  NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured, mpls:
  Not-configured
```

```

CHAP state: Closed
PAP state: Success
  Protocol inet, MTU: 1500
    Flags: Sendbcast-pkt-to-re
    Addresses, Flags: Is-Primary
    Local: 45.63.24.1

```

Meaning This output shows information about the PPPoE logical interface created on the underlying VLAN demux interface. The output includes the PPPoE family and aggregated Ethernet redundant link information, and shows input and output traffic for the PPPoE interface.

Verifying the ANCP Agent Configuration

Purpose Verify that the ANCP values match your configuration and that traffic is flowing.

Action From operational mode, enter the **show ancp subscriber** command.

```

user@host> show ancp subscriber detail
Interface  State           Last change  Primary    Secondary  Current status
ae0        On primary      ge-1/0/1    ge-1/0/2   both up

```

From operational mode, enter the **show ancp cos** command.

```

user@host> show ancp cos

Qos Adjust Flag:      TRUE
Keepalive Timer:      30 secs
Cos State:             WRITE_READY
Connect Time:         Mon Mar 19 15:03:01 2012
Session Time:         Mon Mar 19 15:03:13 2012
Routing Instance Time: Mon Mar 19 15:03:14 2012
Keepalive Time:       Not Set
Rate Update Time:     Mon Mar 19 15:03:15 2012

```

Type	Name	Index	Pending Update	Last Update
iflset	10301	1	None	64 Kbps
iflset	10302	2	None	64 Kbps
iflset	10303	71	None	64 Kbps

Meaning The **show ancp subscriber** output shows subscriber line information such as state and the various traffic rates collected by the ANCP agent—displayed for each subscriber as identified by the ACI. The **show ancp cos** output shows that the ANCP agent is configured to send adjusted rate data to CoS, that keepalives are configured for a 30-second interval, and that the interface sets 10301, 10302, and 10303 are configured and their traffic rates are updating

Related Documentation

- *Dynamic Profiles Overview*
- *Configuring Dynamic DHCP Client Access to a Multicast Network*
- *Subscriber Interfaces and Demultiplexing Overview*
- [ANCP Agent Interactions with AAA on page 403](#)
- [ANCP DSL Attributes Mapped to Juniper Networks DSL Vendor-Specific Attributes on page 405](#)

- [Configuring the ANCP Agent on page 368](#)
- [AAA Service Framework Overview on page 3](#)

CHAPTER 43

Configuring the ANCP Agent Traffic and CoS

- [Traffic Rate Reporting and Adjustment by the ANCP Agent on page 395](#)
- [Preservation of CoS Shaping Across ANCP Agent Restarts on page 398](#)
- [Configuring the ANCP Agent to Report Traffic Rates to CoS on page 399](#)
- [Setting a Recommended Shaping Rate for Traffic on ANCP Interfaces on page 400](#)
- [Setting a Global Adjustment Factor per DSL Subscriber Line for ANCP Agent-Reported Traffic Rates on page 402](#)

Traffic Rate Reporting and Adjustment by the ANCP Agent

The ANCP agent monitors the subscriber access lines and reports to AAA and CoS information about the lines that it receives from the access node.

- [Overview on page 395](#)
- [Traffic Rate Adjustment on page 396](#)
- [Recommended Traffic Shaping Rates on page 397](#)
- [ANCP Agent Keepalives for CoS on page 398](#)

Overview

The ANCP agent reports two kinds of data rates:

- The *net data rate* is the portion of the total data rate that can be used to transmit user information. The net data rate is also called the *unadjusted* traffic rate.
- However, each DSL line type has a certain technology overhead; so the actual rate for user data is less than the net data rate. The *adjusted or calculated* rate is the net data rate reduced by the amount of technology overhead incurred by each DSL line type. The result is a closer approximation of the actual rate of subscriber data traffic. You can configure the ANCP agent to adjust the net data rate by a fixed percentage for each line type to generate the adjusted rate.

The ANCP agent reports traffic rates differently to AAA and CoS.

- The agent always reports both unadjusted and adjusted rates for both upstream and downstream traffic to AAA in response to a AAA request.

- The agent always reports only unadjusted downstream traffic rates to CoS in support of CoS traffic shaping. It never reports upstream traffic rates to CoS because CoS does not shape upstream traffic. It never reports adjusted traffic rates to CoS. In addition to the unadjusted downstream rate, the agent also reports to CoS the overhead mode and bytes for the access line; CoS can use this information when it subsequently shapes the traffic.

When you remove a shaping rate configuration that the ANCP agent previously applied, the traffic shaping rate reverts to the CoS session shaping as determined by the CoS traffic-control profiles specified in the dynamic profile. If the ANCP agent remains running but loses a connection to a particular neighbor whose subscriber traffic has been adjusted as a result of ANCP agent action, the adjusted rate remains in effect. The rate currently in effect changes only when the ANCP agent restores the connection and sends fresh updates to CoS, or when you remove the **qos-adjust** statement.

Because CoS can perform traffic shaping only when a traffic-control profile has been applied to the interface or interface set, the expectation might be that traffic shaping is always influenced by the ANCP agent when the ANCP subscriber interface or interface set has a traffic-control profile. However, this is not always true.

Consider a configuration where a subscriber logical interface is a member of an ACI-based VLAN (interface set) and therefore they share the same ACI. The dynamic profile that instantiates the subscriber interface applies a traffic-control profile to the interface. The profile that instantiates the VLAN applies an interface-shared filter instead of a traffic-control profile.

When the subscriber logs in, the first packet creates the auto-sensed, underlying VLAN. The second packet creates the ACI-based subscriber VLAN. The third packet creates the subscriber logical interface. Because the VLAN comes up first, the ANCP agent attaches to the VLAN and not to the interface.

The agent therefore reports to CoS the downstream data rate only for the VLAN, not for the logical interface. Thus CoS has no information to adjust the shaping rate for the interface, and can only shape traffic for the interface only according to the interface's traffic-control profile.

Although the agent does report the downstream rate for the VLAN, CoS cannot use that information to shape the VLAN traffic, because the VLAN does not have a traffic-control profile. Consequently, the logical interface's rate cannot be affected by the VLAN rate even though the logical interface is a member of that interface set.

Traffic Rate Adjustment

When a DSLAM determines the data rate on the subscriber local loop, it ignores the additional headers on the DSL line that are associated with the overhead of the access mode (ATM or Ethernet) and the technology of the DSL line type. However, when the ANCP agent subsequently reports a net data rate, by default it includes this overhead and therefore reports a slightly higher value than the actual subscriber data rate seen by the DSLAM.

You can configure the ANCP agent to dynamically adjust the net data rate by a fixed percentage to account for the traffic overhead. To do so, include one or more of the **qos-adjust-dsl-line-type** statements at the **[edit protocols ancp]** hierarchy level. Each of these statements sets an adjustment factor for a particular DSL line type such as ADSL or VDS2. The adjustment factor is a percentage value that the ANCP agent applies to the traffic rates it receives from the DSLAM. The percentage accounts for the traffic overhead for that line type. That is, you configure the statements for all relevant line types, and the ANCP agent applies the appropriate adjustment when it identifies the line type for the interface. The adjustment factor applies globally for all subscribers of the particular DSL line type associated with the statement: ADSL, ADSL2, ADSL+, SDS1, VDS1, or VDS2. The ANCP agent subsequently reports the adjusted rate to AAA in addition to the unadjusted data rate.

The **qos-adjust-dsl-line-type** statements are enabled by default with an adjustment factor of 100 percent, meaning that by default the ANCP agent effectively makes no adjustment to the rates.

The ANCP agent reports traffic rates to CoS only when you have included the **qos-adjust** statement at the **[edit protocols ancp]** hierarchy level. However, the ANCP agent only reports net data rates to CoS; it never reports adjusted data rates to CoS. CoS attempts to avoid traffic drops in the access node by itself adjusting the traffic shaping rate that it applies to downstream traffic for a particular VLAN or set of VLANs. The discrepancy between the actual user data rate and the agent-reported net data rate reduces the accuracy of CoS traffic shaping.

Recommended Traffic Shaping Rates

To handle a situation where the router does not receive information from the access node about the downstream and upstream calculated traffic rates for an interface, you can specify recommended *advisory* values for shaping the traffic sent to the interface so that it matches the subscriber local loop speed.

The transmit speed is the recommended traffic value in bits per second used for downstream traffic for an ANCP interface, and is conveyed in the Juniper Networks VSA, Downstream-Calculated-Qos-Rate (IANA 4874, 26–141). The receive speed is the recommended traffic value in bits per second used for upstream traffic for an ANCP interface, and is conveyed in the Juniper Networks VSA, Upstream-Calculated-Qos-Rate VSA (IANA 4874, 26–142).

To set the recommended shaping rates that are used as the default values for these VSAs in static configurations, include the **downstream-rate** and **upstream-rate** statements at the **[edit interfaces interface-name unit logical-unit-number advisory-options]** hierarchy level.

To configure the recommended rates on dynamically created VLAN interfaces, include the **upstream-rate** or **downstream-rate** statements at the **[edit dynamic-profiles profile-name interfaces \$junos-interface-ifd-name unit \$junos-interface-unit advisory-options]** hierarchy level.

To configure the recommended rates on dynamically created ACI interface sets, include the **upstream-rate** or **downstream-rate** statements at the **[edit dynamic-profiles**

`profile-name interface-set $junos-interface-set-name interfaces $junos-interface-ifd-name advisory-options]` hierarchy level.

ANCP Agent Keepalives for CoS

The ANCP agent sends a keepalive message to CoS at specific intervals. If CoS does not receive a keepalive in the expected time, it reverts the shaping rate changes it made in response to the ANCP agent. You can adjust how long CoS waits for a keepalive message by including the **maximum-helper-restart-time** statement at the **[edit protocols ancp]** hierarchy level. The interval between keepalive messages is automatically set to one-third the value of the maximum helper restart time. For example, if you set the maximum helper restart time to 120 seconds, then the ANCP agent sends keepalive messages every 40 seconds. In this example, if CoS does not receive a keepalive message within 120 seconds, then it reverts any policy changes derived from the ANCP agent.

Related Documentation

- [ANCP and the ANCP Agent Overview on page 351](#)
- [Configuring the ANCP Agent on page 368](#)
- *Shaping Rate Adjustments for Subscriber Local Loops Overview*
- *Guidelines for Configuring Shaping-Rate Adjustments for Subscriber Local Loops*
- [ANCP DSL Attributes Mapped to Juniper Networks DSL Vendor-Specific Attributes on page 405](#)
- [Preservation of CoS Shaping Across ANCP Agent Restarts on page 398](#)

Preservation of CoS Shaping Across ANCP Agent Restarts

When the ANCP agent stops due to a process or GRES, CoS enforces the ANCP downstream shaping-rates until the CoS keepalive timer expires. When the timer expires, CoS reverts to the CoS shaping-rate configured for the interfaces.

You configure the CoS keepalive timer by including the **maximum-helper-restart-time seconds** statement at the **[edit protocols ancp]** hierarchy level. It specifies how much time other daemons such as CoS wait for the ANCP agent to restart and is used to configure the CoS rate update keepalive timer.

The ANCP agent does not maintain TCP sessions from neighbors across the restart or GRES. When it restarts, it must re-establish sessions with neighbors and subscriber sessions before the timer expires. For all the re-established sessions, the ANCP agent updates CoS with the updated downstream shaping rates and provides DSL line attributes to the session database for AAA.

If CoS stops or restarts while ANCP is up, the ANCP agent retransmits all known subscriber downstream rates to CoS. Any existing adjusted shaping rates that have not been updated revert to the configured CoS shaping rates when the CoS restart timer expires.

Related Documentation

- [ANCP and the ANCP Agent Overview on page 351](#)
- [Configuring the ANCP Agent on page 368](#)

- [Specifying How Long Processes Wait for the ANCP Agent Restart to Complete on page 373](#)

Configuring the ANCP Agent to Report Traffic Rates to CoS

By default, the ANCP agent does not report the traffic rate on subscriber access lines to CoS. You can include the **qos-adjust** statement at the **[edit protocols ancp]** hierarchy level to configure the ANCP agent to report unadjusted or net downstream data rates to CoS for all subscribers in the network. This information enables CoS to subsequently shape the traffic on these access lines—but only if a shaping rate is configured in a CoS traffic-control profile for the access lines.

When a DSLAM calculates the data rate on the subscriber local loop, it ignores the additional headers on the DSL line that are associated with the overhead of the access mode (ATM or Ethernet). The unadjusted downstream data rate includes these headers in its calculation and therefore reports a slightly higher value than that calculated by the DSLAM. The ANCP agent also reports to CoS the traffic mode and the traffic rate overhead.



NOTE: The ANCP agent never reports upstream traffic rates to CoS, nor does it report adjusted downstream traffic rates to CoS.

If CoS does not receive a keepalive message within the maximum helper restart time, it considers the ANCP agent to be down and immediately reverts to the configured values any traffic shaping updates that were modified as a result of traffic reports from the ANCP agent. The configured values are maintained until the ANCP agent comes back up and sends fresh traffic updates to CoS.

However, if the ANCP agent remains running but loses the connection to a neighbor, CoS does not revert to its configured values. In this case, CoS changes the shaping rate for the subscriber traffic only if the ANCP agent restores the connection to that neighbor and reports new traffic rates to CoS or if you remove the **qos-adjust** statement.



NOTE: Always configure this statement for normal ANCP operations. You may want to disable it for debugging purposes.

To configure the ANCP agent to report unadjusted downstream traffic rates to CoS for traffic shaping:

- Specify that the ANCP agent reports traffic rates to CoS.

```
[edit protocols ancp]
user@host# set qos-adjust
```

Related Documentation

- [Traffic Rate Reporting and Adjustment by the ANCP Agent on page 395](#)
- [Configuring the ANCP Agent on page 368](#)

- [ANCP and the ANCP Agent Overview on page 351](#)
- *Shaping Rate Adjustments for Subscriber Local Loops Overview*
- *Guidelines for Configuring Shaping-Rate Adjustments for Subscriber Local Loops*
- *Enabling Shaping-Rate Adjustments for Subscriber Local Loops*
- *Disabling Shaping-Rate Adjustments for Subscriber Local Loops*
- [Specifying How Long Processes Wait for the ANCP Agent Restart to Complete on page 373](#)
- [maximum-helper-restart-time on page 800](#)

Setting a Recommended Shaping Rate for Traffic on ANCP Interfaces

When the access node sends information about the downstream and upstream calculated traffic rates for an interface, those values are used to shape the traffic sent to the interface so that it matches the subscriber local loop speed. You can specify recommended values that are used when the router does not receive this information from the access node. In this event, these recommended values are used as the default values for the following Juniper VSAs:

- Downstream-Calculated-Qos-Rate (IANA 4871, 26–141)—Conveys the transmit speed, which is the recommended traffic value in bits per second used for downstream traffic for an ANCP interface.
- Upstream-Calculated-Qos-Rate (IANA 4874, 26–142)—Conveys the receive speed, which is the recommended traffic value in bits per second used for upstream traffic for an ANCP interface.

You can configure the recommended rates either on static VLAN and VLAN demux interfaces, or you can specify them in a dynamic profile for dynamic VLAN and VLAN demux interfaces or interface sets.

To configure recommended traffic shaping values for a static interface:

1. Set the rate in bits per second for downstream traffic for the interface.

```
[edit interfaces interface-name unit logical-unit-number advisory-options]  
user@host# set downstream-rate rate
```

2. Set the rate in bits per second for upstream traffic for the interface.

```
[edit interfaces interface-name unit logical-unit-number advisory-options]  
user@host# set upstream-rate rate
```

For example, to set the recommended downstream rate to 16 Mbps and the recommended upstream rate to 1 Mbps on VLAN demux interface demux0.10301:

```
[edit interfaces demux0 unit 10301 advisory-options]  
user@host# set downstream-rate 16M  
user@host# set upstream-rate 1M
```

To configure recommended traffic shaping values for a dynamic interface:

1. Set the rate in bits per second for downstream traffic in the dynamic profile.

```
[edit dynamic-profiles profile-name interfaces $junos-interface-ifd-name unit
$junos-interface-unit advisory-options]
user@host# set downstream-rate rate
```

2. Set the rate in bits per second for upstream traffic in the dynamic profile.

```
[edit dynamic-profiles profile-name interfaces $junos-interface-ifd-name unit
$junos-interface-unit advisory-options]
user@host# set upstream-rate rate
```

For example, to configure the dynamic profile `ancp-dyn-vlan2` to set the recommended downstream rate to 10 Mbps and the recommended upstream rate to 1 Mbps on all interfaces in the dynamically created interface set:

```
[edit dynamic-profiles ancp-dyn-vlan2 interfaces $junos-interface-ifd-name unit
$junos-interface-unit advisory-options]
user@host# set downstream-rate 10M
user@host# set upstream-rate 1M
```

To configure recommended traffic shaping values for a dynamic interface set:

1. Set the rate in bits per second for downstream traffic in the dynamic profile.

```
[edit dynamic-profiles profile-name interfaces interface-set $junos-interface-set-name
interface $junos-interface-ifd-name advisory-options]
user@host# set downstream-rate rate
```

2. Set the rate in bits per second for upstream traffic in the dynamic profile.

```
[edit dynamic-profiles profile-name interfaces interface-set $junos-interface-set-name
interface $junos-interface-ifd-name advisory-options]
user@host# set upstream-rate rate
```

For example, to configure the dynamic profile `ancp-dyn-vlan1` to set the recommended downstream rate to 12 Mbps and the recommended upstream rate to 2 Mbps on all interfaces in the dynamically created interface set:

```
[edit dynamic-profiles ancp-dyn-vlan1 interfaces interface-set $junos-interface-set-name
interface $junos-interface-ifd-name advisory-options]
user@host# set downstream-rate 12M
user@host# set upstream-rate 2M
```

Related Documentation

- [Configuring the ANCP Agent on page 368](#)
- [Configuring AAA to Include Juniper Networks DSL VSAs in RADIUS Messages on page 407](#)
- [Juniper Networks VSAs Supported by the AAA Service Framework on page 21](#)
- [ANCP and the ANCP Agent Overview on page 351](#)

Setting a Global Adjustment Factor per DSL Subscriber Line for ANCP Agent-Reported Traffic Rates

The ANCP agent always reports both upstream and downstream rates to AAA. When a DSLAM calculates the data rate on the subscriber local loop, it ignores the additional headers on the DSL line that are associated with the overhead of the access mode (ATM or Ethernet). When the ANCP agent reports the net upstream data rate or the net downstream data rate, it includes the headers in its calculation and therefore reports a slightly higher value than that calculated by the DSLAM; this is the unadjusted data rate.

The ANCP agent also reports adjusted data rates to AAA. You can configure the agent to adjust the traffic rate to account for the header overhead by including one or more of the **qos-adjust-dsl-line-type** statements. Each of these statements sets an adjustment factor for a particular DSL line type that applies a percentage value to the total downstream and upstream data rates reported by the ANCP agent. That is, you configure the statements for all relevant line types, and the agent applies the appropriate adjustment when it identifies the line type for the interface. The adjustment factor applies globally for all subscribers of that DSL line type. By default, the ANCP agent applies an adjustment factor of 100 percent to all DSL lines, meaning that no adjustment is made. The ANCP agent simply passes on the DSL line rates that include the header information.



NOTE: The ANCP agent reports only unadjusted downstream data rates to CoS, and reports to CoS only when you include the **qos-adjust** statement at the **[edit protocols ancp]** hierarchy level.

To apply a global adjustment factor for DSL subscriber lines:

- Specify the adjustment factor percentage for the desired subscriber line.

```
[edit protocols ancp]
user@host# set qos-adjust-adsl adjustment-factor
user@host# set qos-adjust-adsl2 adjustment-factor
user@host# set qos-adjust-adsl2-plus adjustment-factor
user@host# set qos-adjust-sdsl1 adjustment-factor
user@host# set qos-adjust-vdsl1 adjustment-factor
user@host# set qos-adjust-vdsl2 adjustment-factor
```

Related Documentation

- [Configuring the ANCP Agent on page 368](#)
- [ANCP and the ANCP Agent Overview on page 351](#)

Configuring the ANCP Agent and AAA

- [ANCP Agent Interactions with AAA on page 403](#)
- [ANCP DSL Attributes Mapped to Juniper Networks DSL Vendor-Specific Attributes on page 405](#)
- [Configuring AAA to Include Juniper Networks DSL VSAs in RADIUS Messages on page 407](#)
- [Configuring Immediate Interim Accounting Updates to RADIUS in Response to ANCP Notifications on page 408](#)

ANCP Agent Interactions with AAA

The ANCP agent reports both unadjusted (net) data rates and adjusted data rates for subscriber traffic to AAA for RADIUS authentication and accounting of subscriber sessions. The adjusted data rate enables RADIUS to allocate the appropriate services (including class of service) to PPPoE sessions during authentication. The rate reports also enable RADIUS accounting to track the class of service actually provided for the PPPoE sessions, which in turn enables accurate billing for subscriber services.

The access nodes send ANCP DSL attributes in ANCP messages to the router, where they are stored in the shared database. AAA maps the ANCP DSL attributes to both the Juniper Networks DSL VSAs (used by RADIUS) and the DSL Forum VSA subattributes (also called the DSL Forum VSAs). RADIUS uses these attributes during authentication and accounting for PPPoE sessions on the subscriber access line. The attributes persist even when the ANCP session to a given node has ended, enabling RADIUS to later apply these attributes to new sessions on that subscriber access line. To remove the attributes, you must delete the interface or interface set for the access line from the ANCP agent configuration.

The RADIUS profile must be configured to include the **juniper-dsl-attributes** option, or AAA does not report the attributes to RADIUS. If the ANCP DSL attributes are unavailable, AAA maps the session's advisory upstream and downstream data rates (as configured on the session's underlying interface) to the Juniper Networks VSAs, Upstream-Calculated-Qos-Rate [26-142] and Downstream-Calculated-Qos-Rate [26-141], respectively. AAA subsequently provides only these VSAs to RADIUS.

For successful authentication and accounting by RADIUS, AAA has to correlate PPPoE and DHCP IP demux sessions with their access lines and their associated DSL attributes.

Some access nodes provide the ACI in PADI/PADR packets for the PPPoE sessions or in the DHCP discovery packets for DHCP IP demux sessions.

When the ACI is not provided in a 1:1 VLAN model with interface sets, you must associate the underlying interface for the sessions with the identifier and the interface set. If you do not configure this association, then only the advisory traffic rates are provided to RADIUS. This configuration has no effect when the identifier is provided by the access node.

For the N:1 VLAN model with interface sets, the access node must provide the ACI. If you configure the underlying interface for this model when the access node does not provide the identifier, the subscriber sessions can be incorrectly correlated with access lines.

AAA reports values to RADIUS for the Juniper Networks VSAs 26-141 and 26-142 according to the following scheme:

1. When the PPPoE or DHCP IP demux subscriber session can be correlated with an access line, then the ANCP agent adjusts the downstream and upstream traffic rates reported by the access node according to the ANCP agent CoS configuration. The agent then maps the adjusted rates to Upstream-Calculated-Qos-Rate [26-142] and Downstream-Calculated-Qos-Rate [26-141].
2. If the session cannot be correlated with an access line, but the PPPoE or DHCP discovery packet includes the DSL Forum VSA and the Access-Loop-Encapsulation subattribute includes a value for the AAL5 data link, then the ANCP agent adjusts the Actual-Data-Rate-Downstream and Actual-Data-Rate-Upstream subattributes to account for the ATM 48/53 cell tax. The adjusted rates mapped to Upstream-Calculated-Qos-Rate [26-142] and Downstream-Calculated-Qos-Rate [26-141].
3. If neither of the preceding sets of conditions is satisfied, then the ANCP agent simply maps the recommended downstream and upstream data rates to Upstream-Calculated-Qos-Rate [26-142] and Downstream-Calculated-Qos-Rate [26-141]. The recommended rates are either configured statically for the VLAN or VLAN demux interfaces or are in the dynamic profile that creates the interfaces.

To map an ACI to a static VLAN demux interface, include the **access-identifier *identifier*** statement at the **[edit protocols ancp interfaces demux0.logical-unit-number]** hierarchy level.

To configure advisory upstream and downstream data rates on a static VLAN demux interface, include the **upstream-rate *rate*** or **downstream-rate *rate*** statements at the **[edit interfaces demux0 unit *logical-unit-number*]** hierarchy level.

To configure an underlying interface for the PPPoE sessions in an interface set, include the **underlying-interface *interface-name*** statement at the **[edit protocols ancp interfaces interface-set *interface-set-name*]** hierarchy level.

When an ACI, and therefore a subscriber access line, has been mapped to an interface or interface set, the ACI can be re-mapped to a different interface or set. When this happens, traffic shaping is adjusted accordingly for the interfaces or interface sets involved. This capability is useful for the Business Services model, where a PPPoE session

that is initially classified as a residential household can be reclassified as a business subscriber during RADIUS authentication by using a Junos OS ICE AAA framework Op-Script application.

In the Business Services Model, the PPPoE session initially represents a residential household until RADIUS authentication and authorization takes place. The ANCP agent dynamically maps the household's access line to the appropriate subscriber interface and applies CoS traffic shaping to the interface. During authentication and authorization, the Op-Script application may classify the PPPoE session as a business subscriber rather than a residential subscriber. If this occurs, the application creates multiple static VLANs and groups them into an interface set. Based on the ANCP agent configuration, the application then statically maps the subscriber's access line to this static interface set. This interface set can include only static interfaces.

The ANCP agent reverts CoS traffic shaping from the interface previously used by the subscriber and instead applies the shaping to the interface set. This reversion means that the CoS process applies to the interface the next shaping rate in its adjustment control profile.

Related Documentation

- [ANCP and the ANCP Agent Overview on page 351](#)
- [ANCP DSL Attributes Mapped to Juniper Networks DSL Vendor-Specific Attributes on page 405](#)
- [Configuring the ANCP Agent on page 368](#)
- [Configuring AAA to Include Juniper Networks DSL VSAs in RADIUS Messages on page 407](#)

ANCP DSL Attributes Mapped to Juniper Networks DSL Vendor-Specific Attributes

Digital Subscriber Line (DSL) attributes are RADIUS vendor-specific attributes (VSAs) that are defined by the DSL Forum in RFC 4679, *DSL Forum Vendor-Specific RADIUS Attributes*. The attributes transport DSL information that is not supported by standard RADIUS attributes and which conveys details about the associated DSL subscriber line and traffic. These attributes are contained as subattributes in the single DSL Forum VSA (IANA vendor ID 3561). An ANCP access node can provide this information to the router in a PPPoE PADI message during PPPoE subscriber discovery.

The access node can also report the same information about the DSL subscriber line and traffic information by means of the ANCP DSL TLVs or attributes carried in ANCP messages to the router. The ANCP attributes are defined in RFC 6320, *Protocol for Access Node Control Mechanism in Broadband Networks*. These ANCP DSL attributes correspond to Juniper Networks (IANA vendor ID 4874) DSL VSAs and to DSL Forum VSAs.

The router simply passes the DSL line and traffic information that it receives from the access node to the RADIUS server, without performing any parsing or manipulation. A RADIUS authentication or accounting message can contain any combination of the DSL Forum VSAs and the Juniper Networks DSL VSAs. You can configure the RADIUS access profile to exclude one or more individual attributes, or all DSL Forum attributes, from being included in RADIUS messages.

The DSL Forum attribute and subattributes received by the router during PPPOE and DHCP client discovery are not updated after discovery, whereas the equivalent ANCP DSL attributes are updated whenever there is a change to the access line.

Table 45 on page 406 shows the relationship between the ANCP DSL attributes, Juniper Networks DSL VSAs, and DSL Forum VSAs.

Table 45: Mapping ANCP DSL Attributes to Juniper Networks DSL VSAs and DSL Forum VSAs

ANCP DSL Attribute Name	Juniper Networks VSA Name [Number]	DSL Forum VSA Name [Number]
Access-Aggregation-Circuit-ID-ASCII	Acc-Aggr-Cir-Id-Asc [26-112]	Access-Loop-Encapsulation [26-144]
Access-Aggregation-Circuit-ID-Binary	Acc-Aggr-Cir-Id-Bin [26-111]	Agent-Remote-Id [26-2]
Access-Loop-Circuit-ID	Acc-Loop-Cir-Id [26-110]	Agent-Circuit-Id [26-1]
Actual-Interleaving-Delay-Downstream	Act-Interlv-Delay-Dn [26-126]	Actual-Interleaving-Delay-Downstream [26-142]
Actual-Interleaving-Delay-Upstream	Act-Interlv-Delay-Up [26-124]	Actual-Interleaving-Delay-Upstream [26-140]
Actual-Net-Data-Rate-Downstream	<ul style="list-style-type: none"> L2C-Down-Stream-Data [26-93]—Unadjusted rate Act-Data-Rate-Dn [26-115]—Unadjusted rate Downstream-Calculated-Qos-Rate [26-141]—Rate as adjusted by ANCP 	Actual-Data-Rate-Downstream [26-130]
Actual-Net-Data-Rate-Upstream	<ul style="list-style-type: none"> L2C-Up-Stream-Data [26-92]—Unadjusted rate Act-Data-Rate-Up [26-114]—Unadjusted rate Upstream-Calculated-Qos-Rate [26-142]—Rate as adjusted by ANCP 	Actual-Data-Rate-Upstream [26-129]
Attainable-Net-Data-Rate-Downstream	Att-Data-Rate-Dn [26-118]	Attainable-Data-Rate-Downstream [26-134]
Attainable-Net-Data-Rate-Upstream	Att-Data-Rate-Up [26-117]	Attainable-Data-Rate-Upstream [26-133]
DSL-Line-State	DSL-Line-State [26-127]	—
DSL-Type	DSL-Type [26-128]	—
Maximum-Net-Data-Rate-Downstream	Max-Data-Rate-Dn [26-120]	Maximum-Data-Rate-Downstream [26-136]
Maximum-Net-Data-Rate-Upstream	Max-Data-Rate-Up [26-119]	Maximum-Data-Rate-Upstream [26-135]

Table 45: Mapping ANCP DSL Attributes to Juniper Networks DSL VSAs and DSL Forum VSAs (*continued*)

ANCP DSL Attribute Name	Juniper Networks VSA Name [Number]	DSL Forum VSA Name [Number]
Maximum-Interleaving-Delay-Downstream	Max-Interlv-Delay-Dn [26–125]	Maximum-Interleaving-Delay-Downstream [26–141]
Maximum-Interleaving-Delay-Upstream	Max-Interlv-Delay-Up [26–123]	Maximum-Interleaving-Delay-Upstream [26–139]
Minimum-Net-Low-Power-Data-Rate-Downstream	Min-LP-Data-Rate-Dn [26–122]	Minimum-Data-Rate-Downstream-Low-Power [26–138]
Minimum-Net-Low-Power-Data-Rate-Upstream	Min-LP-Data-Rate-Up [26–121]	Minimum-Data-Rate-Upstream-Low-Power [26–137]
Minimum-Net-Data-Rate-Downstream	Min-Data-Rate-Dn [26–116]	Minimum-Data-Rate-Downstream [26–132]
Minimum-Net-Data-Rate-Upstream	Min-Data-Rate-Up [26–115]	Minimum-Data-Rate-Upstream [26–131]

- Related Documentation**
- [Juniper Networks VSAs Supported by the AAA Service Framework on page 21](#)
 - [Configuring AAA to Include Juniper Networks DSL VSAs in RADIUS Messages on page 407](#)

Configuring AAA to Include Juniper Networks DSL VSAs in RADIUS Messages

You can include the **juniper-dsl-attributes** statement to configure AAA to add the set of Juniper Networks DSL VSAs to the RADIUS authentication and accounting request messages for subscribers. By default, these VSAs are not added to any RADIUS message. See “[ANCP DSL Attributes Mapped to Juniper Networks DSL Vendor-Specific Attributes](#)” on page 405 for a table of the Juniper Networks DSL VSAs.

After you have configured the inclusion of the Juniper Networks VSAs, you can subsequently exclude one or more of the VSAs from being transmitted. To do so, include the **exclude** statement at the **[edit access profile *profile-name* radius attributes]** hierarchy level, and specify which VSAs to exclude.

In contrast to the Juniper Networks DSL VSAs (vendor ID 4874), the DSL Forum VSA (vendor ID 3561) is added to all RADIUS messages by default. The DSL Forum VSA conveys individual DSL Forum attributes. See “[DSL Forum Vendor-Specific Attributes](#)” on page 51 for a table of these VSAs. You can use the **exclude** statement at the **[edit access profile *profile-name* radius attributes]** hierarchy level to prevent this VSA from being included in any RADIUS message.

To add the Juniper Networks DSL VSAs to RADIUS messages:

- Configure the inclusion trigger.
[edit access profile *profile-name* radius options]

```
user@host# set juniper-dsl-attributes
```

To exclude specific Juniper Networks DSL VSAs from RADIUS messages:

- Configure the exclusion trigger.

```
[edit access profile profile-name radius attributes]  
user@host# set exclude vsa-option
```

For example, to exclude the interleaving delay VSAs, configure the following statements:

```
[edit access profile profile-name radius attributes]  
user@host# set exclude max-interlv-delay-dn  
user@host# set excludemax-interlv-delay-up
```

To exclude the DSL Forum (RFC 4679) VSA from RADIUS messages:

- Configure the exclusion trigger.

```
[edit access profile profile-name radius attributes]  
user@host# set exclude dsl-forum-attributes
```

Related Documentation

- [Configuring the ANCP Agent on page 368](#)
- [Setting a Recommended Shaping Rate for Traffic on ANCP Interfaces on page 400](#)
- [Juniper Networks VSAs Supported by the AAA Service Framework on page 21](#)
- [ANCP DSL Attributes Mapped to Juniper Networks DSL Vendor-Specific Attributes on page 405](#)
- [ANCP and the ANCP Agent Overview on page 351](#)

Configuring Immediate Interim Accounting Updates to RADIUS in Response to ANCP Notifications

When an ANCP neighbor reports a change in the upstream traffic rate or downstream traffic rate of an access line, the ANCP agent immediately passes the information to AAA. By default, AAA does not pass this information on to the RADIUS server until the next accounting update. However, you can configure AAA to report the rate change immediately.

When the access profile includes both the **ancp-speed-change-immediate-update** statement and the **update-interval** statement, receipt of the notification from the ANCP agent triggers AAA to send an interim update Accounting-Request message to the RADIUS server for the PPPoE and DHCP IP demux subscribers associated with that access line. The interim update request includes the new access line parameters and the adjusted upstream and downstream traffic rates.

To configure AAA to immediately send rate change information from the ANCP agent to the RADIUS server with interim accounting updates:

1. Enable interim accounting updates and configure the number of minutes between the updates.

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

2. Specify the immediate update.

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

**Related
Documentation**

- [Configuring the ANCP Agent on page 368](#)
- [Configuring Per-Subscriber Session Accounting on page 92](#)

Monitoring and Managing ANCP for Subscriber Access

- [Triggering ANCP OAM to Test the Local Loop on page 411](#)
- [Verifying and Monitoring ANCP Neighbors on page 412](#)
- [Clearing ANCP Neighbors on page 412](#)
- [Verifying and Monitoring ANCP Subscribers on page 413](#)
- [Clearing ANCP Subscribers on page 413](#)
- [Verifying and Monitoring CoS for ANCP Subscribers on page 414](#)
- [Clearing and Verifying ANCP Statistics on page 414](#)

Triggering ANCP OAM to Test the Local Loop

You can trigger ANCP OAM to perform a loopback test on the local loop between the access node and the CPE to help isolate simple faults. On an ATM-based local loop, the ANCP operation triggers the access node to generate ATM (F4/F5) loopback cells on the local loop. On an Ethernet-based local loop, the ANCP operation triggers the access node to generate an Ethernet loopback message on the local loop. When the test completes, the access node sends a message to the router with the results.

Issue the **request ancp oam neighbor** command from CLI operational mode to initiate testing of a local loop identified by the IP address or system name of the ANCP neighbor and the ACI for a subscriber on that access node.

Issue the **request ancp oam interface** command from CLI operational mode to initiate testing of a local loop identified by the ANCP interface or interface set associated with a subscriber and the ACI for a subscriber on that access node.

With both commands, you can also specify how many times the test must be run and how long the router waits for a response to the OAM request.

To initiate ANCP local loop testing:

- Identify the loop by the subscriber identifier and the neighbor's IP address; optionally specify how many times the test runs and the timeout period.

```
user@host> request ancp oam neighbor ip-address 192.168.32.5 subscriber "dslam  
port-2-10" count 5 timeout 600
```

- Identify the loop by the subscriber identifier and the neighbor's system name; optionally specify how many times the test runs and the timeout period.

```
user@host> request ancp oam neighbor system-name ba:ad:be:ef:10:10 subscriber  
"dslam port-2-10" count 10 timeout 600
```

- Identify the loop by the subscriber identifier and the interface associated with the subscriber; optionally specify how many times the test runs and the timeout period.

```
user@host> request ancp oam interface ge-1/0/2.12 identifier-string timeout 15
```

- Identify the loop by the subscriber identifier and the set of interfaces associated with the subscriber; optionally specify how many times the test runs and the timeout period.

```
user@host> request ancp oam interface interface-set vlan5 identifier-string count 3
```

- Related Documentation**
- [ANCP and the ANCP Agent Overview on page 351](#)
 - [Configuring the ANCP Agent on page 368](#)

Verifying and Monitoring ANCP Neighbors

Purpose View ANCP neighbor information:

- Action**
- To display summary information about all ANCP neighbors:

```
user@host> show ancp neighbor
```

- To display information about a specific ANCP neighbor, add the IP address or MAC address to the command:

```
user@host> show ancp neighbor 10.25.64.21
```

- To display detailed information, add **detail** to the command:

```
user@host> show ancp neighbor detail
```

```
user@host> show ancp neighbor ba:ad:be:ef:10:10 detail
```

- To display a count of ANCP neighbors in various states and the total number of neighbors, or a count of DSL lines in various states for all subscribers for a particular neighbor:

```
user@host> show ancp summary neighbor
```

```
user@host> show ancp summary neighbor 10.25.64.21
```

- To display total and state-wise counts of both ANCP neighbors and subscribers:

```
user@host> show ancp summary
```

- Related Documentation**
- [CLI Explorer](#)

Clearing ANCP Neighbors

Purpose Clear ANCP neighbor information.

- Action**
- To clear connections with all ANCP neighbors:


```
user@host> clear ancp neighbor
```

- To clear the connection with a specific ANCP neighbor, add the IP address or MAC address to the command:

```
user@host> clear ancp neighbor ip-address 10.25.64.21
```

```
user@host> clear ancp neighbor system-name ba:ad:be:ef:10:10
```

- To verify that the connection has been cleared:

```
user@host> show ancp neighbor
```

```
user@host> show ancp neighbor 10.25.64.21
```

```
user@host> show ancp neighbor ba:ad:be:ef:10:10
```

Related Documentation

- [CLI Explorer](#)

Verifying and Monitoring ANCP Subscribers

Purpose View ANCP subscriber (local access loop) information:

- Action**
- To display summary information about all ANCP subscribers:

```
user@host> show ancp subscriber
```

- To display information about all ANCP subscribers connected through a particular ANCP neighbor:

```
user@host> show ancp subscriber neighbor 10.25.64.21
```

- To display information about an ANCP subscriber specified by the ACI:

```
user@host> show ancp subscriber "port-2-11"
```

- To display detailed information, add **detail** to the command:

```
user@host> show ancp subscriber detail
```

```
user@host> show ancp subscriber neighbor 10.25.64.21 detail
```

- To display a count of subscribers in various states and the total number of subscribers:

```
user@host> show ancp summary subscriber
```

- To display total and state-wise counts of both ANCP neighbors and subscribers:

```
user@host> show ancp summary
```

Related Documentation

- [CLI Explorer](#)

Clearing ANCP Subscribers

Purpose Clear ANCP subscriber information.

- Action**
- To clear connections with all ANCP subscribers:

```
user@host> clear ancp subscriber
```

- To clear the connection with an ANCP subscriber identified by a particular ACI on all neighbors, add the identifier to the command:

```
user@host> clear ancp subscriber identifier port-2-10
```

- To clear the connection with an ANCP subscriber identified by a particular ACI on a specific neighbor, add the identifier and either the IP address or MAC address to the command:

```
user@host> clear ancp subscriber identifier port-2-10 ip-address 10.25.64.21
```

```
user@host> clear ancp subscriber identifier port-2-10 system-name ba:ad:be:ef:10:10
```

- To verify that the connection has been cleared:

```
user@host> show ancp subscriber
```

Related
Documentation

- [CLI Explorer](#)

Verifying and Monitoring CoS for ANCP Subscribers

Purpose View ANCP CoS state information:

- Action**
- To display summary information about the CoS state for all ANCP subscribers:

```
user@host> show ancp cos
```

- To display information about the CoS state for an ANCP subscriber specified by the ACI:

```
user@host> show ancp cos "port-2-11"
```

- To display the most recently updated CoS information:

```
user@host> show ancp cos last-update
```

- To display the CoS information that is pending (will be used to update the fields):

```
user@host> show ancp cos pending-update
```

Related
Documentation

- [CLI Explorer](#)

Clearing and Verifying ANCP Statistics

Purpose Clear ANCP statistics.

- Action**
- To clear all ANCP statistics:

```
user@host> clear ancp statistics
```

- To clear statistics for a specific ANCP neighbor, add the IP address or MAC address to the command:

```
user@host> clear ancp statistics ip-address 10.25.64.21
```

```
user@host> clear ancp statistics system-name ba:ad:be:ef:10:10
```

- To verify that the connection has been cleared:

user@host> [show ancp neighbor](#)

**Related
Documentation**

- [ANCP and the ANCP Agent Overview on page 351](#)

PART 7

Configuring the Diameter Base Protocol

- [Configuring Diameter and its Applications on page 419](#)
- [Configuring Gx-Plus for Provisioning Subscribers on page 439](#)
- [Configuring JSRC in Subscriber Access Networks on page 451](#)
- [Configuring Service Accounting with JSRC on page 459](#)
- [Configuring Subscribers on Static Interfaces on page 463](#)
- [Configuring the Static Subscribers Global Profile on page 471](#)
- [Configuring the Static Subscribers Group Profile on page 475](#)
- [Configuring the PTSP Feature to Support Dynamic Subscribers on page 479](#)
- [Configuring the PTSP Partition to Connect to the External Policy Manager on page 489](#)
- [Configuring PTSP Services and Rules on page 493](#)
- [Monitoring and Managing Diameter Information for Subscriber Access on page 501](#)
- [Monitoring and Managing Subscriber Information on Static Interfaces on page 505](#)
- [Monitoring and Managing Packet-Triggered Subscribers on page 507](#)

CHAPTER 46

Configuring Diameter and its Applications

- [Diameter Base Protocol Overview on page 419](#)
- [Messages Used by Diameter Applications on page 421](#)
- [Diameter AVPs and Diameter Applications on page 426](#)
- [Configuring Diameter on page 434](#)
- [Configuring the Origin Attributes of the Diameter Instance on page 435](#)
- [Configuring Diameter Peers on page 435](#)
- [Configuring the Diameter Transport on page 436](#)
- [Configuring Diameter Network Elements on page 437](#)

Diameter Base Protocol Overview

The Diameter protocol is defined in *RFC 3588, Diameter Base Protocol*, and provides an alternative to RADIUS that is more flexible and extensible. The Diameter base protocol provides basic services to one or more applications (also called functions) that each runs in a different Diameter instance. The individual application provides the extended AAA functionality. Applications that use Diameter include Gx-Plus, JSRC, and PTSP.

Diameter peers communicate over a reliable TCP transport layer connection by exchanging Diameter messages that convey status, requests, and acknowledgments by means of standard Diameter AVPs and application-specific AVPs. The Diameter transport layer configuration is based on Diameter network elements (DNEs); multiple DNEs per Diameter instance are supported. Currently only the predefined *master* Diameter instance is supported, but you can configure alternative values for many of the master Diameter instance values.

Each DNE consists of a prioritized list of peers and a set of routes that define how traffic is forwarded. Each route associates a destination with a function, a function partition, and a metric. When an application sends a message to a routed destination, all routes within the Diameter instance are examined for a match. When the best route to the destination has been selected, the message is forwarded by means of the DNE that includes that route.

Multiple routes to the same destination can exist within a given DNE and in different DNEs. In the case of multiple routes that match a request for forwarding, the best route is selected as follows:

1. The route with the lowest metric is selected.
2. In the event of a tie, the route with the highest specification score is selected.
3. In the event of another tie, then the names of the DNEs are compared in lexicographical order. The route in the DNE with the lowest value is selected. For example, `dne-austin` has a lower value than `dne-boston`.
4. If the routes are tied within the same DNE, then the route names are compared in lexicographical order. The route with the lowest value is selected.

The specification score of a route is 0 by default. Points are added to the score as follows:

- If the destination realm matches the request, add 1.
- If the destination host matches the request, add 2.
- If the function matches the request, add 3.
- If the function partition matches the request, add 4.

When the state of any DNE changes, the route lookup for all destinations is reevaluated. All outstanding messages to routed destinations are rerouted as needed, or discarded.

To configure a Diameter network element, include the **network-element** statement at the **[edit diameter]** hierarchy level. Include the **route** statement at the **[edit diameter network-element element-name forwarding]** hierarchy level.

To configure a route for the DNE, include the **destination** (optional), **function** (optional), and **metric** statements at the **[edit diameter network-element element-name forwarding route dne-route-name]** hierarchy level.

Specify the Diameter peers associated with the DNE by including one or more **peer** statements at the **[edit diameter network-element element-name]** hierarchy level.

Set the priority for each peer with the **priority** statement at the **[edit diameter network-element element-name peer peer-name]** hierarchy level.

Diameter requires you to configure information about the origin node; this is the endpoint node that originates Diameter for the Diameter instance. Include the **host** and **realm** statements at the **[edit diameter]** hierarchy level to configure the Diameter origin.

You can optionally configure one or more *transports* to specify the source (local) address of the transport layer connection. To configure a Diameter transport, include the **transport** statement at the **[edit diameter]** hierarchy level. Then include the **address** statement at the **[edit diameter transport transport-name]** hierarchy level.

You can optionally specify a logical system and routing instance for the connection by including the **logical-system** and **routing-instance** statements at the **[edit diameter transport transport-name]** hierarchy level. By default, Diameter uses the *default* logical

system and *master* routing instance. The logical system and routing instance for the transport connection must match that for the peer, or a configuration error is reported.

Each Diameter peer is specified by a name. Peer attributes include address and the destination TCP port used by active connections to this peer. To configure a Diameter peer, include the **peer** statement at the **[edit diameter]** hierarchy level, and then include the **address** and **connect-actively** statements at the **[edit diameter peer *peer-name*]** hierarchy level.

To configure the active connection, include the **port** and **transport** statements at the **[edit diameter peer *peer-name* connect-actively]** hierarchy level. The assigned transport identifies the transport layer source address used to establish active connections to the peers. **transport** statements.

Related Documentation

- [Configuring Diameter on page 434](#)
- [Messages Used by Diameter Applications on page 421](#)
- [Diameter AVPs and Diameter Applications on page 426](#)
- [Juniper Networks Session and Resource Control \(SRC\) and JSRC Overview on page 451](#)
- [Juniper Networks Session and Resource Control \(SRC\) and PTSP Overview on page 480](#)
- [Gx-Plus for Provisioning Subscribers Overview on page 439](#)

Messages Used by Diameter Applications

The following Diameter applications are supported by Junos OS:

- JSRC—A Juniper Networks Diameter application registered with the IANA (<http://www.iana.org>) as Juniper Policy-Control-JSRC, with an ID of 16777244. Communicates with the SAE (remote SRC peer).
- PTSP—A Juniper Networks Diameter application registered with the IANA (<http://www.iana.org>) as Juniper JGx, with an ID of 16777273. Communicates with the SAE (remote SRC peer).
- Gx-Plus—An application that extends the 3GPP Gx interface for wireline use cases. 3GPP Gx is registered with the IANA (<http://www.iana.org>). Communicates with a PCRF.

If data for a particular AVP included in a message is not available to the router, Gx-Plus simply omits the AVP from the message it sends to the PCRF. If the PCRF determines it has insufficient information to make a decision, it may deny the request. The Diameter answer messages include the Result-Code AVP (AVP 268); the values of this AVP convey success, failure, or errors to the requestor.

Juniper Networks has also registered the Juniper-Session-Recovery application (16777296) and two new command codes (8388628 for Juniper-Session-Events and 8388629 for Juniper-Session-Discovery) with the IANA (<http://www.iana.org>).

[Table 46 on page 422](#) describes Diameter messages the applications use.

Table 46: Diameter Messages and Diameter Applications

Diameter Message	Code	Application	Description
AA-Request (AAR)	265	JSRC, PTSP	Request from the application to the SAE at new subscriber login or during SAE-application synchronization. The request can be one of three types: address-authorization, provisioning-request, or synchronization.
AA-Answer (AAA)	265	JSRC, PTSP	Response from the SAE to the application's AA-Request message.
Abort-Session-Request (ASR)	274	JSRC, PTSP	Request from the SAE to the application to log out a provisioned subscriber.
Abort-Session-Answer (ASA)	274	JSRC, PTSP	Response from the application to the SAE's ASR message. If the application sends the logout request to AAA, the ASA message includes a success notification (ACK). If the logout failed, the ASA message includes a failure notification (NAK).
Accounting-Request (ACR)	271	JSRC, PTSP	Request from the SAE to the application or from the application to the SAE for statistics.
Accounting-Answer (ACA)	271	JSRC, PTSP	Response to the ACR message to provide statistics for each installed policy (service).

Table 46: Diameter Messages and Diameter Applications (*continued*)

Diameter Message	Code	Application	Description
Credit-Control-Request (CCR)	272	Gx-Plus	<p>Request from Gx-Plus to the PCRF at subscriber login, logout, or update.</p> <p>An initial request (CCR-I) is sent when a subscriber logs in and AAA is requested to activate the subscriber's session. Gx-Plus retries the CCR-I message if a CCA-I message is not received from the PCRF within 10 seconds. The CCR-I message is retried up to 3 times.</p> <p>If no CCA-I is received after the 4 CCR-I messages have been sent—the first message plus 3 retries—then Gx-Plus starts sending CCR-N messages. CCR-N messages are retried forever until a success or failure response is received from the PCRF. CCR-N messages include the Juniper-Provisioning-Source AVP (AVP code 2101) set to local to notify the PCRF that the router has the authority to make a local decision regarding subscriber service activation.</p> <p>An update request (CCR-U) message is sent when a usage threshold is reached. The CCR-U reports the actual usage for all statistics. The PCRF may return a CCA-U message that includes new monitoring thresholds, service activations, service deactivations.</p> <p>A CCR-U is also sent to report the status of service activation or deactivation.</p> <p>A termination request (CCR-T) is sent at subscriber logout to inform the PCRF that a provisioned subscriber session is being terminated. CCR-T messages are retried forever until a success response is received from the PCRF.</p>

Table 46: Diameter Messages and Diameter Applications (*continued*)

Diameter Message	Code	Application	Description
Credit-Control-Answer (CCA)	272	Gx-Plus	<p>Reply from the PCRF to a CCR message.</p> <p>In response to a CCR-I, the PCRF returns a CCA-I message that indicates success (DIAMETER_SUCCESS) or failure (DIAMETER_AUTHORIZATION_REJECTED) depending on whether the subscriber has sufficient credit for the requested services. All other responses are ignored and the CCR-I is retried.</p> <p>In response to a CCR-T, the PCRF returns a CCA-T message that indicates a successful termination with a value of 2001 (DIAMETER_SUCCESS) in the Result-Code AVP. All other responses are ignored and the CCR-T is retried.</p> <p>A CCA-N is a response to a CCR-N.</p>
Juniper-Session-Discovery-Request (JSDR)	8388629	Gx-Plus	Discovery request from the PCRF to Gx-Plus to discover subscriber sessions on the router.
Juniper-Session-Discovery-Answer (JSDA)	8388629	Gx-Plus	<p>Reply from router to a JSDR message; describes session information. The Result-Code AVP includes one of the following values, or an error value:</p> <ul style="list-style-type: none"> • 2001—DIAMETER_SUCCESS; the end of the database was reached, meaning all information has been sent. • 2002—DIAMETER_LIMITED_SUCCESS; some of the session information was sent, but more remains to be sent.
Juniper-Session-Event-Request (JSER)	8388628	Gx-Plus	Request from router to PCRF regarding events that take place on the router. Notifies the PCRF of certain events on the router by including the Juniper-Event-Type AVP (AVP code 2103). Events reported include cold or warm boots, explicit discovery requests, substantial configuration changes, non-response or error response from PCRF, and exhaustion of fault-tolerant resources.
Juniper-Session-Event-Answer (JSEA)	8388628	Gx-Plus	Reply from PCRF to a JSER message.
Push-Profile-Request (PPR)	288	JSRC, PTSP	Request from the SAE to the router to activate or deactivate services for a subscriber.

Table 46: Diameter Messages and Diameter Applications (*continued*)

Diameter Message	Code	Application	Description
Push-Profile-Answer (PPA)	288	JSRC, PTSP	Response from the router to the SAE's PPR message. Includes success or failure notification for each of the service activation or deactivation commands in the request.
Re-Auth-Request (RAR)	258	Gx-Plus	Audit request from the PCRF to router to determine whether a specific subscriber is still present.
Re-Auth-Answer (RAA)	258	Gx-Plus	Reply from router to a RAR message; indicates whether the subscriber is active. The Result-Code AVP includes one of the following values: <ul style="list-style-type: none"> • 2001—DIAMETER_SUCCESS; subscriber entry was found. • 5002—DIAMETER_UNKNOWN_SESSION_ID; subscriber entry was not found. • 3002—DIAMETER_UNABLE_TO_DELIVER; Gx-Plus is not configured.
Session-Resource-Query (SRQ)	277	JSRC, PTSP	Request from the router to the SAE or from the SAE to the router to initiate synchronization between router and the SAE.
Session-Resource-Reply (SRR)	277	JSRC, PTSP	Response to the SRQ message to begin synchronization.
Session-Termination-Request (STR)	275	JSRC, PTSP	Notification from the router to the SAE that a provisioned subscriber has logged out.
Session-Termination-Answer (STA)	275	JSRC, PTSP	Response from the SAE to the router's STR message. Includes success or failure notification.

Related Documentation

- [Juniper Networks Session and Resource Control \(SRC\) and JSRC Overview on page 451](#)
- [Understanding JSRC-SAE Interactions on page 453](#)
- [Juniper Networks Session and Resource Control \(SRC\) and PTSP Overview on page 480](#)
- [Understanding PTSP-SAE Interactions on page 481](#)
- [Gx-Plus for Provisioning Subscribers Overview on page 439](#)
- [Understanding Gx-Plus Interactions Between the Router and the PCRF on page 441](#)

Diameter AVPs and Diameter Applications

Diameter conveys information by including various attribute-value pairs (AVPs) in Diameter messages. [Table 47 on page 426](#) lists the standard Diameter AVPs used in interactions with the supported Diameter applications. Diameter reserves AVP code numbers 0 through 255 for RADIUS AVPs that are implemented in Diameter.

Table 47: Standard Diameter AVPs

Attribute Number	Diameter AVP	Application	Description	Type
1	User-Name	Gx-Plus, JSRC	Specifies the username. For a subscriber managed by AAA, the value is the subscriber's login name. For a static interface, the value is the interface name, which is used as the subscriber's login name.	UTF8String
8	Framed-IP-Address	Gx-Plus, JSRC, PTSP	Identifies the IPv4 address configured for the subscriber. This is the same value as for RADIUS Framed-IP-Address attribute [8].	OctetString
55	Event-Timestamp	Gx-Plus, JSRC, PTSP	Specifies the time of the event that triggered the message in which this AVP is included. Time is indicated in seconds since January 1, 1900, 00:00 UTC.	Time
85	Acct-Interim-Interval	JSRC, PTSP	<p>Number of seconds between each interim accounting update for this session.</p> <p>The router uses the following guidelines for interim accounting:</p> <ul style="list-style-type: none"> Attribute value is within the acceptable range (600 through 86,400 seconds)—Accounting is updated at the specified interval. Attribute value is less than the minimum acceptable value—Accounting is updated at the minimum interval (600 seconds). Attribute value is greater than the maximum acceptable value—Accounting is updated at the maximum interval (86,400 seconds). 	Unsigned32
87	NAS-Port-Id	Gx-Plus, JSRC, PTSP	Identifies the port of the NAS that authenticates the user. This is the same value as for RADIUS NAS-Port-Id attribute [87].	UTF8String
263	Session-ID	Gx-Plus, JSRC, PTSP	Specifies the subscriber session identifier. The router assigns the value to uniquely identify a subscriber session.	UTF8String

Table 47: Standard Diameter AVPs (*continued*)

Attribute Number	Diameter AVP	Application	Description	Type
268	Result-Code	Gx-Plus, JSRC, PTSP	<p>Indicates whether a request completed successfully. Provides an error code if the request failed.</p> <p>The following classes are recognized by Diameter:</p> <ul style="list-style-type: none"> • 1xxx—Informational • 2xxx—Success • 3xxx—Protocol errors • 4xxx—Transient errors • 5xxx—Permanent failures <p>Unrecognized classes, which begin with numerals 6–9 or 0, are handled as permanent failures.</p> <p>JSRC and PTSP support the following values; all non-success values are treated as permanent failures:</p> <ul style="list-style-type: none"> • 1001—DIAMETER MULTI ROUND AUTH • 2001—DIAMETER SUCCESS • 5002—DIAMETER UNKNOWN SESSION ID • 5012—DIAMETER UNABLE TO COMPLY <p>JSRC also supports the following value, which is treated as a permanent failure:</p> <ul style="list-style-type: none"> • 3004—DIAMETER TOO BUSY; this is a transient condition, typically when the router already has a request in process for a specified subscriber. <p>Gx-Plus supports the following values for errors in a PCRF response; when these values are received or the response is malformed or unrecognizable, the request is retried.</p> <ul style="list-style-type: none"> • 3001—DIAMETER COMMAND NOT SUPPORTED; the application is not running or the command is not recognized. • 3004—DIAMETER TOO BUSY; the received message is above either the quota of downstream transactions or the outstanding message memory limit for messages from the network. • 5012—DIAMETER UNABLE TO COMPLY; the received message is greater than the local limit. 	Unsigned32

Table 47: Standard Diameter AVPs (*continued*)

Attribute Number	Diameter AVP	Application	Description	Type
277	Auth-Session-State	JSRC, PTSP	Indicates whether AAA session state is maintained. <ul style="list-style-type: none"> 0—STATE MAINTAINED 1—NO STATE MAINTAINED 	Enumerated
295	Termination-Cause	JSRC, PTSP	Indicates the reason why a session was terminated on the access device. <ul style="list-style-type: none"> 1—DIAMETER LOGOUT 2—DIAMETER SERVICE NOT PROVIDED 3—DIAMETER BAD ANSWER 4—DIAMETER ADMINISTRATIVE 5—DIAMETER LINK BROKEN 6—DIAMETER AUTH EXPIRED 7—DIAMETER USER MOVED 8—DIAMETER SESSION TIMEOUT 	Enumerated
415	CC-Request-Number	Gx-Plus	Identifies a request within a session. The combination of Session-Id and CC-Request-Type is globally unique. The number is incremented for each request during the course of a session. The number is reset when a router high availability event takes place.	Unsigned32
416	CC-Request-Type	Gx-Plus	Specifies the type of credit control request: <ul style="list-style-type: none"> INITIAL REQUEST (1) UPDATE REQUEST (2) TERMINATION_REQUEST (3) EVENT REQUEST (4) 	Enumerated
431	Granted-Service-Unit	Gx-Plus	Contains the amount that can be provided of one or more of the following requested units specified by the client: CC-Input-Octets, CC-Output-Octets, CC-Time, or CC-Total-Octets. Included in CCA-I messages, and may be included in CCA-U messages.	Grouped
446	Used-Service-Unit	Gx-Plus	Contains the amount of the requested units that have been actually used; measured from 4 when the service is activated. The units are one or more of the following requested units specified by the client: CC-Input-Octets, CC-Output-Octets, CC-Time, or CC-Total-Octets. Included in CCR-U messages.	Grouped

Table 47: Standard Diameter AVPs (*continued*)

Attribute Number	Diameter AVP	Application	Description	Type
480	Accounting-Record-Type	JSRC, PTSP	<p>Specifies the type of account record for service accounting:</p> <ul style="list-style-type: none"> • INTERIM_RECORD—Accounting record sent between the start and stop records, at intervals specified by the Acct-Interim-Interval AVP (AVP code 85). It contains cumulative accounting data for the existing accounting session. • START_RECORD—Accounting record sent when the service is activated to initiate the accounting session. It contains accounting data relevant to the initiation of that session. • STOP_RECORD—Accounting record sent when the service is deactivated to terminate the accounting session. It contains cumulative data relevant to that session. 	Enumerated
1001	Charging-Rule-Install	Gx-Plus	Requests the installation of the rule (activation of the service) designated by the included Charging-Rule-Name AVP (1005). This AVP has a vendor ID of 10415 (3GPP).	Grouped
1002	Charging-Rule-Remove	Gx-Plus	Requests the removal of the rule (deactivation of the service) designated by the included Charging-Rule-Name AVP (1005). This AVP has a vendor ID of 10415 (3GPP).	Grouped
1005	Charging-Rule-Name	Gx-Plus	Name of a specific rule that has been installed, modified, or removed.	OctetString
1066	Monitoring-Key	Gx-Plus	Specifies which of the monitoring structures to use. Included in Charging-Rule-Install AVP (1001). The MX router does not support aggregation of statistics across services, so the value of this AVP must be different for each service. This AVP has a vendor ID of 10415 (3GPP).	OctetString
1067	Usage-Monitoring-Information	Gx-Plus	Sets monitoring thresholds. When service statistics match at least one of the granted service values, the router sends a CCR-U report with the current statistics to the PCRF. Includes the Monitoring-Key AVP (1066) and the Granted-Service-Unit AVP (431). This AVP has a vendor ID of 10415 (3GPP).	Grouped

Juniper Networks AVPs are used in addition to the standard Diameter AVPs. These AVPs have an enterprise number of 2636. [Table 48 on page 430](#) lists the Juniper Networks AVPs that the supported Diameter applications use.

Table 48: Juniper Networks Diameter AVPs

Attribute Number	Diameter AVP	Application	Description	Type
2004	Juniper-Service-Bundle	JSRC	Specifies the name of the service bundle.	OctetString
2010	Juniper-DHCP-Options	JSRC	Specifies the client's DHCP options.	OctetString
2011	Juniper-DHCP-GI-Address	JSRC	Specifies the DHCP relay agent's IP address.	OctetString
2020	Juniper-Policy-Install	JSRC, PTSP	Specifies policies to be activated for the subscriber. Includes Juniper-Policy-Name and Juniper-Policy-Definition	Grouped
2021	Juniper-Policy-Name	JSRC, PTSP	Defines the name of a policy decision.	OctetString
2022	Juniper-Policy-Definition	JSRC, PTSP	Defines a policy decision. Includes Juniper-Policy-Name, Juniper-Template-Name, and Juniper-Substitution.	Grouped
2023	Juniper-Template-Name	JSRC, PTSP	Profile name defined by the router. PTSP supports only the <code>__svc_rule__</code> policy template.	UTF8String
2024	Juniper-Substitution	JSRC, PTSP	Defines the substitution attributes. Includes Juniper-Substitution-Name and Juniper-Substitution-Value.	OctetString
2025	Juniper-Substitution-Name	JSRC, PTSP	Defines the name of the variable to be replaced.	OctetString
2026	Juniper-Substitution-Value	JSRC, PTSP	Defines the value of the variable to be replaced.	OctetString
2027	Juniper-Policy-Remove	JSRC, PTSP	Specifies policies to be deactivated for the subscriber. Includes Juniper-Policy-Name.	Grouped
2035	Juniper-Policy-Failed	JSRC, PTSP	Specifies the name of the policy activation or deactivation that failed.	OctetString
2038	Juniper-Policy-Success	JSRC, PTSP	Specifies the name of the policy activation or deactivation that succeeded.	OctetString
2046	Juniper-Logical-System	JSRC, PTSP	Specifies the logical system.	UTF8String
2047	Juniper-Routing-Instance	JSRC, PTSP	Specifies the routing instance.	UTF8String
2048	Juniper-Jsrc-Partition	JSRC, PTSP	Specifies the logical system and routing instance for the subscriber or request. Includes Juniper-Logical-System and Juniper-Routing-Instance	Grouped

Table 48: Juniper Networks Diameter AVPs (*continued*)

Attribute Number	Diameter AVP	Application	Description	Type
2050	Juniper-Request-Type	JSRC, PTSP	Describes the type of request: <ul style="list-style-type: none"> 1—ADDRESS_AUTHORIZATION 2—PROVISIONING_REQUEST 3—SYNCHRONIZATION 	Enumerated
2051	Juniper-Synchronization-Type	JSRC, PTSP	Describes the type of synchronization: <ul style="list-style-type: none"> 1—FULL-SYNC 2—FAST-SYNC 3—NO-STATE-TO-SYNC 	Enumerated
2052	Juniper-Synchronization	JSRC, PTSP	Describes the state of synchronization: <ul style="list-style-type: none"> 1—NO-SYNC; this is the default state 2—SYNC-IN-PROGRESS 3—SYNC-COMPLETE 	Enumerated
2053	Juniper-Acct-Record	JSRC, PTSP	Statistics data for each policy installed for this subscriber. Includes Juniper-Policy-Name.	Grouped
2054	Juniper-Acct-Collect	JSRC, PTSP	Specifies whether to collect accounting data for the installed policy (service) when included in the Juniper-Policy-Install AVP: <ul style="list-style-type: none"> 1—COLLECT_ACCT 2—NOT_COLLECT_ACCT 	Enumerated
2058	Juniper-State-ID	JSRC, PTSP	Specifies the value assigned to each synchronization cycle for the purpose of identifying which messages to discard. All solicited requests containing the same Juniper-State-ID belong to the same Session-Resource-Query (SRQ) synchronization cycle. Messages from a previous synchronization cycle are discarded. When a new cycle begins, the value of the Juniper-State-ID AVP is increased by 1. NOTE: For solicited synchronization requests, the SRQ message contains the incremented Juniper-State-ID value. For unsolicited synchronization requests, the Session-Resource-Reply (SRR) message contains the incremented Juniper-State-ID value.	Unsigned32
2100	Juniper-Virtual-Router	Gx-Plus, JSRC	Specifies the name of the virtual router associated with the session.	UTF8String

Table 48: Juniper Networks Diameter AVPs (*continued*)

Attribute Number	Diameter AVP	Application	Description	Type
2101	Juniper-Provisioning-Source	Gx-Plus	Specifies the provisioning source for the session in CCR-N and JSDA messages: <ul style="list-style-type: none"> 1—Local 2—Remote 	Enumerated
2102	Juniper-Provisioning-Descriptor	Gx-Plus	Defines the group used in JSDA messages that includes the session ID, and optionally Juniper-Provisioning-Source and subscriber data.	Grouped
2103	Juniper-Event-Type	Gx-Plus	Communicates the event type in JSER messages: <ul style="list-style-type: none"> 1—Cold boot; all sessions are lost 2—Warm boot; sessions are preserved 3—Discovery requested by the operator 4—<i>Are you there?</i> (AYT); application level ping sent when the notification is due to no response or an erroneous response from the PCRF, or due to a configuration change. 5—AWD; application-level watchdog sent by the router when there has been no other activity for 15 seconds. The watchdog is sent every 5 seconds unless preempted by higher-priority synchronization event. 	Enumerated
2104	Juniper-Discovery-Descriptor	Gx-Plus	Defines the group used in JSDR and JSDA messages that includes parameters of a discovery request: discovery type, request string, verbosity, max results.	Grouped
2105	Juniper-Discovery-Type	Gx-Plus	Specifies the discovery subcommand for JSDR and JSDA messages: <ul style="list-style-type: none"> 1—Exact: look up the data for the specified session. 2—Bulk: Provide get-bulk kinds of information after the specified string. 3—Done: Stop retries for all sessions up to the specified session. 	Enumerated

Table 48: Juniper Networks Diameter AVPs (*continued*)

Attribute Number	Diameter AVP	Application	Description	Type
2106	Juniper-Verbosity-Level	Gx-Plus	Specifies the verbosity level for JSDR and JSDA messages: <ul style="list-style-type: none"> 1—Summary; include only the Session-Id AVP. 2—Brief; include the Session-Id, Juniper-Virtual-Router, and Framed-IP-Address AVPs. 3—Detail; include the Session-Id, Juniper-Provisioning-Source, Juniper-Virtual-Router, Framed-IP-Address, and Event-Timestamp AVPs. 4—Extensive; include all available session information. 	Enumerated
2107	Juniper-String-A	Gx-Plus	Specifies a generic string that is interpreted according to the context.	UTF8String
2108	Juniper-String-B	Gx-Plus	Specifies a generic string that is interpreted according to the context.	UTF8String
2109	Juniper-String-C	Gx-Plus	Specifies a generic string that is interpreted according to the context.	UTF8String
2110	Juniper-Unsigned32-A	Gx-Plus	Specifies a generic, unsigned 32-bit integer that is interpreted according to the context.	Unsigned32
2111	Juniper-Unsigned32-B	Gx-Plus	Specifies a generic, unsigned 32-bit integer that is interpreted according to the context.	Unsigned32
2112	Juniper-Unsigned32-C	Gx-Plus	Specifies a generic, unsigned 32-bit integer that is interpreted according to the context.	Unsigned32

Tekelec AVPs are used only for Gx-Plus. These AVPs have an enterprise number of 21274. [Table 49 on page 433](#) lists the Tekelec AVPs. These four variables are used to provide substitution values for user-defined CoS service variables.

Table 49: Tekelec Diameter AVPs

Attribute Number	Diameter AVP	Application	Description	Type
5555	Tekelec-Charging-Rule-Argument-Name	Gx-Plus	Defines the name of the service variable to be replaced.	OctetString
5556	Tekelec-Charging-Rule-Argument-Value	Gx-Plus	Defines the value of the service variable to be replaced.	OctetString

Table 49: Tekelec Diameter AVPs (*continued*)

Attribute Number	Diameter AVP	Application	Description	Type
5557	Tekelec-Charging-Rule-Argument	Gx-Plus	Defines the substitution attributes used to replace service variables. Includes Tekelec-Charging-Rule-Argument-Name AVP (5555) and Tekelec-Charging-Rule-Argument-Value AVP (5556).	Grouped
5558	Tekelec-Charging-Rule-With-Arguments	Gx-Plus	Requests the installation of the rule (activation of the service) designated by the included Charging-Rule-Name AVP (1005). Requested service variable substitutions are provided by the optionally included Tekelec-Charging-Rule-Argument AVP (5557).	Grouped

Related Documentation

- [Understanding JSRC-SAE Interactions on page 453](#)
- [Understanding PTSP-SAE Interactions on page 481](#)
- [Understanding Gx-Plus Interactions Between the Router and the PCRF on page 441](#)
- [Diameter Base Protocol Overview on page 419](#)
- [Juniper Networks Session and Resource Control \(SRC\) and JSRC Overview on page 451](#)
- [Juniper Networks Session and Resource Control \(SRC\) and PTSP Overview on page 480](#)
- [Gx-Plus for Provisioning Subscribers Overview on page 439](#)

Configuring Diameter

You configure Diameter by specifying the endpoint origin, the remote peers, the transport layer connection, and network elements that associate routes with peers. Only the master Diameter instance is currently supported. You can configure alternative values for the master instance only in the context of the master routing instance

To configure Diameter base protocol:

1. Configure the origin realm and origin host of the Diameter master instance.
See [“Configuring the Origin Attributes of the Diameter Instance” on page 435](#)
2. Configure the Diameter peers.
See [“Configuring Diameter Peers” on page 435](#)
3. (Optional) Configure the Diameter transport layer elements.
See [“Configuring the Diameter Transport” on page 436](#)
4. (Optional) Configure the Diameter network elements.

See [“Configuring Diameter Network Elements” on page 437](#)

5. (Optional) Configure trace options for troubleshooting the configuration.

See [“Tracing Diameter Base Protocol Processes for Subscriber Access” on page 543](#).

Related Documentation

- [Diameter Base Protocol Overview on page 419](#)

Configuring the Origin Attributes of the Diameter Instance

You can configure the identifying characteristics of the endpoint node that originates Diameter messages for the Diameter instance. The hostname is supplied as the value for the Origin-Host AVP by the Diameter instance. The realm is supplied as the value for the Origin-Realm AVP by the Diameter instance.

To configure the origin attributes for a Diameter instance:

1. Specify the name of the host that originates the Diameter message.

```
[edit diameter origin]
user@host# set host host14
```

2. Specify the realm of the host that originates the Diameter message.

```
[edit diameter origin]
user@host# set realm example.com
```

Related Documentation

- [Configuring Diameter on page 434](#)
- [origin on page 832](#)

Configuring Diameter Peers

You can configure the peers to which Diameter sends messages. By default, logical system *default* and routing instance *master* are used. Port 3868 is used for active connections to peers by default.

To configure a remote peer for a Diameter instance:

1. Specify the name of the Diameter peer.

```
[edit diameter]
user@host# set peer p3
```

2. Specify the address of the Diameter peer.

```
[edit diameter peer p3]
user@host# set address 192.168.23.10
```

3. (Optional) Specify a routing instance, a logical system, or a logical system and routing instance for the Diameter peer.

```
[edit diameter peer p3]
user@host# set routing-instance ri8
```

```
[edit diameter peer p3]
user@host# set logical-system ls10
```

```
[edit diameter peer p3]
user@host# set logical-system ls10 routing-instance ri8
```

4. (Optional) Specify the port that Diameter uses for active connections to the peer.

```
[edit diameter peer p3]
user@host# set connect-actively port 49152
```

5. Specify the transport that Diameter uses for active connections to the peer.

```
[edit diameter peer p3]
user@host# set connect-actively transport t6
```

Related Documentation

- [Configuring Diameter on page 434](#)

Configuring the Diameter Transport

You can configure one or more transports for a Diameter instance to set the IP address for the local connection, and optionally configure a logical system or routing instance context. By default, the logical system *default* and the routing instance *master* are used. The logical system and routing instance for the transport connection must match that for the peer, or a configuration error is reported. Multiple peers can share the same transport.

To configure a transport for a Diameter instance:

1. Configure the transport name.

```
[edit diameter]
user@host# set transport t1
```

2. Configure the local IP address for the Diameter local transport connection.

```
[edit diameter transport t1]
user@host# set address 10.9.20.0
```

3. (Optional) Configure a logical system and optionally a routing instance for the transport.

```
[edit diameter transport t1]
user@host# set logical-system ls5
```

4. (Optional) Configure a routing instance for the transport.

```
[edit diameter transport t1]
user@host# set routing-instance ri10
```

Related Documentation

- [Configuring Diameter on page 434](#)

Configuring Diameter Network Elements

A Diameter network element (DNE) consists of associated functions, a list of prioritized peers, and a set of forwarding rules. The forwarding rules define individual routes through a set of associated destinations, functions, and metrics.

Before you configure Diameter network elements, perform the following task:

- Define the Diameter peers. See [“Configuring Diameter Peers” on page 435](#).

To configure a Diameter network element:

1. Specify the name of the network element.

```
[edit diameter]
user@host# set network-element dne25
```

2. (Optional) Associate one or more functions with the network element. All functions are associated by default.

```
[edit diameter network-element dne25]
user@host# set function jsrsc
```

3. Associate a Diameter peer with the network element and set the priority for the peer.

```
[edit diameter network-element dne25]
user@host# set peer peer1 priority 1
```

4. Specify a route that is reachable through the network element based on the forwarding rules that you define.

```
[edit diameter network-element dne25]
user@host# set forwarding route dne-route2
```

5. Specify a metric for the route.

```
[edit diameter network-element dne25 forwarding route dne-route2]
user@host# set metric 15
```

6. (Optional) Associate the route with a destination host and realm.

```
[edit diameter network-element dne25 forwarding route dne-route2]
user@host# set destination host host5 realm example.com
```

7. (Optional) Specify a function (application) associated with the route.

```
[edit diameter network-element dne25 forwarding route dne-route2]
user@host# set function jsrsc
```

Related Documentation

- [Configuring Diameter on page 434](#)

Configuring Gx-Plus for Provisioning Subscribers

- [Gx-Plus for Provisioning Subscribers Overview on page 439](#)
- [Understanding Gx-Plus Interactions Between the Router and the PCRF on page 441](#)
- [Configuring Gx-Plus on page 446](#)
- [Configuring the Gx-Plus Partition on page 447](#)
- [Configuring Gx-Plus Global Attributes on page 448](#)
- [Provisioning Subscribers with Gx-Plus on page 449](#)

Gx-Plus for Provisioning Subscribers Overview

Gx-Plus is a Diameter-based application that extends the capability of the Gx interface. The 3rd Generation Partnership Project (3GPP) defined Gx as the online policy interface between the Policy Control and Charging Rules Function (PCRF) and the Policy and Charging Enforcement Function (PCEF), to provide control over policy and flow-based charges for subscribers. The PCRF is a centralized policy decision point that deploys business policy rules to allocate broadband network resources and manages flow-based charges for subscribers and services. The router functions as the PCEF in this environment.

Gx-Plus provides provisioning, activation, and deactivation of services; threshold triggers for service statistics processing; service accounting; subscriber session termination; fault recovery; and event (subscriber login and logout) notifications. The terminology typically used for PCRFs varies slightly from standard Junos OS terminology. The terms listed in [Table 50 on page 439](#) are interchangeable.

Table 50: Differences Between Gx-Plus and Junos OS Terminology

Gx-Plus	Junos OS
policy	service
rule	service
rule install or installation	service activation or instantiation
rule uninstall	service deactivation

Table 50: Differences Between Gx-Plus and Junos OS Terminology (*continued*)

Gx-Plus	Junos OS
usage monitoring	service accounting
<p>Gx-Plus enables the router acting as a PCEF to exchange Diameter Credit-Control Application (DCCA) messages with a PCRF residing on a server to request credit authorization and service provisioning for authenticated subscribers. When an application requests AAA to activate a subscriber's session, the router sends a Credit-Control-Request (CCR) message to determine whether the subscriber has credit for the desired services and to request provisioning of those services from the PCRF policy manager.</p> <p>The PCRF responds with a Credit-Control-Answer (CCA) message that indicates success or failure for credit authorization. If the subscriber has sufficient credit for the requested services, credit is authorized. If the subscriber has insufficient credit for the services, credit authorization fails.</p> <p>The CCA can include services to be activated for the subscriber. If the response times out, the subscriber is logged in but only default services—if present—are activated for the subscriber. The router interprets the omission of the Result-Code AVP from the CCA as a provisioning authorization failure and does not allow the subscriber to log in.</p> <p>When a subscriber client application, such as DHCP, sends a subscriber logout notice to AAA, the router in turn sends a CCR message to the PCRF to request subscriber termination. The PCRF acknowledges the logout with a CCA message.</p> <p>Different Diameter message types exchanged by the router and the PCRF contain different sets of attribute-value pairs (AVPs). If data for an AVP is not available for a request to the PCRF, that AVP is omitted from the message. If the PCRF subsequently has insufficient information to decide on the request, it may deny the request.</p> <p>Gx-Plus establishes sessions that correspond to IPv4 DHCP sessions on dual-stack IPv6/IPv4 or IPv4-only subscriber interfaces, depending on the access profile. By default, IPv6 information is not communicated to the PCRF. You must explicitly configure Gx-Plus to include IPv6 information. When you do so, Gx-Plus can establish sessions that correspond to DHCPv6 sessions on IPv6-enabled subscriber interfaces and on dual-stack IPv6/IPv4-enabled interfaces.</p> <p>For dual-stack DHCP subscribers (DHCPv4 and DHCPv6 on the same VLAN), each DHCP session is treated as a separate Gx-Plus session. However, only a single Gx-Plus session exists for dual-stack PPP sessions.</p> <p>Gx-Plus includes the following fault tolerance and recovery capabilities:</p> <ul style="list-style-type: none"> • Unlimited retries of unacknowledged provisioning requests • Unlimited retries of logout requests • Router event notification • Router discovery 	



NOTE: More than one Diameter-based application (function), such as Gx-Plus or JSRC, can run on a router simultaneously.

Related Documentation

- [Messages Used by Diameter Applications on page 421](#)
- [Diameter AVPs and Diameter Applications on page 426](#)
- [Understanding Gx-Plus Interactions Between the Router and the PCRF on page 441](#)
- [Configuring Gx-Plus on page 446](#)

Understanding Gx-Plus Interactions Between the Router and the PCRF

This topic describes the sequences of Diameter messages exchanged by means of Gx-Plus between the Policy Control and Rules Charging Function (PCRF) and the router acting as a Policy and Charging Enforcement Function (PCEF) as they interact to perform the following tasks for subscriber access:

- Subscriber login
- Fault tolerance and event notification
- Subscriber audit
- Subscriber logout

Subscriber Login

Gx-Plus provisioning is enabled for subscribers when you include the **provisioning-order gx-plus** statement at the **[edit access profile *profile-name*]** hierarchy level. When an application requests AAA to activate the subscriber's session, the router sends a CCR-I message to the PCRF to request provisioning for the subscriber session. The CCR-I message must include the Juniper-Virtual-Router, Framed-IP-Address, and NAS-Port-ID AVPs. The request is not generated when no IPv4 address has been assigned to the subscriber, when IPv6 is enabled and an IPv6 address has been assigned, or when the NAS-Port-ID is unknown.

The PCRF returns a CCA-I message that includes the Result-Code AVP (AVP code 268). The router considers a CCA-I that does not include the Result-Code AVP as a failed response. The CCA-I can return the Charging-Rule-Install AVP (AVP code 1001), which identifies services to be activated.

If the Result-Code value is DIAMETER_SUCCESS (2001), the router communicates to AAA that the requested service is activated. If the Result-Code value is DIAMETER_AUTHORIZATION_REJECTED, the router communicates to AAA that the service activation is not permitted. If the Result-Code AVP has any other value, or is missing, the request is retried. A total of three CCR-I messages can be sent.

If the PCRF does not indicate success or failure, then by default the router continues to send requests, but the retry requests are CCR-N messages (no-response notifications) that include the Juniper-Provisioning-Source AVP (AVP code 2101). This AVP indicates

that the router has local decision-making authority to provision services in the absence of a PCRF response to the CCR-I. This AVP is not present in the CCR-I message.

A subscriber login initiates the following sequence of events:


1. A client application—such as DHCP, PPP, or static subscriber sessions—requests AAA to authenticate the subscriber.
2. Authentication begins if the subscriber access profile specifies RADIUS authentication. Login continues when the authentication is successful. Login fails when the **authentication-order** statement in the profile does not specify RADIUS authentication or no authentication. Login fails unless the **authentication-order** statement in the profile specifies RADIUS authentication or no authentication. Login also fails when authentication fails.
3. Default services are activated for the subscriber. Any services that the authentication server includes in the authentication grant are activated. Additionally, a default service may have been configured for the client application.
4. If the subscriber access profile specifies Gx-Plus provisioning, the router initiates the Gx-Plus message exchange by sending a CCR-I message to the PCRF. The router waits for the PCRF to respond with a CCA-I message within a non-configurable timeout period.

When the PCRF responds within the timeout period and includes the Charging-Rule-Install AVP in the CCA-I message, subscriber login is delayed while the router deactivates any default services and attempts to activate the specified services.

- If all the specified services are activated, then the login completes.
- If any of the services cannot be activated, the router sends the PCRF a CCR-U message with the status of the services (a rule report). The PCRF responds to this message with a CCA-U that can contain a new set of services for activation.
- The router ignores any default services, even if the CCA-I message does not include any services. In this circumstance, no services are activated.

If the PCRF does not return a CCA-I within the timeout period, subscriber login completes.

- The router searches first for services returned from the authentication server and activates any it finds. If no such services are found, then the router activates any locally configured default services. Subscriber login completes when default service activation is successful, but fails when any default service fails to activate. Because default services are not required to be present, login also completes when no default services are found.
- If login completes (with or without a default service), the router periodically resends the CCR-I message to the PCRF. If the PCRF subsequently returns a CCA-I, the router deactivates the default service, if any, and then activates any services included in the CCA-I. If the message does not include any services, then no services are activated, not even a default service.

- If any of the services contained in the CCA-I cannot be activated, the router sends the PCRF a CCR-U message with the status of the services (a rule report). The PCRF responds to this message with a CCA-U that can contain a new set of services for activation.
5. The router begins to monitor session accounting statistics if the CCA-I message includes any threshold triggers for usage monitoring. The Usage-Monitoring-Information AVP (AVP code 1067) contains the threshold triggers in the Granted-Service-Unit AVP (AVP code 431). The triggers are the values granted by the PCRF for the following statistics: duration of the session, input octets count, output octets count, and total octets count.
 - a. If the service statistics meet or exceed any of these trigger thresholds during the session, the router sends a CCR-U message to the PCRF with accounting information in the Usage-Monitoring-Information AVP (AVP code 1067). The AVP now contains the Used-Service-Unit AVP (AVP code 446) to report the current values for all four statistics.
 - b. In response, the PCRF may return a CCA-U message with the Usage-Monitoring-Information AVP, which can include any of the following: the Granted-Service-Unit AVP with new threshold triggers (absolute values rather than increments to the previous thresholds), the Charging-Rule-Install AVP (AVP code 1001) for service activations, or the Charging-Rule-Remove AVP (AVP code 1002) for service deactivations.
-
- 

NOTE: The router does not aggregate statistics across services.
-
6. When the subscriber logs out, the router sends a CCR-T message (termination notice) to the PCRF, which responds with a CCA-T message.

Fault Tolerance and Event Notification

Although the probability is low, the PCRF and the router can have different values for the number of subscribers. This error can arise from the following scenarios:

- CCA-I loss: if no CCA-I is delivered to the router, then the PCRF considers a subscriber as provisioned whereas the router considers it not provisioned.
- CCR-T loss: if no CCR-T is delivered to the PCRF, then the PCRF considers a subscriber to be provisioned whereas the router considers the subscriber not provisioned (logged out).

Loss of messages can be greater during cold boots and high availability events. Unacknowledged CCR-I and CCR-T requests are retransmitted forever until a satisfactory response is received to reduce the incidence of failure, and significant events are reported to Gx-Plus. By default, the number of outstanding requests is limited to 40 to avoid overloading the PCRF. This limit reduces the possibility of losing requests. You can modify this number by including the **max-outstanding-requests** statement at the **[edit access-gx-plus global]** hierarchy level.

Gx-Plus does not rely on the connection state between devices to detect router or PCRF outages, because some events do not affect the connection state and others are not detected when there is a Diameter relay or proxy between the devices. Event notifications (JSER messages) are sent when certain events take place on the router. The Juniper-Event-Type AVP (AVP code 2103) in the message describes the event.

Event notifications are retried until Gx-Plus returns a JSEA message with a Result-Code value of DIAMETER_SUCCESS (2001) to acknowledge receipt of the event notification. When retrying notifications, one notification is sent for each outstanding event. No other request are sent as long as there is any outstanding event other than an application watch dog (AWD).

Table 51 on page 444 lists router events and the subsequent router and PCRF actions.

Table 51: Router Events, Router Actions, and PCRF Actions

Router Event	Router Action	PCRF Action
The router receives no response from the PCRF or an error response.	Send event notification.	Respond to event notification.
The configuration changes. Significant changes such as the origin host or realm and the Gx-Plus partition destination host or realm also increment the value of the Origin-State-Id AVP.	Send event notification.	Respond to event notification and perform discovery.
The router receives an explicit discovery request from the PCRF.	Send event notification.	Respond to event notification.
The router undergoes a cold boot and all sessions are lost. This can result from a catastrophic failure or power cycle.	Send event notification.	Respond to event notification and clear the database.
The router undergoes a warm boot.	Send event notification.	Respond to event notification and clear the database.
Recovery resources that are needed to continuously retry unacknowledged requests (CCR-N and CCR-T messages) are exhausted. The value of the Origin-State-Id AVP is incremented. This event is unlikely to occur.	Send event notification.	Respond to event notification and perform discovery.

An important aspect of Gx-Plus fault tolerance is that subscriber login and termination requests are retried (replayed) forever until a satisfactory response is received from the PCRF. In rare circumstances, this can result in a stack of pending requests being replayed over and over.

You can issue the **clear network-access gx-plus replay** command to clear all pending requests. This command causes Gx-Plus to send a JSER message to PCRF that includes the Juniper-Event-Type AVP (AVP code 2103) with a value of 3 indicating a discovery request. The PCRF then returns a JDER message to initiate discovery of all subscribers. When this discovery completes, all pending subscriber requests are cleared.

PCRF-Generated Discovery

The PCRF runs a discovery process in response to data loss, exhaustion of router resources, operator request, or router request. The JS DR message specifies the level of verbosity desired in the reply from Gx-Plus. The message also specifies whether the request is for data about a particular session or information similar to an SNMP Get-Bulk for all sessions. Gx-Plus returns a JS DA message that indicates complete success, limited success, or an error. In the event of success, the requested data is also returned.

Subscriber Accounting

When the PCRF returns a CCA-I message to the router, the message may contain thresholds for any of several usage statistics for a subscriber service: Duration, input data, output data, or total data for the service session. Upon receipt of a threshold, the router begins monitoring the subscriber's service session activity for that statistic. When the usage statistic reaches the threshold, it triggers the router to send a Gx-Plus usage notification message (CCR-U) to the PCRF. In response, the PCRF may send a CCA-U message to specify a new threshold, activate new services, or deactivate current services.

The PCRF can also send a CCR-U message that explicitly requests usage monitoring for statistics at different levels. The router can monitor usage at the subscriber level or at the service level. The Granted-Service-Unit AVP in the message specifies one or more of the following the statistics:

- CC-Input-Octets
- CC-Output-Octets
- CC-Total-Octets
- CC-Time

If any other statistics are specified, the router sends the PCRF a CCA message indicating that incorrect statistics were requested. When the specified threshold for a monitored statistic is reached, the router sends a CCR-U that contains the usage report for the statistics. In response, the PCRF sends another CCA-R with new thresholds or a request to activate or deactivate services.

Subscriber Audit

The PCRF can send a reauthorization request (RAR message) to Gx-Plus at any time to determine whether a particular subscriber is still logged in. You can also manually trigger the PCRF to do so by issuing the **clear network-access aaa gx-plus replay** command.

The Session-Id AVP identifies the subscriber session. Gx-Plus returns an RAA message to provide status on the subscriber session. When the session is still up (found in the session database) the Result-Code AVP value in the RAA message is DIAMETER_SUCCESS (2001). When the session is not found, the Result-Code value is DIAMETER_UNKNOWN_SESSION_ID (5002). A Result-Code value of DIAMETER_UNABLE_TO_DELIVER (3002) indicates that Gx-Plus is not configured.

Subscriber Logout

When the client application sends a subscriber logout notice to AAA, Gx-Plus sends a CCR-T message to notify the PCRF that the provisioned subscriber session is being terminated. The PCRF returns a CCA-T message that includes the Result-Code AVP. If the Result-Code value is DIAMETER_SUCCESS, Gx-Plus notifies AAA, and AAA notifies the application that the logout is complete. If Gx-Plus does not receive a CCA-T message, or if the Result-Code AVP has any other value or is missing, then the termination request is retried until the CCA-T message is returned with DIAMETER_SUCCESS.

Related Documentation

- [Gx-Plus for Provisioning Subscribers Overview on page 439](#)
- [Messages Used by Diameter Applications on page 421](#)
- [Diameter AVPs and Diameter Applications on page 426](#)
- [Configuring Gx-Plus on page 446](#)
- [Default Subscriber Service Overview on page 199](#)
- [Configuring a Default Subscriber Service on page 200](#)

Configuring Gx-Plus

You can configure the Gx-Plus client application to work with a PCRF policy manager residing on a server. The PCRF is a centralized policy decision point that deploys business rules to allocate broadband network resources and manage subscribers and services. AAA on the router (acting as the PCEF) uses Gx-Plus to request service provisioning from the PCRF.



NOTE: Contact the Juniper Networks Technical Assistance Center (JTAC) for information on supported PCRFs.

To configure Gx-Plus:

1. Configure the Gx-Plus partition.
See [“Configuring the Gx-Plus Partition” on page 447](#).
2. Configure Gx-Plus global attributes: the number of outstanding requests permitted and the inclusion of IPv6 subscribers.
See [“Configuring Gx-Plus Global Attributes” on page 448](#).
3. Configure Gx-Plus provisioning for subscribers.
See [“Provisioning Subscribers with Gx-Plus” on page 449](#).
4. (Optional) Override PCRF control of a subscriber session to correct services or troubleshoot a problem.

See “Disabling PCRF Control of a Subscriber Session” on page 581.

5. (Optional) Configure Gx-Plus event tracing as part of general authentication service tracing operations.

See “Tracing General Authentication Service Processes” on page 559.

Related Documentation

- [Gx-Plus for Provisioning Subscribers Overview on page 439](#)

Configuring the Gx-Plus Partition

Gx-Plus works within a specific logical system: routing instance context, called a partition.



NOTE: Currently, only a single partition is supported; you must configure it within the default logical system: routing instance context.

Before you configure the Gx-Plus partition, perform the following task:

- Configure the Diameter instance at the **[edit diameter]** hierarchy level. See “Configuring Diameter” on page 434.

Configuration for the Gx-Plus partition consists of naming the partition and then associating a Diameter instance, the PCRF hostname, and the PCRF realm with the partition.

To configure the Gx-Plus partition:

1. Create the partition or specify the name of an existing partition.

```
[edit access gx-plus]
user@host# set partition partition-name
```

2. Specify the Diameter instance for the Gx-Plus partition.



NOTE: Currently, only the default Diameter instance, *master*, is supported.

```
[edit access gx-plus partition partition-name]
user@host# set diameter-instance instance-name
```

3. (Optional) Configure the destination host for the Gx-Plus partition.

```
[edit access gx-plus partition partition-name]
user@host# set destination-host hostname
```

4. Configure the destination realm for the Gx-Plus partition.

```
[edit access gx-plus partition partition-name]
user@host# set destination-realm realm
```

The following example shows a Gx-Plus partition configuration.

```
gx-plus {
```

```
partition partition1 {  
    diameter-instance master;  
    destination-host pcrf1;  
    destination-realm generic.example.com;  
}  
}
```

- Related Documentation**
- [Configuring Gx-Plus on page 446](#)
 - [Gx-Plus for Provisioning Subscribers Overview on page 439](#)

Configuring Gx-Plus Global Attributes

You can configure attributes that apply to all Gx-Plus partitions globally.

When a request from Gx-Plus to the PCRF is not answered or is improperly answered, Gx-Plus keeps retrying the request until it receives an appropriate answer. If the number of requests grows too large, the PCRF can become overloaded and messages can be lost. To reduce this risk, you can set a limit on the number of outstanding requests to the PCRF that Gx-Plus can retry.

By default, Gx-Plus does not include IPv6 subscribers in Gx-Plus provisioning requests to the PCRF. Instead, Gx-Plus only establishes sessions that correspond to IPv4 DHCP sessions on dual-stack IPv6/IPv4 or IPv4-only subscriber interfaces. You must explicitly configure Gx-Plus to include IPv6 information. When you do so, Gx-Plus can establish sessions that correspond to DHCPv6 sessions on IPv6-enabled subscriber interfaces and on dual-stack IPv6/IPv4-enabled interfaces.

To configure Gx-Plus global attributes:

1. (Optional) Set a limit on the number of outstanding requests.

```
[edit access gx-plus global]  
user@host# set max-outstanding-requests number
```

2. (Optional) Include IPv6 subscribers in provisioning requests.

```
[edit access gx-plus global]  
user@host# set include-ipv6
```

For example to limit the number of outstanding requests to 30 and to include IPv6 subscribers:

```
[edit access gx-plus global]  
user@host# set max-outstanding-requests 30  
user@host# set include-ipv6
```

- Related Documentation**
- [Configuring Gx-Plus on page 446](#)
 - [Gx-Plus for Provisioning Subscribers Overview on page 439](#)

Provisioning Subscribers with Gx-Plus

You can configure AAA to use Gx-Plus to request provisioning from a PCRF to instantiate services for an authenticated subscriber.

Before you configure Gx-Plus provisioning for subscribers, perform the following task:

- Create the subscriber access profile at the **[edit access profile]** hierarchy level. See [“Configuring an Access Profile for Subscriber Management” on page 107](#).

To configure Gx-Plus provisioning:

- Specify **gx-plus** as the provisioning method in the profile.

```
[edit access profile profile-name]  
user@host# set provisioning-order gx-plus
```

Related Documentation

- [Configuring Gx-Plus on page 446](#)
- [Gx-Plus for Provisioning Subscribers Overview on page 439](#)

CHAPTER 48

Configuring JSRC in Subscriber Access Networks

- [Juniper Networks Session and Resource Control \(SRC\) and JSRC Overview on page 451](#)
- [Understanding JSRC-SAE Interactions on page 453](#)
- [Configuring JSRC on page 455](#)
- [Configuring the JSRC Partition on page 456](#)
- [Assigning a Partition to JSRC on page 457](#)
- [Authorizing Subscribers with JSRC on page 457](#)
- [Provisioning Subscribers with JSRC on page 458](#)

Juniper Networks Session and Resource Control (SRC) and JSRC Overview

The Juniper Networks Session and Resource Control (SRC) environment provides a central administrative point for managing subscribers and their services. The SRC software runs on Juniper Networks C Series Controllers. The SRC software uses the Diameter protocol for communications between the local SRC peer on a Juniper Networks routing platform and the remote SRC peer on a C Series Controller. The local SRC peer is known as JSRC and is part of the AAA application. The remote SRC peer is the service activation engine (SAE); the SAE acts as the controlling agent in the SRC environment. JSRC and the SAE jointly provide the remote control enforcement functionality (RCEF).

JSRC has the following responsibilities:

- Request address authorization from the SAE.
- Request service activations from the SAE.
- Activate and deactivate services as specified by the SAE. JSRC can activate multiple policies with the same service (dynamic profile) name.
- Optionally report volume statistics for service accounting.
- Log out subscribers as specified by the SAE.
- Update the SAE with status of new service activations and deactivations.
- Synchronize subscriber state and service information with the SAE.
- Notify the SAE when subscribers log out.

The SRC software enables the SAE to activate and deactivate subscriber services (described by SRC policies) and log out subscribers. The SAE can control only those resources that have been provisioned through SAE. Therefore, the SAE receives information about only those subscribers for whom JSRC has requested provisioning from the SAE. For example, when a subscriber logs in, but the configuration did not require the session activation path to include SAE provisioning, the SAE does not receive information about this subscriber and cannot control the subscriber session.

Similarly, the SAE can control only the subscriber services that it has activated. When a service is not activated from the SAE—a RADIUS-activated service, for example—the SAE receives no information about the service and has no control over it.

The SAE can also direct JSRC to collect accounting statistics per service session.



NOTE: More than one Diameter-based application (function) can run on a router simultaneously.

Hardware Requirements for JSRC for Subscriber Access

JSRC is supported on Juniper Networks MX Series 3D Universal Edge Routers. JSRC currently supports subscriber sessions on static and dynamic interfaces.

Related Documentation

- [Understanding JSRC-SAE Interactions on page 453](#)
- [Messages Used by Diameter Applications on page 421](#)
- [Diameter AVPs and Diameter Applications on page 426](#)
- [Configuring JSRC on page 455](#)

Understanding JSRC-SAE Interactions

This topic describes the sequences of Diameter messages exchanged between JSRC (the local SRC peer) and the SAE (the remote SRC peer) as they interact to perform the following tasks for subscriber access:

- Subscriber login
- Service activation
- Service deactivation
- Resynchronization
- SAE-initiated subscriber logout
- Statistics collection and reporting
- Subscriber-initiated logout

Subscriber Login

JSRC authorization is enabled for DHCP subscribers when you include the **authorization-order jsrc** statement at the **[edit access profile *profile-name*]** hierarchy level. This setting causes AAA to ignore the authentication order setting in the access profile. As a result, AAA does not authenticate the DHCP subscribers. For non-DHCP subscribers, AAA ignores the **authorization-order** statement.

When a DHCP subscriber attempts to log in, DHCP sends an authentication request to AAA. In turn, JSRC sends a Diameter AA-Request message to the SAE. SAE returns a Diameter AA-Answer message that can include the Framed-IP-Address attribute and the Juniper-DHCP-Options AVP (AVP code 2010). JSRC ignores any other optional AVPs included in this AA-Answer message.

JSRC provisioning is enabled for DHCP (and SSC) subscribers when you include the **provisioning-order** statement at the **[edit access profile *profile-name*]** hierarchy level. When the application requests AAA to activate the subscriber's session, JSRC sends an AA-Request message that includes the Juniper-Request-Type AVP (AVP code 2050) with a value that indicates service provisioning is requested from the SAE.

The SAE returns a AA-Answer message that contains an ACK if the request is accepted or a NAK if the request is denied. If the request is accepted, the AA-Answer message includes the Juniper-Policy-Install AVP (AVP code 2020), which is used to specify the service to attach to the subscriber's interface. When this AVP is included, the SAE sets the Result-Code AVP to 1001 (DIAMETER_MULTI_ROUND_AUTH). This code means that the JSRC must send another AA-Request message to the SAE to report the success or failure of the policy instantiation (service activation) by AAA. JSRC ignores any other optional AVPs included in this AA-Answer message. The SAE returns an AA-Answer message to acknowledge this second AA-Request message.

Subscriber Service Activation and Deactivation

SAE policies provision subscriber services. After a subscriber is logged in, the SAE can send a PPR message to JSRC to activate or deactivate services. A given PPR can include the Juniper-Policy-Install AVP (AVP code 2020) to activate a service, the Juniper-Policy-Remove AVP (AVP code 2027) to deactivate a service, or both (for different services). A PPR can include no more than three of these AVPs (install, remove, or mixed).

JSRC sends a PPA message to the SAE when it has completed the tasks requested in the PPR. The PPA indicates the success or failure of the actions requested in the PPR.



NOTE: If you use RADIUS or the CLI to deactivate a service that the SAE, the SAE becomes unsynchronized with the state of subscribers on the routing engine.

Subscriber Resynchronization

During resynchronization, JSRC informs the SAE about the services that are active for the provisioned subscribers. Either JSRC or the SAE initiates the resynchronization.

- The SAE initiates resynchronization at startup or when a backup SAE takes over session control due to resource limits or conditions on the primary SAE. The SAE clears its database of all entries in preparation for the synchronization.
- JSRC initiates resynchronization at JSRC startup, such as when AAA starts or restarts.

JSRC can also initiate resynchronization in another circumstance. When an SAE in a multi-SAE environment becomes active, it must send an SRQ to JSRC as its first message. JSRC then locks the Origin-Host AVP of the active SAE. JSRC subsequently triggers resynchronization if it receives a message from any other SAE as indicated by the Origin-Host AVP. Such an incident can occur if communication between the active SAE and a standby SAE is interrupted.

Both entities initiate a resynchronization by sending an SRQ message. The recipient responds with an SRR message. After the SRR is sent, regardless of whether the SAE or JSRC initiates the synchronization, JSRC sends an AA-Request message to the SAE for each provisioned subscriber present in the session database. The AA-Request message includes a Juniper-Policy-Install AVP for the active services. The SAE returns an AA-Answer message with an ACK to acknowledge receipt.

Subscriber Session Terminated by the SAE

When the SAE terminates a subscriber session, it sends an ASR message to JSRC. JSRC causes AAA to send a logout request to the DHCP (or SSC) client application. When the DHCP client application accepts the logout request, JSRC includes an ACK in the ASR message it sends to the SAE to signify success. If the DHCP client application does not accept the request, then JSRC includes a NAK in the ASR to signify failure. The DHCP client application is responsible for initiating the actual logout sequence with AAA.

Statistics Collection and Reporting per Service Rule

Statistics information can be sent from the router to the SAE or from the SAE to the router. Both the Diameter Accounting-Request (ACR) and Accounting-Answer (ACA) messages include the Juniper-Acct-Record AVP (AVP code 2053), which identifies the policy (service) for which accounting information is requested.

Subscriber Logout

When the DHCP (or SSC) client application sends a subscriber logout notice to AAA, JSRC sends an STR message to notify the SAE that the provisioned subscriber session is being terminated. The SAE returns an STA message to JSRC, and JSRC notifies DHCP that the logout is complete.

Related Documentation

- [Juniper Networks Session and Resource Control \(SRC\) and JSRC Overview on page 451](#)
- [Messages Used by Diameter Applications on page 421](#)
- [Diameter AVPs and Diameter Applications on page 426](#)
- [Configuring JSRC on page 455](#)

Configuring JSRC

You can configure the JSRC client application to work with Session and Resource Control (SRC) to centrally manage subscribers and services. JSRC requests address and service authorizations from the remote SRC peer (the SAE), activates and deactivates services as specified by the SAE, logs out subscribers as specified by the SAE, and synchronizes subscriber state and service information with the SAE.

To configure JSRC:

1. Configure the JSRC partition.
[See “Configuring the JSRC Partition” on page 456.](#)
2. Assign the JSRC partition.
[See “Assigning a Partition to JSRC” on page 457.](#)
3. Configure JSRC authorization for subscribers.
[See “Authorizing Subscribers with JSRC” on page 457.](#)
4. Configure JSRC provisioning for subscribers.
[See “Provisioning Subscribers with JSRC” on page 458.](#)
5. Configure service accounting by JSRC.
[See “Configuring Service Accounting with JSRC” on page 460.](#)
6. Configure JSRC event tracing as part of general authentication service tracing operations.
[See “Tracing General Authentication Service Processes” on page 559.](#)

- Related Documentation**
- [Juniper Networks Session and Resource Control \(SRC\) and JSRC Overview on page 451](#)

Configuring the JSRC Partition

JSRC works within a specific logical system: routing instance context, called a partition.



NOTE: Currently, only a single partition is supported; you must configure it within the default logical system: routing instance context.

Before you configure the JSRC partition, perform the following task:

- Configure the Diameter instance at the **[edit diameter]** hierarchy level. See [“Configuring Diameter” on page 434](#).

Configuration for the JSRC partition consists of naming the partition and then associating a Diameter instance, the SAE hostname, and the SAE realm with the partition.

To configure the JSRC partition:

1. Create the partition.

```
[edit jsrc]
user@host# set partition partition1
```

2. Specify the Diameter instance for the JSRC partition.



NOTE: Currently, only the default Diameter instance, *master*, is supported.

```
[edit jsrc partition partition1]
user@host# set diameter-instance master
```

3. Configure the destination host for the JSRC partition.

```
[edit jsrc partition partition1]
user@host# set destination-host sae1
```

4. Configure the destination realm for the JSRC partition.

```
[edit jsrc partition partition1]
user@host# set destination-realm generic.example.com
```

- Related Documentation**
- [Configuring JSRC on page 455](#)

Assigning a Partition to JSRC

You must associate a configured JSRC partition with the JSRC instance that you are configuring.

Before you assign a partition to JSRC, perform the following task:

- Configure the JSRC partition. See [“Configuring the JSRC Partition” on page 456](#)

To assign the JSRC partition:

- Specify the partition name.

```
[edit jsrc]
user@host# set jsrc-partition partition1
```

Related Documentation

- [Configuring JSRC on page 455](#)

Authorizing Subscribers with JSRC

You can configure AAA to use JSRC in an SRC environment to request authorization from the SAE when AAA is verifying whether a DHCP subscriber can access the router. When JSRC authorization is configured, AAA ignores any configured authentication order settings.

Before you configure JSRC authorization, perform the following tasks:

- Create the subscriber access profile at the **[edit access profile]** hierarchy level.
- Define the subscriber username with the **username-include** statement in the authentication configuration for DHCP local server or DHCP relay.

To configure JSRC authorization:

- Specify **jsrc** as the authorization method in the profile.

```
[edit access profile dhcpsub1]
user@host# set authorization-order jsrc
```

Related Documentation

- [Configuring JSRC on page 455](#)
- [Creating Unique Usernames for DHCP Clients on page 218](#)
- [profile on page 858](#)

Provisioning Subscribers with JSRC

You can configure AAA to use JSRC in an SRC environment to request provisioning from the SAE to instantiate services for an authenticated subscriber.

Before you configure JSRC provisioning for subscribers, perform the following task:

- Create the subscriber access profile at the **[edit access profile]** hierarchy level.

To configure JSRC provisioning:

- Specify **jsrc** as the provisioning method in the profile.

```
[edit access profile dhcpsub1]  
user@host# set provisioning-order jsrc
```

Related Documentation

- [Configuring JSRC on page 455](#)

Configuring Service Accounting with JSRC

- [Service Accounting with JSRC on page 459](#)
- [Configuring Service Accounting with JSRC on page 460](#)

Service Accounting with JSRC

A service session represents a service for a specific subscriber. Service sessions exist in the context of a subscriber session. JSRC activates and deactivates services as specified by the SAE (remote SRC peer). JSRC can collect and report service accounting data by volume. JSRC accounting requires that either classic firewall filters or fast update firewall filters be configured to count service packets—the service packet information provides the volume statistics.



NOTE: JSRC supports only volume statistics accounting for service sessions. Time statistics and subscriber accounting are not supported.

JSRC service accounting supports both accounting based on service activation/deactivation and interim accounting.

- **Service activation/deactivation accounting**—When accounting is enabled, JSRC sends an accounting start message to the SAE when it activates a service and an accounting stop message when it deactivates the service. The start message initiates the accounting session and provides initial information about the service session. The stop message terminates the accounting session and reports the final (cumulative) accounting data.
- **Interim accounting**—When interim accounting is enabled for a service session, JSRC sends interim accounting messages to the SAE at a specified interval to report the cumulative accounting information available at that time. Interim accounting is ignored when accounting is not enabled for the corresponding service session.

JSRC accounting for a service begins when the service is activated, and remains in effect while the service is active. The SAE specifies the service (policy) to be activated for the subscriber with the Juniper-Policy-Install AVP (AVP code 2020). When this AVP includes the Juniper-Acct-Collect AVP (AVP code 2054), JSRC initiates service activation/deactivation accounting for the service.

JSRC initiates interim accounting when the Juniper-Policy-Install AVP includes the Acct-Interim-Interval AVP (AVP code 85). In this case, JSRC updates the accounting values at the interval specified in the AVP— in the range 600 through 86,400 seconds. Aggregate counters are reported for the dual stack case.

JSRC and the SAE exchange Diameter Accounting-Request (ACR) and Accounting-Answer (ACA) messages to communicate accounting data. Both messages include the Juniper-Acct-Record AVP (AVP code 2053) to identify the service for which accounting information is requested.

JSRC sends ACR messages to report accounting data to the SAE. The ACR message includes the Accounting-Record-Type AVP (AVP code 480) to specify the kind of accounting record that it is sending. When a service is activated, this AVP has a value of START_RECORD. When a service is deactivated, it has a value of STOP_RECORD. For interim accounting, ACR messages are sent at the specified accounting interval and the AVP has a value of INTERIM_RECORD.

In addition to specifying the accounting record type, the ACR messages include standard RADIUS attributes to specify the desired statistics: Acct-Input-Octets [42], Acct-Output-Octets [43], Acct-Input-Packets [47], Acct-Output-Packets [48], and Acct-Session-Time [46].

The SAE returns ACA messages to the JSRC to acknowledge receipt of the ACR messages.

An access profile specifies subscriber access authentication and accounting parameters. When a service is activated through JSRC, the accounting reports can be sent either to the SAE or to RADIUS. The default configuration sends the reports to the SAE; you can also configure this by including the **service accounting-order activation-protocol** statement in the access profile. To send the reports instead to the RADIUS server, include the **service accounting-order radius** statement in the access profile.

When a service is activated through RADIUS rather than through JSRC, the accounting reports of the service session are sent to the RADIUS server.

**Related
Documentation**

- [Configuring Service Packet Counting on page 95](#)
- [Messages Used by Diameter Applications on page 421](#)
- [Diameter AVPs and Diameter Applications on page 426](#)

Configuring Service Accounting with JSRC

You can configure JSRC to report accounting statistics for service sessions.

In addition to the configuration shown here, the network context for JSRC service accounting includes the configuration of firewall filters to count the statistics, Diameter, JSRC, the subscriber services, RADIUS, and the SRC.

To configure service accounting by JSRC:

1. Configure JSRC to provision subscriber services.


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

2. Configure service accounting to be provided by the application that provisions the service—JSRC.

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

**Related
Documentation**

- [Service Accounting with JSRC on page 459](#)

Configuring Subscribers on Static Interfaces

- [Subscribers on Static Interfaces Overview on page 463](#)
- [Configuring Subscribers over Static Interfaces on page 466](#)
- [Example: Configuring Static Subscribers for Subscriber Access on page 467](#)

Subscribers on Static Interfaces Overview

You can associate subscribers with statically configured interfaces and provide dynamic service activation and activation for these subscribers. When the static interface comes up, the event is treated as a subscriber login. When the interface goes down, it is treated as a subscriber logout. After the subscribers are present in the session database (SDB), JSRC can report the subscribers to the SAE so that the SRC software can subsequently manage the subscribers.

Alternatively, you can configure the static subscribers to be authenticated and authorized by means of RADIUS. In this case, RADIUS can then activate and deactivate services with change of authorization (CoA) messages. However, this configuration does not prevent the interface from coming up and forwarding traffic. Further, authorization parameters are not imposed on the subscriber interface.

Currently, only Ethernet interfaces support static subscribers. Only one static subscriber can exist over a given interface. An interface cannot appear in more than one group. Static subscribers cannot be created over dynamic interfaces.

Static subscribers are intended to work with JSRC. Include the **provisioning-order jsrc** statement at the **[edit access profile *profile-name*]** hierarchy level to enable JSRC to handle the subscribers at the direction of the SRC software.

If the authentication request fails for a static subscriber, a 60-minute, nonconfigurable timer begins counting down. The request is reissued when the timer expires. This action repeats for as long as the interface is operationally up.

You can force a logout of the static subscriber by issuing the **request services static-subscribers logout interface *interface-name*** command. A static subscriber can also be logged out by AAA or an external policy manager. In both cases, no subsequent logins can take place on the underlying interface until you reset the state by issuing the **request**

services static-subscribers login interface *interface-name* command or the router or process reboots.

You can log out an interface group by issuing the **request services static-subscriber logout group *group-name*** command. You can subsequently log in a group of interfaces by issuing the **request services static-subscriber login group *group-name*** command.

No new CLI statements are required to configure the dynamic profile for static subscribers. The dynamic profile can be very simple; it is activated at login and deactivated at logout. If you do not configure a profile, then the *junos-default-profile* is automatically activated.

During a graceful Routing Engine switchover (GRES) event, active static subscribers are recovered, inactive subscribers are cleaned up, and logout continues for subscribers that were in the process of logging out.

Include the **static-subscribers** statement at the **[edit system services]** hierarchy level to configure static subscribers. Include the **traceoptions** statement at the **[edit system processes static-subscribers]** hierarchy level to configure tracing operations for static subscribers.

You can configure the access profile, dynamic profile, and authentication parameters for all static subscribers or for a particular group of static subscribers:

- To configure the access profile that triggers AAA services for the static subscriber for all static subscribers, include the **access-profile** statement at the **[edit system services static-subscribers]** hierarchy level. Alternatively, include this statement at the **[edit system services static-subscribers group *group-name*]** hierarchy level to apply the profile to a specific group and override a top-level configuration.
- To configure the dynamic profile that is instantiated when the static subscriber logs in for all static subscribers, include the **dynamic-profile** statement at the **[edit system services static-subscribers]** hierarchy level. Alternatively, include this statement at the **[edit system services static-subscribers group *group-name*]** hierarchy level to apply the profile to a specific group and override a top-level configuration. Do not specify a dynamic profile that creates a dynamic interface.
- To configure the authentication parameters that trigger an Access-Request message to AAA for all static subscribers, include the **authentication** statement at the **[edit system services static-subscribers]** hierarchy level. Alternatively, include the statement at the **[edit system services static-subscribers group *group-name*]** hierarchy level to configure authentication for a specific group and override a top-level configuration. If you do not configure authentication, then by default the interface name is modified and used as the default username for the subscriber session and the authentication request.

The configurable authentication parameters include the password and details of how the username is formed. Include the **password** statement at the **[edit system services static-subscribers authentication]** hierarchy level to configure the authentication password for all static subscribers. Alternatively, include the statement at the **[edit system services static-subscribers group *group-name* authentication]** hierarchy level to configure authentication for a specific group and override a top-level configuration.

The username that is sent to AAA for authentication must include at least one of the following attributes:

- Domain name
- User prefix
- Interface name
- Logical system name
- Routing instance name

To configure how the username is formed for all static subscribers, include the desired statements at the **[edit system services static-subscribers authentication]** hierarchy level: **domain-name**, **user-prefix**, **logical-system-name**, or **routing-instance-name**. Alternatively, include the desired statements at the **[edit system services static-subscribers group group-name authentication]** hierarchy level to configure the username for a specific group and override a top-level configuration.

If you change the authentication configuration for an existing group or for static subscribers globally, the change has no effect on existing static subscribers. The changes are applied only to any new logins that are attempted after you commit the changes.

A group configuration must specify all the interfaces that you expect to support static subscribers. Include the **interface** statement at the **[edit system services static-subscribers group group-name]** hierarchy level to specify the interfaces. This statement enables you to specify a single interface or a range of interfaces.

You must also statically configure these interfaces before any static subscribers can be supported on them. You must configure the static interfaces in the same logical system and routing instance as the group that includes the interfaces.

If you change the interfaces that are included in an existing interface group, existing static subscribers are automatically logged out and then back in when you commit the changes. However, changes made to the configuration of the interface itself have no effect on the login or logout state of the static subscriber associated with that interface.

By default, multiple subscribers are not supported on top of the same VLAN logical interface. If you want to support this behavior, then you can manage multiple subscribers on a single logical interface in one of two ways. You can either merge attributes such as firewall filters and CoS attributes for the multiple subscribers, or you can replace the current attributes with those of a new subscriber whenever a new subscriber logs into the underlying VLAN logical interface.

- To enable attribute merging for all static interfaces, include the **aggregate-clients merge** statement at the **[edit system services static-subscribers]** hierarchy level. Alternatively, include this statement at the **[edit system services static-subscribers group group-name]** hierarchy level to enable attribute merging for a specific group of static interfaces and override a top-level configuration.
- To enable attribute replacement for all static interfaces, include the **aggregate-clients replace** statement at the **[edit system services static-subscribers]** hierarchy level.

Alternatively, include this statement at the **[edit system services static-subscribers group group-name]** hierarchy level to enable attribute replacement for a specific group of static interfaces and override a top-level configuration.

- Related Documentation**
- [Configuring Subscribers over Static Interfaces on page 466](#)
 - [Juniper Networks Session and Resource Control \(SRC\) and JSRC Overview on page 451](#)
 - [Understanding JSRC-SAE Interactions on page 453](#)

Configuring Subscribers over Static Interfaces

This topic describes the procedure for configuring subscribers over static interfaces (static subscribers).

Before you configure subscribers over static interfaces, perform the following tasks:

- Configure the static interfaces on which you want to create and manage subscribers.
- Create an access profile to trigger AAA services for static subscribers.
- Create a dynamic profile that is instantiated when static subscribers log in.

To configure static subscribers:

1. Specify the global access profile that triggers AAA services for static subscribers.
See [“Specifying the Static Subscriber Global Access Profile” on page 471](#).
2. Specify the global dynamic profile that is instantiated when static subscribers log in.
See [“Specifying the Static Subscriber Global Dynamic Profile” on page 471](#).
3. Configure global method to handle multiple subscribers on a VLAN Logical Interface.
See [“Enabling Multiple Subscribers on a VLAN Logical Interface for All Static Subscribers” on page 472](#)
4. Configure the global authentication password for static subscribers.
See [“Configuring the Static Subscriber Global Authentication Password” on page 473](#).
5. Configure the global username for static subscribers.
See [“Configuring the Static Subscriber Global Username” on page 473](#).
6. Configure a group of subscribers to share values different from the global configuration.
See [“Creating a Static Subscriber Group” on page 475](#).
7. Specify the access profile for the static subscriber group.
See [“Specifying the Static Subscriber Group Access Profile” on page 476](#).
8. Specify the dynamic profile for the static subscriber group.
See [“Specifying the Static Subscriber Group Dynamic Profile” on page 476](#).

9. Configure method to handle multiple subscribers on a VLAN Logical Interface for a static subscriber group.
See [“Enabling Multiple Subscribers on a VLAN Logical Interface for a Static Subscriber Group”](#) on page 477.
10. Configure the authentication password for the static subscriber group.
See [“Configuring the Static Subscriber Group Authentication Password”](#) on page 477.
11. Configure the username for the static subscriber group.
See [“Configuring the Static Subscriber Group Username”](#) on page 478.
12. (Optional) Force a static subscriber to be logged out from an interface.
See [“Forcing a Static Subscriber to Be Logged Out”](#) on page 505.
13. (Optional) Enable an interface to accept static subscriber logins.
See [“Resetting the State of an Interface for Static Subscriber Login”](#) on page 505.
14. (Optional) Force static subscribers to be logged out from a group of interfaces.
See [“Forcing a Group of Static Subscribers to Be Logged Out”](#) on page 506.
15. (Optional) Enable a group of interfaces to accept static subscriber logins.
See [“Resetting the State of an Interface Group for Static Subscriber Login”](#) on page 506.
16. Configure trace options for troubleshooting the configuration.
See [“Tracing Static Subscriber Operations”](#) on page 571.

**Related
Documentation**

- [Subscribers on Static Interfaces Overview](#) on page 463
- [\[edit system services static-subscribers\] Hierarchy Level](#) on page 621

Example: Configuring Static Subscribers for Subscriber Access

This example shows a static subscriber configuration.

1. Configure the access profile to be used for static subscribers.

```
access {
  profile access5 {
    provisioning-order jsr;
    accounting {
      order radius;
    }
    authentication {
      order radius;
    }
  }
}
```

2. Configure the dynamic profile to be used for static subscribers.

If you do not configure this profile, the default profile, junos-default-profile, is used.

3. Configure the static interfaces on which to layer the static subscribers.
4. Configure the parameters that apply globally to all static subscribers in the configuration context.

```
static-subscribers {  
  access-profile access5;  
  dynamic-profile dyn-profile-1;  
  authentication {  
    password Gj85*3mS;  
    username-include {  
      user-prefix Building5;  
      interface;  
      logical-system-name;  
      routing-instance-name;  
      domain-name example.com;  
    }  
  }  
}
```

5. If you want to override the global parameters for certain static subscribers, create a group of static interfaces for those subscribers and configure parameters to apply to that group. Repeat this step for as many groups as you need.

```
static-subscribers {  
  group boston {  
    interface ge-1/0/1.1 upto ge-1/0/1.102  
    interface ge-1/0/1.6 exclude  
    interface ge-1/0/1.70 upto ge-1/0/1.80 exclude  
    access-profile boston-acs;  
    dynamic-profile dyn-profile-2;  
    authentication {  
      password knTS$ $k2;  
      username-include {  
        user-prefix 2ndFloor;  
        interface;  
        logical-system-name;  
        routing-instance-name;  
        domain-name example.net;  
      }  
    }  
  }  
}
```

6. Configure tracing options for static subscriber events.

```
static-subscribers {  
  traceoptions {  
    file filename <files number> <match regular-expression> <size maximum-file-size>  
      <world-readable | no-world-readable>;  
    flag flag;  
    level (all | error | info | notice | verbose | warning);  
    no-remote-trace;  
  }  
}
```


- Related Documentation**
- [Subscribers on Static Interfaces Overview on page 463](#)
 - [Configuring Subscribers over Static Interfaces on page 466](#)

Configuring the Static Subscribers Global Profile

- [Specifying the Static Subscriber Global Access Profile on page 471](#)
- [Specifying the Static Subscriber Global Dynamic Profile on page 471](#)
- [Enabling Multiple Subscribers on a VLAN Logical Interface for All Static Subscribers on page 472](#)
- [Configuring the Static Subscriber Global Authentication Password on page 473](#)
- [Configuring the Static Subscriber Global Username on page 473](#)

Specifying the Static Subscriber Global Access Profile

You specify a previously created access profile that triggers AAA services for all static subscribers. This value can be overridden for a group of static subscribers when a different profile is configured for that group.

To specify the access profile used for all static subscribers:

- Specify the profile name.

```
[edit system services static-subscribers]
user@host# set access-profile access5
```

Related Documentation

- [Configuring Subscribers over Static Interfaces on page 466](#)
- [Specifying the Static Subscriber Group Access Profile on page 476](#)
- [profile on page 858](#)

Specifying the Static Subscriber Global Dynamic Profile

You specify a previously created dynamic profile that is instantiated when a static subscriber logs in. This profile is used for all static subscribers. This value can be overridden for a group of static subscribers when a different profile is configured for that group.

To specify the dynamic profile used for all static subscribers:

- Specify the profile name.

```
[edit system services static-subscribers]
user@host# set dynamic-profile dyn-profile-1
```

**Related
Documentation**

- [Configuring Subscribers over Static Interfaces on page 466](#)
- [Specifying the Static Subscriber Group Dynamic Profile on page 476](#)
- *dynamic-profiles*

Enabling Multiple Subscribers on a VLAN Logical Interface for All Static Subscribers

For a given interface, only a single static subscriber (or group) is logged in. Although we do not recommend this practice, you might have other kinds of subscribers configured on the same interface, such as a DHCP subscriber managed by the DHCP application. You can use the **aggregate-clients** statement to extend the dynamic profile for all static subscribers to enable multiple subscribers to share the same VLAN logical interface.

You can specify that attributes (such as CoS or firewall) for the multiple subscribers are merged for the logical interface. That is, the profiles for multiple subscribers of different types are instantiated on the interface, but the profile attributes of each are merged together. Alternatively, you can specify that the instantiated profile for the current subscriber is replaced by the profile of a new subscriber that logs in using the same logical interface. This configuration can be overridden for a group of static subscribers when a different configuration is applied for that group.

To enable multiple subscribers to share the same VLAN logical interface for all static subscribers, do one of the following:

- Specify that the multiple subscriber attributes are merged for the logical interface.

```
[edit system services static-subscribers dynamic-profile dyn-profile-1]
user@host# set aggregate-clients merge
```

- Specify that the entire logical interface is replaced when a new subscriber logs into the network using the same VLAN logical interface.

```
[edit system services static-subscribers dynamic-profile dyn-profile-3]
user@host# set aggregate-clients replace
```

**Related
Documentation**

- [Configuring Subscribers over Static Interfaces on page 466](#)
- [Specifying the Static Subscriber Group Dynamic Profile on page 476](#)
- [dynamic-profile on page 720](#)

Configuring the Static Subscriber Global Authentication Password

You configure a password that is included in the Access-Request message sent to AAA to authenticate all static subscribers. This value can be overridden for a group of static subscribers when a different password is configured for that group.

To specify the authentication password used for all static subscribers:

- Specify the password.

```
[edit system services static-subscribers authentication]
user@host# set password Gj85*3mS
```

Related Documentation

- [Configuring Subscribers over Static Interfaces on page 466](#)
- [Configuring the Static Subscriber Group Authentication Password on page 477](#)
- [authentication on page 652](#)

Configuring the Static Subscriber Global Username

You configure how the username is formed. The username serves as the username for all static subscribers that are created and is included in the Access-Request message sent to AAA to authenticate all static subscribers. This value can be overridden for a group of static subscribers when a different username is configured for that group.

The username must include at least one of the five possible elements. The value of each element is concatenated in a specific order; the resulting string is the username. If you specify their inclusion, the interface name, logical system name, and routing instance name are derived from the configuration context. The elements are ordered as follows:

user-prefix.interface.logical-system-name.routing-instance-name@domain-name

To configure the username for all static subscribers:

- (Optional) Specify a prefix for the username.

```
[edit system services static-subscribers authentication username-include]
user@host# set user-prefix Building5
```

- (Optional) Specify that the interface name is included in the username.

```
[edit system services static-subscribers authentication username-include]
user@host# set interface
```

- (Optional) Specify that the logical system name is included in the username.

```
[edit system services static-subscribers authentication username-include]
user@host# set logical-system-name
```

- Specify that the routing instance name is included in the username.

```
[edit system services static-subscribers authentication username-include]
user@host# set routing-instance-name
```

5. Specify the domain name included in the username.

```
[edit system services static-subscribers authentication username-include]  
user@host# set domain-name campus.example.com
```

Configured in the default logical system and master routing instance for interface ge-0/1/1.100, this sample configuration generates the following username:

Building5.ge-0-1-1-100.default.master.campus.example.com

**Related
Documentation**

- [Configuring Subscribers over Static Interfaces on page 466](#)
- [Configuring the Static Subscriber Group Username on page 478](#)
- [username-include on page 987](#)

Configuring the Static Subscribers Group Profile

- [Creating a Static Subscriber Group on page 475](#)
- [Specifying the Static Subscriber Group Access Profile on page 476](#)
- [Specifying the Static Subscriber Group Dynamic Profile on page 476](#)
- [Enabling Multiple Subscribers on a VLAN Logical Interface for a Static Subscriber Group on page 477](#)
- [Configuring the Static Subscriber Group Authentication Password on page 477](#)
- [Configuring the Static Subscriber Group Username on page 478](#)

Creating a Static Subscriber Group

You can override the configuration that is applied globally to static subscribers by creating a static subscriber group that consists of a set of statically configured interfaces. You can then apply a common configuration for the group with values different from the global values for access and dynamic profiles, password, and username.

To configure an interface group for static subscribers:

1. Access the **[edit system services static-subscribers]** hierarchy level.
2. Create the group and assign the name.

```
[edit system services static-subscribers]  
user@host# edit group boston
```

3. Specify the names of one or more interfaces on which static subscribers can be created. You can repeat the **interface interface-name** statement to specify multiple interfaces within the group, but you cannot use the same interface in more than one group.

```
[edit system services static-subscribers group boston]  
user@host# set interface ge-1/0/1.1  
user@host# set interface ge-1/0/1.2
```

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

```
[edit system services static-subscribers group boston]  
user@host# set interface ge-1/0/1.3 upto ge-1/0/1.9
```

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

```
[edit system services static-subscribers group boston]
user@host# set interface ge-1/0/1.1 upto ge-1/0/1.102
user@host# set interface ge-1/0/1.6 exclude
user@host# set interface ge-1/0/1.70 upto ge-1/0/1.80 exclude
```

**Related
Documentation**

- [Configuring Subscribers over Static Interfaces on page 466](#)
- [Specifying the Static Subscriber Group Access Profile on page 476](#)
- [Specifying the Static Subscriber Group Dynamic Profile on page 476](#)
- [Configuring the Static Subscriber Group Authentication Password on page 477](#)
- [Configuring the Static Subscriber Group Username on page 478](#)

Specifying the Static Subscriber Group Access Profile

You can override the configured global access profile by specifying a different profile for a group of static subscribers. The access profile triggers AAA services for that group of static subscribers.

To specify the access profile used for a group of static subscribers:

- Specify the profile name.

```
[edit system services static-subscribers group boston]
user@host# set access-profile boston-acs
```

**Related
Documentation**

- [Configuring Subscribers over Static Interfaces on page 466](#)
- [profile on page 858](#)

Specifying the Static Subscriber Group Dynamic Profile

You can override the configured global dynamic profile by specifying a different profile for a group of static subscribers. The dynamic profile is instantiated when any static subscriber in the group logs in.

To specify the dynamic profile used for a group of static subscribers:

- Specify the profile name.

```
[edit system services static-subscribers group boston]
user@host# set dynamic-profile dyn-profile-2
```

**Related
Documentation**

- [Configuring Subscribers over Static Interfaces on page 466](#)
- [Specifying the Static Subscriber Global Dynamic Profile on page 471](#)
- [dynamic-profiles](#)

Enabling Multiple Subscribers on a VLAN Logical Interface for a Static Subscriber Group

For a given interface, only a single static subscriber group (or static subscriber) is logged in. Although we do not recommend this practice, you might have other kinds of subscribers configured on the same interface, such as a DHCP subscriber managed by the DHCP application. You can use the **aggregate-clients** statement to extend the dynamic profile for a static subscriber group to enable multiple subscribers to share the same VLAN logical interface.

You can specify that attributes (such as CoS or firewall) for the multiple subscribers are merged for the logical interface. That is, the profiles for multiple subscribers of different types are instantiated on the interface, but the profile attributes of each are merged together. Alternatively, you can specify that the instantiated profile for the current subscriber group is replaced by the profile of a new subscriber that logs in using the same logical interface. This configuration overrides the configuration applied to all static subscribers that are not members of the group.

To enable multiple subscribers to share the same VLAN logical interface for a static subscriber group, do one of the following:

- Specify that the multiple subscriber attributes are merged for the logical interface.

```
[edit system services static-subscribers group boston dynamic-profile dyn-profile-2]
user@host# set aggregate-clients merge
```

- Specify that the entire logical interface is replaced when a new subscriber logs into the network using the same VLAN logical interface.

```
[edit system services static-subscribers group boston dynamic-profile dyn-profile-4]
user@host# set aggregate-clients replace
```

Related Documentation

- [Configuring Subscribers over Static Interfaces on page 466](#)
- [Specifying the Static Subscriber Group Dynamic Profile on page 476](#)
- [dynamic-profile on page 720](#)

Configuring the Static Subscriber Group Authentication Password

You can override the configured global authentication password by specifying a different password for a group of static subscribers. This password is included in the Access-Request message sent to AAA to authenticate all static subscribers in the group.

To specify the authentication password used for a group of static subscribers:

- Specify the password.

```
[edit system services static-subscribers group boston authentication]
user@host# set password knTS$Sk2
```

Related Documentation

- [Configuring Subscribers over Static Interfaces on page 466](#)

- [Configuring the Static Subscriber Global Authentication Password on page 473](#)
- [authentication on page 652](#)

Configuring the Static Subscriber Group Username

You can override the configured global username by specifying a different username for a group of static subscribers. The username serves as the username for a group of static subscribers that is created and is included in the Access-Request message sent to AAA to authenticate that group.

The username must include at least one of the five possible elements. The value of each element is concatenated in a specific order; the resulting string is the username. If you specify their inclusion, the interface name, logical system name, and routing instance name are derived from the configuration context. The elements are ordered as follows:

user-prefix.interface.logical-system-name.routing-instance-name@domain-name

To configure the username for a group of static subscribers:

1. (Optional) Specify a prefix for the username.

```
[edit system services static-subscribers group boston authentication username-include]
user@host# set user-prefix 2ndFloor
```

2. (Optional) Specify that the interface name is included in the username.

```
[edit system services static-subscribers group boston authentication username-include]
user@host# set interface
```

3. (Optional) Specify that the logical system name is included in the username.

```
[edit system services static-subscribers group boston authentication username-include]
user@host# set logical-system-name
```

4. Specify that the routing instance name is included in the username.

```
[edit system services static-subscribers group boston authentication username-include]
user@host# set routing-instance-name
```

5. Specify the domain name included in the username.

```
[edit system services static-subscribers group boston authentication username-include]
user@host# set domain-name building5.example.com
```

Configured in the default logical system and master routing instance for interface ge-0/1/2.50, this sample configuration generates the following username:

2ndfloor.ge-0-1-2-50.default.master.building5.example.com

Related Documentation

- [Configuring Subscribers over Static Interfaces on page 466](#)
- [Configuring the Static Subscriber Global Username on page 473](#)
- [username-include on page 987](#)

Configuring the PTSP Feature to Support Dynamic Subscribers

- [PTSP Overview on page 479](#)
- [Juniper Networks Session and Resource Control \(SRC\) and PTSP Overview on page 480](#)
- [Understanding PTSP-SAE Interactions on page 481](#)
- [Packet-Triggered Subscribers Services Overview on page 482](#)
- [Configuring the PTSP Application on page 486](#)
- [Configuring PTSP on page 486](#)

PTSP Overview

The packet-triggered subscribers and policy control (PTSP) feature allows the application of policies to individual source IP addresses flowing through a given interface. A subscriber context is created for each distinct source IP address seen in a given underlying interface. This feature can be used to support dynamic subscribers that are controlled by a subscriber termination device, such as a B-RAS or GGSN device, that is connected to an MX Series 3D Universal Edge Router.

PTSP has the following responsibilities:

- Create a subscriber context for each distinct IPv4 address on a given interface (subscriber context).
- Apply policies to or remove policies from the subscriber context.
- Collect statistics and report for each individual policy for each subscriber context.
- Derive information about subscribers.

You can associate specific subscriber contexts based on IPv4 addresses and provide service activation and deactivation for these subscribers. The Multiservices DPC (MS-DPC) maintains a table of addresses for each subscriber and any corresponding policies. If an address is not found in the subscriber table, then a new subscriber context is created. All policies are defined on a per-subscriber basis. Once the subscribers are present in the subscriber table, PTSP enforces the policies active for the subscriber context. PTSP can report the subscribers to the SAE using the Diameter protocol so that the SRC software can manage the subscribers and services with dynamic policies. You can also configure

static policies, but dynamic policies take precedence over static policies. When you download a new dynamic policy, it takes effect only for new flows. All new flows and TCP connections use the new dynamic policy. Existing flows are not affected by the new policy unless they timeout, after which they are considered a new flow.

Statistics collection that is aggregated on a service rule basis is also shared with the SAE using the Diameter application. These statistics are not written to a flat file. Statistics collection that is aggregated on an application or application group basis is written to a flat file. These statistics are not shared with the SAE using the Diameter protocol.

Hardware Requirements for PTSP for Subscriber Access

PTSP is supported on Juniper Networks MX Series 3D Universal Edge Routers. You must have a Multiservices DPC (MS-DPC) on the MX Series router.

Related Documentation

- [Configuring PTSP on page 486](#)

Juniper Networks Session and Resource Control (SRC) and PTSP Overview

The Juniper Networks Session and Resource Control (SRC) environment provides a central administrative point for managing subscribers and their services. The SRC software runs on Juniper Networks C Series Controllers. The SRC software uses the Diameter protocol for communications between the local peer on a Juniper Networks routing platform and the remote SRC peer on a C Series Controller. The local peer is known as PTSP and is part of the AAA application. The remote SRC peer is the service activation engine (SAE); the SAE acts as the controlling agent in the SRC environment.

The SRC software enables the SAE to activate and deactivate subscriber services (described by SRC policies). The SAE installs or removes policies using a service rule policy template called `__svc_rule__`. This policy template indicates which policy is applied to a new subscriber session. Additional policies are bound to new sessions; they do not affect existing sessions. Note that policy name must be unique between PPR requests. You can use the same rule name within a single request, but you cannot use the same name again in a separate request.

Statistics collection that is aggregated on a service rule basis is also shared with the SAE using the Diameter protocol.



NOTE: More than one Diameter-based application (function) can run on a router simultaneously.



NOTE: When the SRC software downloads PTSP policies, it matches all the application groups defined in the rule of the PTSP policy if the **application-group-any** keyword is used in the policy. The **application-group-any** keyword is not configured on the router although the application group name is defined in the application identification configuration database on the router to process application-aware access list (AACL) rules for accepting or discarding packets. The keyword is considered as an exception because the application group is defined in the application identification database.

Related Documentation

- [Messages Used by Diameter Applications on page 421](#)
- [Diameter AVPs and Diameter Applications on page 426](#)
- [Understanding PTSP-SAE Interactions on page 481](#)
- [Configuring the PTSP Application on page 486](#)
- [Configuring PTSP on page 486](#)

Understanding PTSP-SAE Interactions

This topic describes the sequences of Diameter messages exchanged between PTSP and the SAE as they interact to perform the following tasks for subscriber access:

- Subscriber login

When a packet-triggered subscriber logs in, PTSP sends a Diameter AA-Request message to request service provisioning from the SAE that includes the Session-Id attribute for the new subscriber. If the AA-Request fails, then the subscriber is not considered logged in and the subscriber session is not managed by the SAE. Only the static PTSP rules apply to the subscriber.

The SAE returns a Diameter AA-Answer message with the Result-Code. The AA-Answer message can include the Juniper-Policy-Install AVP (AVP code 2020), which is used to specify a service to attach to the subscriber's IP address.

PTSP can send an AA-Request message to the SAE to confirm activation. The SAE returns a AA-Answer message in acknowledgment. If the AA-Request message fails or the SAE does not respond with an AA-Answer message, the subscriber session is managed by the SAE.

- Service activation and deactivation

The SAE policies provision subscriber services. After a packet-triggered subscriber is logged in, the SAE can send a PPR message to PTSP to activate or deactivate services. A given PPR can include the Juniper-Policy-Install AVP (AVP code 2020) to activate a service or the Juniper-Policy-Remove AVP (AVP code 2027) to deactivate a service.

PTSP sends a PPA message to the SAE when it has completed the tasks requested in the PPR. The PPA indicates the success or failure of the actions requested in the PPR.

- Resynchronization

Either PTSP or the SAE initiates the resynchronization.

The SAE initiates resynchronization at startup or when a backup SAE takes over session control due to resource limits or conditions on the primary SAE. The SAE clears its database of all entries in preparation for the synchronization.

PTSP initiates resynchronization at startup, such as when AAA starts or restarts. PTSP uses the Juniper-Last-Origin-Host AVP (AVP code 2055) to keep track of the active SAE host in a multi-SAE environment. When an SAE in a multi-SAE environment becomes active, it must send an SRQ to PTSP as its first message. PTSP initiates a synchronization when it receives any other message type from an SAE that is different from the SAE indicated in the Juniper-Last-Origin-Host AVP.

Both entities initiate a resynchronization by sending an SRQ message. The recipient responds with an SRR message.

- Statistics collection and reporting per service rule

Statistics information can be sent from the router to the SAE or from the SAE to the router. Both the Diameter Accounting-Request and Accounting-Answer messages include the Juniper-Acct-Record AVP (AVP code 2053) which identifies the policy for which accounting information is requested.

- Subscriber logout

PTSP can determine when there is a logout request for a packet-triggered subscriber in two ways:

- The SAE terminates a subscriber session by sending an ASR message to PTSP.
- PTSP monitors a subscriber session and starts the logout process after 30 minutes of inactivity.

The subscriber logout triggers the final statistics aggregation for all policies and the removal of any policies installed by the SAE. PTSP sends an STR message that indicates the logout event to the SAE.

**Related
Documentation**

- [Juniper Networks Session and Resource Control \(SRC\) and PTSP Overview on page 480](#)
- [Messages Used by Diameter Applications on page 421](#)
- [Diameter AVPs and Diameter Applications on page 426](#)
- [Configuring the PTSP Application on page 486](#)
- [Configuring PTSP on page 486](#)

Packet-Triggered Subscribers Services Overview

The packet-triggered subscribers and policy control (PTSP) feature allows the application of policies to dynamic subscribers that are controlled by a subscriber termination device. You can associate specific subscriber contexts based on IPv4 addresses and provide dynamic service activation and deactivation for these subscribers. Once the subscribers

are present in the subscriber database on the router, PSTP can report the subscribers to the SAE using the PTSP application so that the SRC software can manage the subscribers and services.

PTSP policies can be downloaded dynamically from the external policy manager (such as SRC) or configured statically on the router. The PTSP policies can be configured for each distinct IPv4 source address for a given interface on which the service is configured. Each distinct IPv4 address is considered a subscriber and all PTSP policies are applied on a per-subscriber basis. Dynamic policies, which are always specific to a subscriber, take precedence over static policies.

You can set up PTSP policies to:

- Manage traffic by configuring filtering, rate-limiting, and QoS enforcement in the rules.
- Steer traffic by specifying the forwarding instance in the forward rule.
- Collect accounting information by service rule or by application.

When you configure PTSP policies, you must specify the type of statistics collection (**count**) and the IP address used to identify the packet-triggered subscriber (**demux**) in the service rule. All service rules attached to a given service set must have the same settings for these options.

For the statistics collection type, terms and rules also cannot mix and match the following styles:

- rule—Statistics are aggregated in one bucket for the service rule and Diameter is used to report the statistics.
- application—Statistics are aggregated by application for a specific application, for a specific application group, or in one bucket. The statistics are reported in a flat file.

Subscriber instantiation is triggered for ingress packets by the IP address. When source address is specified, the source IP address of the ingress packets is used to establish the subscriber context. When destination address is specified, the destination IP address of the ingress packets is used to establish the subscriber context. If the IP address does not correspond to a known subscriber, then a new subscriber context is created to log in the packet-triggered subscriber.

The match conditions include local address, local port, remote address, and remote port. The following table describes how the **demux** value changes the IP address or port used for these terms.

Match Conditions	demux source-address		demux destination-address	
	Ingress Flows	Egress Flows	Ingress Flows	Egress Flows
local-address	Source address	Destination address	Destination address	Source address
remote-address	Destination address	Source address	Source address	Destination address
local-port	Source port	Destination port	Destination port	Source port

Match Conditions	demux source-address		demux destination-address	
	Ingress Flows	Egress Flows	Ingress Flows	Egress Flows
remote-port	Destination port	Source port	Source port	Destination port

Subscriber Identification Method for PTSP Partition

The PSTP functionality uses RADIUS attributes, such as *User-Name* to identify subscribers in a RADIUS partition. If a service provider uses a different RADIUS attribute other than *User-Name*, the authentication of subscribers and establishment of client sessions fail. To enable service providers to use a subscriber-identification method that suits their network needs, you can add flexible configurations in the packet-triggered subscriber process.

The PTSP configurable user-identification feature allows you to do the following:

- Configure the subscriber identification method for PTSP partitions, based on the network topology and the service provider requirements.
- Insert subscriber-specific tags for the subscriber's HTTP traffic for which the reference to subscriber-specific tagging is provided using subscriber identification.

The PTSP application generates the subscriber-identification parameter as a text-string by combining the RADIUS attribute value and the internal attribute value of the PTSP partition. The text-string is generated in the same order as the attributes that are configured in the PTSP partition.



NOTE: Only RADIUS partitions support user-identification to configure the subscriber-identification method for PTSP partitions.

PTSP Services on Aggregated and Redundant Services PICs

The packet-triggered subscribers and policy control (PTSP) feature supports both Aggregated Multiservices (AMS) and Redundant Multiservices (RMS) PICs. RMS services interfaces support 1:1 redundancy between two logical PICs and in an active or standby model. AMS services interfaces support load sharing and N:1 redundancy between N logical PICs.



NOTE: The PTSP services do not support load balancing on AMS.

In 1:1 redundancy, if services PIC fails:

- The subscriber is logged out, the traffic is switched to the redundant services PIC, and the subscriber receives a new session ID to log in with.
- The subscriber's last configured accounting data is retrieved as the latest interim accounting record.

In AMS, the PTSP subscriber's traffic is redistributed to other services PIC and the same subscriber may appear on different services PICs. The subscriber with no new data flow is logged out after idle timeout with the complete accounting data. The following example depicts the AMS scenario:

```
ams0 {
  load-balancing-options {
    member-interface mams-4/0/0;
    member-interface mams-4/1/0;
    member-interface mams-5/0/0;
    member-failure-options {
      redistribute-all-traffic;
    }
  }
  unit 1 {
    family inet;
  }
}
```

The traffic on ms-4/0/0 is redistributed to ms-4/1/0 only after ms-5/0/0 has failed. In this example, there are two subscribers: s1 on ms-4/0/0 and s2 on ms-4/1/0. The two subscribers have the same source IP address. If there is no new traffic, s1 is eventually logged out after idle timeout.



NOTE: PTSP does not support any type of hash key for traffic sharing among logical PICs configured with the same PTSP service set. For PTSP to work, all traffic for any given subscriber needs to reach the same logical PIC within an AMS container. For this to happen, the AMS hashing algorithm needs to align with the PTSP demux type, as follows:

- If PTSP is configured for source-demux, then the AMS hashing algorithm must be based on the source-ip-address only.
- If PTSP is configured for destination-demux, then the AMS hashing algorithm must be based on the destination-ip-address only.
- No other type of AMS hashing algorithm is compatible with PTSP.



NOTE: The packet level idle timeout for every packet is assigned from a given subscriber transiting the router. If the timeout limit sets in, the subscriber is logged out. The valid range for the subscriber packet idle timeout is 15 to 1440 minutes.

Related Documentation

- [Configuring PTSP on page 486](#)
- [Configuring Static PTSP Rules on page 495](#)

Configuring the PTSP Application

You can configure the PTSP client application to work with the Session and Resource Control (SRC) peer to centrally manage packet-triggered subscribers and services. PTSP requests address and service authorizations from the remote SRC peer (the SAE), activates and deactivates services as specified by the SAE, logs out subscribers as specified by the SAE, and synchronizes subscriber state and service information with the SAE. The PTSP application also performs statistics collection and reporting.

To configure the PTSP application:

1. Configure the PTSP partition.
See [“Configuring the PTSP Partition” on page 491](#).
2. Assign the PTSP partition.
See [“Assigning the PTSP Partition” on page 492](#).
3. Configure statistics collection and reporting.
See [“Tracing Packet-Triggered Subscriber Operations” on page 575](#).

Related Documentation

- [Juniper Networks Session and Resource Control \(SRC\) and PTSP Overview on page 480](#)

Configuring PTSP

You can configure the packet-triggered subscribers and policy control (PTSP) feature on MX Series routers to allow the application of policies to dynamic subscribers that are controlled by a subscriber termination device, such as a B-RAS or GGSN device, connected to an MX Series router. The subscribers are associated by their IPv4 address and dynamic or static policies can be applied. Dynamic policies take precedence over static policies. When you download a new dynamic policy, it takes effect only for new flows. All new flows and TCP connections use the new dynamic policy. Existing flows are not affected by the new policy unless they timeout, after which they are considered a new flow.

To configure PTSP services on the MX Series router:

1. Configure the Multiservices DPC.
See [“Configuring the Multiservices DPC for PTSP” on page 493](#).
2. Configure the Diameter application to support the download of dynamic PTSP policies from the external policy manager (such as SRC). The PTSP application also provides statistics collection and reporting.
See [“Configuring the PTSP Application” on page 486](#).
3. Configure the static PTSP service rules.
See [“Configuring Static PTSP Rules” on page 495](#).
4. Configure statistics collection and reporting in a flat file.

See [“Configuring a Statistics Profile for PTSP” on page 577](#) and [“Tracing PTSP Operations” on page 579](#).

Related Documentation

- [PTSP Overview on page 479](#)

Configuring the PTSP Partition to Connect to the External Policy Manager

- [Understanding the Subscriber Profiles for Client Sessions per PTSP Partition on page 489](#)
- [Configuring the PTSP Partition on page 491](#)
- [Assigning the PTSP Partition on page 492](#)

Understanding the Subscriber Profiles for Client Sessions per PTSP Partition

Subscriber profiles for service activation enables you to specify which service plug-ins become activated on a per-subscriber basis. Previously, the only control mechanism for specifying service activation was to attach a service-set configuration to a selected interface or route. The new utility allows you to enable or disable services based on the subscriber associated with every data flow. As a result, you can apply differentiated services to different sets of subscribers. You can exercise the control mechanism in one of two ways: by using a CLI operational command or a RADIUS attribute.



NOTE: This feature applies only to MP-SDK services and does not depend on the specific services enabled or disabled, except that PTSP must be included in the chain.

The procedure consists of three steps:

1. Configure a service set that includes all the services to be applied to flows. You can include a default subscriber profile that controls which services are and are not active by default. The default profile applies to all subscribers until overridden for a specific subscriber. In the absence of a default subscriber profile, all services specified in the service set are applied by default. You can also include one or more alternative subscriber profiles that can be implemented to override the default profile. The following sample configuration illustrates these components:

```
services {  
  service-set ss1 {  
    application-identification-profile appidr1;  
    idp-profile idpr1;  
    aacl-rules aaclr1;  
    hcm_rules hcmr1;
```

```

sfw_rules sfwr1;
subscriber-profile {
    sp1;
}
interface-service {
    service-interface ms-3/0/0.0;
}
}
}
subscriber-profile sp1 {
    disable HCM;
    enable IDP {
        concurrent-data-sessions 10;
    }
    disable AACL;
    max-data-sessions-per-subscriber {
        limit 10;
        exceed-action [ syslog drop ];
    }
}
subscriber-profile sp2 {
    enable HCM;
    disable IDP;
    enable AACL;
    max-data-sessions-per-subscriber {
        limit 100;
        exceed-action [ syslog ];
    }
}

```

Initially, all traffic reaching the service plane under service set ss1 receives all the services configured in service set ss1 that are enabled by the default subscriber profile sp1 applied to it. In the example, APPID, stateful firewall, and IDP are enabled, whereas HCM and AACL are disabled. However IDP is enabled for only at most 10 sessions concurrently. Beyond that threshold, IDP is also disabled. Also, because of the max-data-sessions-per-subscriber setting, any subscriber is allowed a maximum of ten concurrent data sessions. Beyond that threshold, data sessions are logged and dropped.

2. There are two ways to dynamically override the default subscriber profile associated with a particular PTSP subscriber:
 - CLI operational command
 - RADIUS attribute or VSA in an access-accept message.

From the previous example, assume that the subscriber profile for subscriber X is dynamically set to sp2. After that, any new data session associated with subscriber X has a different set of services applied to it. In the example, it would be APPID, stateful firewall, HCM, and AACL. Also, because the max-data-sessions-per-subscriber setting changes to 100, subscriber X now has no upper limit on the number of concurrent data sessions, although if that number crosses the 100 threshold, the threshold-crossing event is logged.

The following examples illustrate the dynamic override settings:

Operational command

```
user@router>request services subscriber clear subscriber-profile
client-id client-id
```

```
user@router>request services subscriber set subscriber-profile
subscriber-profile-name client-id client-id
```

RADIUS configuration

```
user@router# set system services packet-triggered-subscribers
partition-radius foo subscriber-service-profile attribute-26.4874.31
```

3. Processing of a new data session at the service plane takes place as follows, with respect to subscriber profiles:
 1. A new flow starts. MP-SDK sends a SESSION-INTEREST event to the service plug-ins. The first plug-in in the chain is the subscribers (PTSP) plug-in.
 2. The subscribers plug-in matches the flow to its subscriber by searching its database. It sets the subscriber ID in the session metadata.
 3. The subscriber plug-in checks for the corresponding subscriber profile and which services are enabled. It then sets the services mask of enabled and disabled services in the session metadata.
 4. MP-SDK or JSF invokes only the services that are enabled per the services mask. The other services are skipped, even if configured in the service set.



NOTE: : Subscriber-profile changes affect only the upcoming flows. Existing flows remain unaffected.

Configuring the PTSP Partition

PTSP works within a specific logical system: routing instance context, called a partition. The partition is configured to connect to the external policy manager.



NOTE: Currently, only a single partition is supported; you must configure it within the default logical system: routing instance context.

Before you configure the PTSP partition to connect to the external policy manager, perform the following task:

- Configure the Diameter instance for the remote SRC peer at the **[edit diameter]** hierarchy level. See [“Configuring Diameter” on page 434](#).

Configuration for the PTSP partition consists of naming the partition and then associating a Diameter instance, the SAE hostname, and the SAE realm with the partition.

To configure the PTSP partition:

1. Create the partition at the `[edit system services packet-triggered-subscribers]` hierarchy level.

```
[edit system services packet-triggered-subscribers]
user@host# edit partition ptsp-default
```

2. Specify the Diameter instance for the PTSP partition.

```
[edit system services packet-triggered-subscribers partition ptsp-default]
user@host# set diameter-instance master
```

3. Configure the destination host for the PTSP partition.

```
[edit system services packet-triggered-subscribers partition ptsp-default]
user@host# set destination-host sael
```

4. Configure the destination realm for the PTSP partition.

```
[edit system services packet-triggered-subscribers partition ptsp-default]
user@host# set destination-realm generic.example.com
```

5. Configure the subscriber ID for the PTSP partition.

```
[edit system services packet-triggered-subscribers partition-radius
radius-partition-name]
user@host# set subscriber-identification
```

Related Documentation • [Configuring the PTSP Application on page 486](#)

Assigning the PTSP Partition

You must associate the PTSP partition with the logical system:routing instance.



NOTE: Currently, only the global logical system:routing instance, *master* logical system and default routing instance, is supported.

Before you assign the PTSP partition, perform the following task:

- Configure the PTSP partition. See [“Configuring the PTSP Partition” on page 491](#).

To assign the PTSP partition:

- Specify the partition name at the `[edit system]` hierarchy level.

```
[edit system]
user@host# set packet-triggered-subscribers-partition ptsp-default
```

Related Documentation • [Configuring the PTSP Application on page 486](#)

Configuring PTSP Services and Rules

- [Configuring the Multiservices DPC for PTSP on page 493](#)
- [Configuring PTSP Service Rules on page 494](#)
- [Configuring Static PTSP Rules on page 495](#)
- [Configuring PTSP Rule Sets on page 497](#)
- [Configuring PTSP Service Sets on page 497](#)
- [Configuring the PTSP Forwarding Instance on page 498](#)

Configuring the Multiservices DPC for PTSP

To configure the Multiservices Dense Port Concentrator (MS-DPC) to support PTSP services, perform the following tasks:

- [Enabling the PTSP Service Package on the Multiservices DPC on page 493](#)
- [Configuring Services Interface for PTSP on page 494](#)

Enabling the PTSP Service Package on the Multiservices DPC

The PTSP feature runs on the Multiservices DPC, you must enable the PTSP service package on the Multiservices DPC before you can configure the PTSP software. The name of the PTSP service package is **jservices-ptsp**.

To enable the PTSP service package:

1. Determine the FPC slot number and the PIC number of the MS-DPC on which you want to enable the PTSP service package.

```
user@host> show chassis hardware
```

In this example, the FPC slot number is 3 and the PIC number is 0.

2. Enable the jservices-ptsp package on the Multiservices DPC.

```
[edit chassis]
```

```
user@host# set fpc 3 pic 0 adaptive-services service-package extension-provider  
package jservices-ptsp
```

Configuring Services Interface for PTSP



NOTE: ams- interfaces and rms- interfaces can be configured for PTSP.

To configure the services interface for PTSP:

1. Enter edit mode for the interface.

```
[edit]
user@host# edit interfaces ms-3/0/0
```

2. Configure a logical unit and specify the protocol family.

```
[edit interfaces ms-3/0/0]
user@host# set unit 0 family inet
```

- Related Documentation**
- [Configuring PTSP on page 486](#)
 - [PTSP Overview on page 479](#)

Configuring PTSP Service Rules

PTSP policies can be downloaded dynamically from the external policy manager (such as SRC) or configured statically on the router. The PTSP policies can be configured for each distinct IPv4 source address for a given interface on which the service is configured. Each distinct IPv4 address is considered a subscriber and all PTSP policies are applied on a per-subscriber basis.

Dynamic policies, which are always specific to a subscriber, take precedence over static policies. When you download a new dynamic policy, it takes effect only for new flows. All new flows and TCP connections use the new dynamic policy. Existing flows are not affected by the new policy unless they timeout, after which they are considered a new flow.

To configure the PTSP policies, perform these tasks:

- To download dynamic policies and to collect statistics with Diameter, configure the Diameter application for PTSP. See [“Configuring the PTSP Application” on page 486](#).
- To configure static policies, see [“Configuring Static PTSP Rules” on page 495](#). To collect statistics in a flat file, see [“Configuring a Statistics Profile for PTSP” on page 577](#).

- Related Documentation**
- [Configuring PTSP on page 486](#)
 - [PTSP Overview on page 479](#)

Configuring Static PTSP Rules

You can configure the static PTSP policies on the router. If the PTSP service is configured on the underlying interface, the PTSP service enforces the policies associated with the subscriber context.

To configure static PTSP rules:

1. Specify the rule that you want to configure.

```
[edit services ptsp]
user@host# edit rule ptspRule1
```

2. Specify the direction in which the rule match is applied.

```
[edit services ptsp rule ptspRule1]
user@host# set match-direction input
```

3. Specify the IP address used for the subscriber context. Subscriber instantiation is always triggered for ingress packets, so this value indicates which IP address in the ingress packets for the flow is used.

```
[edit services ptsp rule ptspRule1]
user@host# set demux source-address
```

4. Specify the statistics aggregation, collection, and reporting style. Terms and rules cannot mix and match different styles.

```
[edit services ptsp rule ptspRule1]
user@host# set count-type rule
```

If you specify the rule style, statistics collection is performed by the Diameter application. If you specify the application style, statistics collection is in a flat file controlled by the local policy decision function (L-PDF).

5. (Optional) Specify the forward rule used for forwarding packets. See [“Configuring the PTSP Forwarding Instance” on page 498](#).

```
[edit services ptsp rule ptspRule1]
user@host# set forward-rule forward-rule-name
```

6. Configure the term precedence for the rule.

```
[edit services ptsp rule ptspRule1]
user@host# edit term 1
```

7. Configure the match conditions for the term. See [Table 52 on page 496](#).

```
[edit services ptsp rule ptspRule1 term 1]
user@host# set from remote-address-range low 203.0.0.2 high 203.0.0.100
user@host# set from remote-address-range low 204.0.0.2 high 204.0.0.253
```

8. (Optional) Specify the action taken when the match conditions are met. See [Table 53 on page 496](#).

```
[edit services ptsp rule ptspRule1 term 1]
user@host# set then count rule
user@host# set then accept
```

Table 52 on page 496 describes the match conditions for PTSP rules.

Table 52: PTSP Match Conditions

Match Condition	Description
application-group-any	Application group name defined in the application identification configuration.
application-groups [<i>application-group-name</i>]	Application group name defined in the application identification configuration.
applications	Application name defined in the application identification configuration.
local-port-range low <i>low-value</i> high <i>high-value</i>	Local port range.
local-ports <i>value-list</i>	Local ports.
protocol <i>protocol-number</i>	IP protocol number.
remote-address (<i>address</i> any-unicast)	Remote IP address. IPv4 only.
remote-address-range low <i>low-value</i> high <i>low-value</i>	Remote address range. IPv4 only.
remote-port-range low <i>low-value</i> high <i>high-value</i>	Remote port range.
remote-ports <i>value-list</i>	Remote ports.
remote-prefix-list <i>prefix-list-name</i>	Prefixes in the specified list.

Table 53 on page 496 describes the actions for PTSP rules.

Table 53: PTSP Actions

Action or Action Modifier	Description
accept	Accept the packet.
count	Increment the specified counter.
discard	Drop the packet.
forwarding-class	Classify the packet into the specified forwarding class.
police	Rate-limit packets based on the specified policer.

Related Documentation

- [Configuring the PTSP Forwarding Instance on page 498](#)
- [Configuring a Statistics Profile for PTSP on page 577](#)

- [Configuring PTSP on page 486](#)
- [PTSP Overview on page 479](#)
- [Packet-Triggered Subscribers Services Overview on page 482](#)

Configuring PTSP Rule Sets

You can define a collection of PTSP rules to determine the actions performed on packets.

To configure static PTSP rule sets:

1. Specify the rule set that you want to configure.

```
[edit services ptsp]
user@host# edit rule-set ptspRules
```

2. Specify the rules in the order that you want them processed.

```
[edit services ptsp rule-set ptspRules]
user@host# set rule ptspRule1
user@host# set rule ptspRule2
```

Related Documentation

- [Configuring Static PTSP Rules on page 495](#)

Configuring PTSP Service Sets

To configure the service set for the PTSP application:

1. Configure the service set that you want to contain the PTSP service.

```
[edit services service-set ptspServiceSet]
user@host# set service-set ptspServiceSet
```

2. Specify the PTSP rules that constitute the service set that is applied to the services interface.

```
[edit services service-set ptspServiceSet]
user@host# set ptsp-rules ptsp-rule1
user@host# set ptsp-rules ptsp-rule2
```

3. Configure the services interface.



NOTE: ams- interfaces and rms- interfaces are supported for PTSP.

```
[edit services service-set ptspServiceSet]
user@host# set interface-service service-interface ms-3/0/0.0
```

4. Associate the service set with the underlying interface from which the subscribers originate. The service set must be applied to the interface facing the subscriber, that is, the interface with the IP address of the subscriber.

```
[edit interfaces ge-4/0/0 unit 0 family inet service]
user@host# set input service-set ptspServiceSet
```

```
user@host# set output service-set ptspServiceSet
```

- Related Documentation**
- [Configuring Static PTSP Rules on page 495](#)
 - [Configuring PTSP Rule Sets on page 497](#)

Configuring the PTSP Forwarding Instance

Before you can forward PTSP traffic, perform these tasks for each forwarding instance:

1. Configure each PTSP forwarding instance as a routing instance type of forwarding.
2. Configure a firewall filter with an action that specifies the routing instance configured in Step 1.
3. Configure the unit number for the Multiservices interface that specifies the filter configured in Step 2 as the input filter.



NOTE: To avoid service set dependency on specific unit numbers, use the same unit number across all Multiservices interfaces where PTSP services are applied.

4. Configure the PTSP forward rule to specify the forwarding instance.



NOTE: When the forwarding instance action is performed on the flow, any postservice filters are not applied to the underlying interface.

If you want to forward traffic for PTSP subscribers, you must specify the forwarding instance for specific subscribers based on IP address, network, or prefix list. The match direction for forward rules is always input.

To configure the PTSP forwarding instance:

1. Specify the PTSP forward rule that you want to use when configuring a PTSP forwarding instance.

```
[edit services ptsp]
user@host# edit forward-rule ptspForward
```

2. Set the term precedence for the forward rule. Term with lowest precedence is evaluated first.

```
[edit services ptsp forward-rule ptspForward]
user@host# edit term 5
```

3. Configure the match conditions for the IP address, address range, or prefix list. See [Table 54 on page 499](#).

```
[edit services ptsp forward-rule ptspForward term 5]
user@host# set from local-address 200.0.0.1
```

Table 54: PTSP Forward Rule Match Conditions

Match Condition	Description
<code>application-groups</code> [<i>application-group-name</i>]	Application group name defined in the application identification configuration.
<code>applications</code>	Application name defined in the application identification configuration.
<code>local-address</code> (<i>address</i> <i>any-unicast</i>)	Local IP address. IPv4 only.
<code>local-address-range</code> <i>low low-value high high-value</i>	Local address range. IPv4 only.
<code>local-prefix-list</code> <i>prefix-list-name</i>	Prefixes in the specified list.



NOTE: You can specify match conditions for applications or application groups that support application identification (APPID) services, but we do not recommend specifying the forwarding instance action when you are using these match conditions in PTSP policies. In this situation, some network topologies may route packets in a manner that causes the flow to be dropped. For example, the APPID services might forward some packets on the default routing instance while the PTSP services forward other packets in the same flow to another routing instance.

4. Configure the forwarding instance action with the routing instance name and the unit number.

```
[edit services ptsp forward-rule ptspForward term 5]
user@host# set then forwarding-instance less-effort-ri 144
```



NOTE: When the forwarding instance action is performed on the flow, any postservice filters are not applied to the underlying interface.

- Related Documentation**
- [APPID Overview](#)
 - [Routing Instances Overview](#)

Monitoring and Managing Diameter Information for Subscriber Access

- [Verifying Diameter Node, Instance, and Route Information on page 501](#)
- [Verifying and Managing Diameter Function Information on page 502](#)
- [Verifying and Managing Diameter Peer Information on page 503](#)
- [Verifying Diameter Network Element Information on page 504](#)

Verifying Diameter Node, Instance, and Route Information

Purpose View Diameter node information:

Action • To display summary information about all Diameter nodes:

`user@host> show diameter`

- To display summary information about all Diameter nodes and add information about Diameter functions, instances, network elements, and peers:

`user@host> show diameter brief`

- To display brief information about all Diameter nodes and add information about Diameter routes:

`user@host> show diameter detail`

- To display summary information about all Diameter instances:

`user@host> show diameter instance`

- To display detailed information about all Diameter instances:

`user@host> show diameter instance detail`

- To display information about a specific Diameter instance, add the instance name to the command:

`user@host> show diameter instance master`

`user@host> show diameter instance detail master`

- To display summary information about all Diameter routes:

`user@host> show diameter route`

- To display detailed information about all Diameter routes:

```
user@host> show diameter route detail
```

- To display information about a specific Diameter route, add the route name to the command:

```
user@host> show diameter route dne-route2
```

```
user@host> show diameter route detail dne-route2
```

**Related
Documentation**

- [Configuring Diameter on page 434](#)
- [Configuring Gx-Plus on page 446](#)
- [CLI Explorer](#)

Verifying and Managing Diameter Function Information

Purpose View or clear Diameter function information:

Action

- To display summary information about all functions associated with Diameter:

```
user@host> show diameter function
```

- To display detailed information about all functions associated with Diameter:

```
user@host> show diameter function detail
```

- To display information about a specific function associated with Diameter, add the function name to the command:

```
user@host> show diameter function jsrc
```

```
user@host> show diameter function detail ptsp
```

- To display summary statistics about all functions associated with Diameter:

```
user@host> show diameter function statistics
```

- To display detailed statistics about all functions associated with Diameter:

```
user@host> show diameter function statistics detail
```

- To display statistics about a specific function associated with Diameter, add the function name to the command:

```
user@host> show diameter function statistics gx-plus
```

```
user@host> show diameter function statistics detail jsrc
```

- To delete current statistics for all functions associated with Diameter:

```
user@host> clear diameter function statistics
```

- To delete current statistics for a specific function associated with Diameter:

```
user@host> clear diameter function gx-plus statistics
```

**Related
Documentation**

- [Configuring Diameter on page 434](#)
- [Configuring Gx-Plus on page 446](#)

- [CLI Explorer](#)

Verifying and Managing Diameter Peer Information

Purpose View or clear Diameter peer information:

- Action**
- To display summary information about all Diameter peers:
`user@host> show diameter peer`
 - To display detailed information about all Diameter peers:
`user@host> show diameter peer detail`
 - To display information about a specific Diameter peer, add the peer name to the command:
`user@host> show diameter peer peer235`
`user@host> show diameter peer detail peer235`
 - To display summary information about Diameter peer-to-network-element mapping for all peers:
`user@host> show diameter peer map`
 - To display detailed information about Diameter peer-to-network-element mapping for all peers:
`user@host> show diameter peer map detail`
 - To display information about Diameter peer-to-network-element mapping for a specified peer, add the peer name to the command:
`user@host> show diameter peer map peer235`
`user@host> show diameter peer map detail peer235`
 - To display summary statistics about all Diameter peers:
`user@host> show diameter peer statistics`
 - To display detailed statistics about all Diameter peers:
`user@host> show diameter peer statistics detail`
 - To display summary statistics about a specified Diameter peer:
`user@host> show diameter peer statistics peer235`
 - To display detailed statistics about a specified Diameter peer:
`user@host> show diameter peer statistics detail peer235`
 - To delete the specified Diameter peer and all of its statistics.
`user@host> clear diameter peer peer5 connection`
 - To delete the specified Diameter peer and its current statistics:
`user@host> clear diameter peer peer5 statistics`

- Related Documentation**
- [Configuring Diameter on page 434](#)
 - [CLI Explorer](#)

Verifying Diameter Network Element Information

Purpose View Diameter network element information:

- Action**
- To display summary information about Diameter network elements:
`user@host> show diameter network-element`
 - To display detailed information about Diameter network elements:
`user@host> show diameter network-element detail`
 - To display information about Diameter network elements for a specified network element, include the element name in the command:
`user@host> show diameter network-element dne-1`
`user@host> show diameter network-element detail dne-1`
 - To display summary information about Diameter network-element-to-peer mapping for all network elements:
`user@host> show diameter network-element map`
 - To display detailed information about Diameter network-element-to-peer mapping for all network elements:
`user@host> show diameter network-element map detail`

- Related Documentation**
- [Configuring Diameter on page 434](#)
 - [CLI Explorer](#)

CHAPTER 57

Monitoring and Managing Subscriber Information on Static Interfaces

- [Forcing a Static Subscriber to Be Logged Out on page 505](#)
- [Resetting the State of an Interface for Static Subscriber Login on page 505](#)
- [Forcing a Group of Static Subscribers to Be Logged Out on page 506](#)
- [Resetting the State of an Interface Group for Static Subscriber Login on page 506](#)
- [Verifying Information about Subscriber Sessions on Static Interfaces on page 506](#)

Forcing a Static Subscriber to Be Logged Out

You can force a static subscriber to be logged out on an interface. After you do so, no subscriber can subsequently log in on that interface until the interface state is reset either by a router reset or by entering the **request services static-subscribers login interface** command.

- To forcibly log out a static subscriber on a static interface:
`user@host> request services static-subscribers logout interface ge-2/0/1.5`

Related Documentation

- [Resetting the State of an Interface for Static Subscriber Login on page 505](#)

Resetting the State of an Interface for Static Subscriber Login

When a static subscriber has been forcibly logged out on an interface with the **request services static-subscribers logout interface** command, you can reset the state of the interface. This action enables a static subscriber to log in on the interface. If you do not reset the state manually, then no static subscribers can log in on the interface until the state is reset by a router reset.

- To reset the state of a static interface:
`user@host> request services static-subscribers login interface ge-2/0/1.5`

Related Documentation

- [Forcing a Static Subscriber to Be Logged Out on page 505](#)

Forcing a Group of Static Subscribers to Be Logged Out

You can force the static subscribers on all interfaces in a group to be logged out. After you do so, no subscriber can subsequently log in on an interface in that group until the interface state is reset either by a router reset or by entering the **request services static-subscribers login group** command.

- To forcibly log out all static subscribers on a static interface group:

```
user@host> request services static-subscribers logout group boston
```

Related Documentation

- [Resetting the State of an Interface Group for Static Subscriber Login on page 506](#)

Resetting the State of an Interface Group for Static Subscriber Login

When static subscribers have been forcibly logged out on an interface group with the **request services static-subscribers logout group** command, you can reset the state of the group. This action enables static subscribers to log in on the interfaces in the group. If you do not reset the state manually, then no static subscribers can log in on any interface in the group until the state is reset by a router reset.

- To reset the state of a static interface group:

```
user@host> request services static-subscribers login group boston
```

Related Documentation

- [Forcing a Group of Static Subscribers to Be Logged Out on page 506](#)

Verifying Information about Subscriber Sessions on Static Interfaces

Purpose View information about subscriber sessions on static interfaces:

- Action**
- To display information about all static subscriber sessions:

```
user@host> show static-subscribers sessions
```

- To display information about the subscriber sessions for the specified group of static interfaces:

```
user@host> show static-subscribers sessions group boston
```

- To display information about the subscriber session for the specified interface:

```
user@host> show static-subscribers sessions interface ge-0/0/1.1
```

Related Documentation

- For more information, see the [CLI Explorer](#)
- [Configuring Subscribers over Static Interfaces on page 466](#)
- [Subscribers on Static Interfaces Overview on page 463](#)

CHAPTER 58

Monitoring and Managing Packet-Triggered Subscribers

- [Verifying and Managing PTSP Configuration on page 507](#)

Verifying and Managing PTSP Configuration

Purpose Display and clear information about packet-triggered subscribers and PTSP services.

- Action**
- To display bandwidth information about subscribers:
user@host> [show services subscriber bandwidth](#)
 - To display information about the active dynamic policies applied to a subscriber:
user@host> [show services subscriber dynamic-policies client-id client-id](#)
 - To display information about the data flows associated with a subscriber:
user@host> [show services subscriber flows client-id client-id](#)
 - To display information about the active packet-triggered subscriber sessions on the router:
user@host> [show services subscriber sessions](#)
 - To display information about the data traffic statistics for the packet-triggered subscriber:
user@host> [show services subscriber statistics client-id client-id](#)
 - To clear the active packet-triggered subscriber session on the router and log out the subscriber:
user@host> [clear services subscriber sessions client-id client-id](#)

Related Documentation

- [CLI Explorer](#)

PART 8

Configuring Router Advertisement for Subscriber Management

- [Configuring the Dynamic Router Advertisement Protocol on page 511](#)

Configuring the Dynamic Router Advertisement Protocol

- [Dynamic Router Advertisement and Subscriber Access on page 511](#)
- [Dynamic Router Advertisement Configuration Overview on page 511](#)
- [Configuring Dynamic Router Advertisement on page 512](#)

Dynamic Router Advertisement and Subscriber Access

Subscriber access supports the configuration of the Router Advertisement Protocol at the **[edit dynamic-profiles profile-name protocols]** hierarchy level. Statements configured at this hierarchy level are identical in function to those same statements used for static Router Advertisement Protocol configuration, with the exception of the **interface** and **prefix** statements which use dynamic variables.

- Related Documentation**
- For general information about configuring the Router Advertisement Protocol, see the *Junos OS Routing Protocols Library for Routing Devices*.

Dynamic Router Advertisement Configuration Overview

In a network deployment where router interfaces are configured statically, you might need to configure the Router Advertisement Protocol on only a small number of interfaces on which it might run. However, in a subscriber access network, static configuration of the Router Advertisement Protocol becomes impractical because the number of interfaces that potentially need the Router Advertisement Protocol increases substantially. In addition, deploying services in a dynamic environment requires dynamic modifications to interfaces as they are created.

Subscriber access supports the configuration of the Router Advertisement Protocol at the **[edit dynamic-profiles profile-name protocols]** hierarchy level. By specifying Router Advertisement Protocol statements within a dynamic profile, you can dynamically apply a Router Advertisement configuration when a subscriber connects to an interface using a particular access technology (for example, DHCP), enabling the subscriber to access a carrier (multicast) network.

To minimally configure the Router Advertisement Protocol requires that you include the **router-advertisement** statement at the **[edit dynamic-profiles profile-name protocols]**

hierarchy level and the **interface** statement along with the *\$junos-interface-name* dynamic variable. All other statements are optional.



NOTE: Statements used for Router Advertisement Protocol configuration at the [edit dynamic-profiles *profile-name* protocols] hierarchy level are identical in function to those same statements used for static Router Advertisement Protocol configuration, with the exception of the interface and prefix statements, which use dynamic variables.

**Related
Documentation**

- *Dynamic Profiles Overview*
- *Configuring Dynamic DHCP Client Access to a Multicast Network*
- *Configuring an Address-Assignment Pool for Router Advertisement*
- [Configuring Dynamic Router Advertisement on page 512](#)

Configuring Dynamic Router Advertisement

Configuration for Dynamic Router Advertisement is identical to that performed for static Router Advertisement interfaces, as described in conjunction with configuring Neighbor Discovery, with the exception of their being configured at the [edit dynamic-profiles *profile-name* protocols router-advertisement] hierarchy level.

**Related
Documentation**

- For specific Router Advertisement configuration tasks, see the *Junos OS Routing Protocols Library for Routing Devices*

PART 9

Troubleshooting

- [Configuring AAA Testing and Troubleshooting on page 515](#)
- [Tracing Extended DHCP Operations on page 521](#)
- [Configuring Subscriber Management Database Log Files on page 529](#)
- [Configuring Subscriber Management Database Trace Flags and Operations on page 531](#)
- [Configuring Subscriber Management Session Database Log Files on page 533](#)
- [Configuring Subscriber Management Session Database Trace Flags and Operations on page 535](#)
- [Configuring Diameter Base Protocol Log Files on page 539](#)
- [Configuring Diameter Base Protocol Trace Flags and Operations on page 543](#)
- [Troubleshooting Diameter Networks on page 547](#)
- [Configuring ANCP Log Files on page 549](#)
- [Configuring ANCP Trace Flags and Operations on page 553](#)
- [Configuring General Authentication Service Log Files on page 557](#)
- [Configuring General Authentication Service Trace Flags and Operations on page 559](#)
- [Configuring Static Subscriber Interfaces Log Files on page 567](#)
- [Configuring Static Subscriber Interfaces Trace Flags and Operations on page 571](#)
- [Configuring PTSP Tracing Operations on page 575](#)
- [Overriding PCRF Session Control to Troubleshoot a Session or Services on page 581](#)
- [Contacting Juniper Technical Support on page 583](#)

CHAPTER 60

Configuring AAA Testing and Troubleshooting

- [AAA Configuration Testing and Troubleshooting on page 515](#)
- [Testing a Subscriber AAA Configuration on page 515](#)

AAA Configuration Testing and Troubleshooting

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

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



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

Related Documentation

- [Testing a Subscriber AAA Configuration on page 515](#)

Testing a Subscriber AAA Configuration

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

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



.....

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

.....


```

Action user@host>test aaa ppp user thomastank@xyz.net password 00N15&
Authentication Grant
*****User Attributes*****
    User Name - thomastank@xyz.net
    Client IP Address - 192.168.1.1
    Client IP Netmask - 255.255.0.0
    Virtual Router Name - default
    Agent Remote Id - NULL
    Reply Message - NULL
    Primary DNS IP Address - 0.0.0.0
    Secondary DNS IP Address - 0.0.0.0
    Primary WINS IP Address - 0.0.0.0
    Secondary WINS IP Address - 0.0.0.0
    Primary DNS IPv6 Address - ::
    Secondary DNS IPv6 Address - ::
    Framed Pool - not set
    Class Attribute - TEST
    Service Type - 0
    Client IPv6 Address - ::
    Client IPv6 Mask - null
    Framed IPv6 Prefix - ::/0
    Framed IPv6 Pool - not-set
    NDRA IPv6 Prefix - not-set
    Login IPv6 Host - ::
    Framed Interface Id - 0:0:0:0
    Delegated IPv6 Prefix - ::/0
    Delegated IPv6 Pool - not-set
    User Password - 00N15&
    CHAP Password - NULL
    Mac Address - AB:CD:00:00:00:01
    Idle Timeout - 600
    Session Timeout - 6000
    Service Name (1) - cos-service(video_sch, nc_sch)

    Service Statistics (1) - 1
    Service Acct Interim (1) - 600
    Service Activation Type (1) - 1
    Service Name (2) - filter-service(in_filter,
out_filter)
    Service Statistics (2) - 2
    Service Acct Interim (2) - 900
    Service Activation Type (2) - 1
    Cos shaping rate - 100m
    Filter Id - not set
    Framed MTU - (null)
    Framed Route - not set
    Ingress Policy Name - not set
    Egress Policy Name - not set
    IGMP - disabled
    Redirect VR Name - default
    Service Bundle - Null
    Framed Ip Route Tag - not set
    Ignore DF Bit - disabled
    IGMP Access Group Name - not set
    IGMP Access Source Group Name - not set
    MLD Access Group Name - not set
    MLD Access Source Group Name - not set
    IGMP Version - not set
    MLD Version - not set
    IGMP Immediate Leave - disabled

```

```

MLD Immediate Leave - disabled
IPv6 Ingress Policy Name - not set
IPv6 Egress Policy Name - not set
Acct Session ID - 1
Acct Interim Interval - 750
Acct Type - 1
Ingress Statistics - disabled
Egress Statistics - disabled
Chargeable user identity - 0
NAS Port Id - -0/0/0.0
NAS Port - 4095
NAS Port Type - 15
Framed Protocol - 1
IPv4 ADF Rule - 010100
IPv4 ADF Rule - 010101
IPv6 ADF Rule - 030100
IPv6 ADF Rule - 030101
****Pausing 10 seconds before disconnecting the test user*****
Logging out subscriber
  Terminate Id - not set
Test complete. Exiting

```

You can use the **agent-remote-id ari** option with the **test aaa dhcp user** and **test aaa ppp user** commands to verify DHCP and PPP subscriber authentication in those networks that support the DSL Forum Agent-Remote-Id (VSA 26-2).

If you specify the DSL Forum Agent-Remote-Id, the output includes the specified value. If you do not specify the VSA, then the Agent-Remote-Id value is shown as **NULL**.

user@host>**test aaa ppp user** thomastank agent-remote-id "(202)555-1212"

```

Authentication Grant
*****User Attributes*****
  User Name - thomastank
  Client IP Address - 192.168.1.1
  Client IP Netmask - 255.255.0.0
  ...
  NAS Ip Address - 0.0.0.0
  Agent Remote Id - (202)555-1212
  ...

```

The following example shows output when the authentication grant fails due to an invalid password:

user@host>**test aaa ppp user** thomastank@xyz.net password 55N33%%56

```

Authentication Deny
Reason : Access Denied
Received Attributes :
  User Name - thomastank@xyz.net
  Client IP Address - 0.0.0.0
  Client IP Netmask - 0.0.0.0
  Virtual Router Name - default
  Agent Remote Id - NULL
  Reply Message - NULL
  Primary DNS IP Address - 0.0.0.0
  Secondary DNS IP Address - 0.0.0.0
  Primary WINS IP Address - 0.0.0.0
  Secondary WINS IP Address - 0.0.0.0
  Primary DNS IPv6 Address - ::
  Secondary DNS IPv6 Address - ::
  Framed Pool - not set

```

```

Class Attribute - not set
Service Type - 0
Client IPv6 Address - ::
Client IPv6 Mask - null
Framed IPv6 Prefix - ::/0
Framed IPv6 Pool - not-set
NDRA IPv6 Prefix - not-set
Login IPv6 Host - ::
Framed Interface Id - 0:0:0:0
Delegated IPv6 Prefix - ::/0
Delegated IPv6 Pool - not-set
User Password - 55N333%56
CHAP Password - NULL
Mac Address - AB:CD:00:00:00:01
Filter Id - not set
Framed MTU - (null)
Framed Route - not set
Ingress Policy Name - not set
Egress Policy Name - not set
IGMP - disabled
Redirect VR Name - default
Service Bundle - Null
Framed Ip Route Tag - not set
Ignore DF Bit - disabled
IGMP Access Group Name - not set
IGMP Access Source Group Name - not set
MLD Access Group Name - not set
MLD Access Source Group Name - not set
IGMP Version - not set
MLD Version - not set
IGMP Immediate Leave - disabled
MLD Immediate Leave - disabled
IPv6 Ingress Policy Name - not set
IPv6 Egress Policy Name - not set
Acct Session ID - 12
Acct Interim Interval - 0
Acct Type - 0
Ingress Statistics - disabled
Egress Statistics - disabled
Chargeable user identity - 0
NAS Port Id - -0/0/0.0
NAS Port - 4095
NAS Port Type - 15
Framed Protocol - 0
Test complete. Exiting

```

Related Documentation • [AAA Configuration Testing and Troubleshooting on page 515](#)

Tracing Extended DHCP Operations

- [Tracing Extended DHCP Operations on page 521](#)
- [Tracing Extended DHCP Operations for Specific Interfaces on page 527](#)

Tracing Extended DHCP Operations

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

You can configure DHCP trace operations at the global level and at the interface level. Global DHCP tracing logs all DHCP-related events, whereas interface-level tracing logs only interface-specific DHCP events. If you configure interface-level trace operations, you can specify tracing for a range of interfaces or an individual interface. However, only a single interface-level log file is supported. That is, you cannot specify different interface-level log files for different interfaces or groups of interfaces.

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

- Important events for both global and per-interface tracing are logged in a file located in the `/var/log` directory. By default, the router uses the filename, `jdhcpd`. You can specify a different filename, but you cannot change the directory in which trace files are located.
- When the trace log file *filename* reaches 128 kilobytes (KB), it is compressed and renamed *filename.0.gz*. Subsequent events are logged in a new file called *filename*, until it reaches capacity again. At this point, *filename.0.gz* is renamed *filename.1.gz* and *filename* is compressed and renamed *filename.0.gz*. This process repeats until the number of archived files reaches the maximum file number. Then the oldest trace file—the one with the highest number—is overwritten.

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

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

To configure global DHCP tracing operations.

- Specify tracing operations for DHCP local server and DHCP relay:

```
[edit system processes dhcp-service]
user@host# edit traceoptions
```

The tracing configuration is applied globally to all DHCP applications in every LS:RI. Configuration of event tracing on a per-LS:RI basis is not supported. DHCP tracing is configurable only in the default LS:RI. However, DHCP applications (local server or relay) do not have to be configured in the default LS:RI.



NOTE: We recommend that you use configure tracing statements at the `[edit system processes dhcp-service]` hierarchy level.

Because you can configure DHCP tracing at three different hierarchy levels (one new and recommended, two old and deprecated), the following rules apply to manage the interaction:

- When you configure a filename or any other options for the trace log file, the configuration at the `[edit system processes dhcp-service]` hierarchy level has the highest precedence, followed by the configuration at the `[edit system services dhcp-local-server]` hierarchy level, and finally with the lowest precedence, the configuration at the `[edit forwarding-options dhcp-relay]` hierarchy level.
- The flag configurations for multiple hierarchy levels are merged and applied to all trace log events.
- The deprecated statements do not support filtering the generation of DHCP trace log events by severity level. If you use these statements, trace logging operates with an implicit severity of **all**, regardless of the severity level configured at the `[edit system processes dhcp-service]` hierarchy level.

For information about configuring per-interface tracing options, see [“Tracing Extended DHCP Operations for Specific Interfaces” on page 526](#).

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

- [Configuring the Extended DHCP Log Filename on page 523](#)
- [Configuring the Number and Size of Extended DHCP Log Files on page 523](#)
- [Configuring Access to the Extended DHCP Log File on page 524](#)
- [Configuring a Regular Expression for Extended DHCP Messages to Be Logged on page 524](#)
- [Configuring the Extended DHCP Tracing Flags on page 524](#)
- [Configuring the Severity Level to Filter Which Extended DHCP Messages Are Logged on page 525](#)
- [Tracing Extended DHCP Operations for Specific Interfaces on page 526](#)

Configuring the Extended DHCP Log Filename

By default, the name of the file that records trace output is **jdhcpd**. You can specify a different name by including the **file** option. DHCP local server and DHCP relay agent both support the **file** option for the **traceoptions** statement and the **interface-traceoptions** statement.

To change the filename:

- Specify a filename for global tracing operations.

```
[edit system processes dhcp-service traceoptions]
user@host# set file filename
```

- Specify a filename for per-interface tracing operations.

```
[edit system processes dhcp-service interface-traceoptions]
user@host# set file filename
```

Configuring the Number and Size of Extended DHCP Log Files

You can optionally specify the number of compressed, archived trace log files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB); the default size is 128 kilobytes (KB).

The archived files are differentiated by a suffix in the format **.number.gz**. The newest archived file is **.0.gz** and the oldest archived file is **.(maximum number)-1.gz**. When the current trace log file reaches the maximum size, it is compressed and renamed, and any existing archived files are renamed. This process repeats until the maximum number of archived files is reached, at which point the oldest file is overwritten.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation, **filename**, reaches 2 MB, **filename** is compressed and renamed **filename.0.gz**, and a new file called **filename** is created. When the new **filename** reaches 2 MB, **filename.0.gz** is renamed **filename.1.gz** and **filename** is compressed and renamed **filename.0.gz**. This process repeats until there are 20 trace files. Then the oldest file, **filename.19.gz**, is simply overwritten when the next oldest file, **filename.18.gz** is compressed and renamed to **filename.19.gz**.

DHCP local server and DHCP relay agent both support the **files** and **size** options for the **traceoptions** statement and the **interface-traceoptions** statement. To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output for global tracing operations.

```
[edit system processes dhcp-service traceoptions]
user@host# set file filename files number size maximum-file-size
```

- Specify the name, number, and size of the file used for the trace output for per-interface tracing operations.

```
[edit system processes dhcp-service interface-traceoptions]
user@host# set file filename files number size maximum-file-size
```

Configuring Access to the Extended DHCP Log File

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

DHCP local server and DHCP relay agent both support the **world-readable** option and the **no-world-readable** option for the **traceoptions** statement and the **interface-traceoptions** statement. To specify that all users can read the log file:

- Configure the log file to be world-readable for global tracing operations.

```
[edit system processes dhcp-service traceoptions]  
user@host# set file filename world-readable
```

- Configure the log file to be world-readable for per-interface tracing operations.

```
[edit system processes dhcp-service interface-traceoptions]  
user@host# set file filename world-readable
```

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

- Configure the log file to be no-world-readable for global tracing operations.

```
[edit system processes dhcp-service traceoptions]  
user@host# set file filename no-world-readable
```

- Configure the log file to be no-world-readable for per-interface tracing operations.

```
[edit system processes dhcp-service interface-traceoptions]  
user@host# set file filename no-world-readable
```

Configuring a Regular Expression for Extended DHCP Messages to Be Logged

By default, the trace operation output includes all messages relevant to the logged events. You can refine the output by including regular expressions to be matched.

DHCP local server and DHCP relay agent both support the **match** option for the **traceoptions** statement and the **interface-traceoptions** statement. To configure regular expressions to be matched:

- Specify the regular expression for global tracing operations.

```
[edit system processes dhcp-service traceoptions]  
user@host# set file filename match regular-expression
```

- Specify the regular expression for per-interface tracing operations.

```
[edit system processes dhcp-service interface-traceoptions]  
user@host# set file filename match regular-expression
```

Configuring the Extended DHCP Tracing Flags

By default, only important events are logged. You can specify which events and operations are logged by specifying one or more tracing flags.

DHCP local server and DHCP relay agent both support the **flag** option for the **traceoptions** statement and the **interface-traceoptions** statement. A smaller set of flags is supported for interface-level tracing than for global tracing. To configure the flags for the events to be logged:

- Specify the flags for global tracing operations.

```
[edit system processes dhcp-service traceoptions]
user@host# set flag flag
```

- Specify the flags for per-interface tracing operations.

```
[edit system processes dhcp-service interface-traceoptions]
user@host# set flag flag
```

Configuring the Severity Level to Filter Which Extended DHCP Messages Are Logged

The messages associated with a logged event are categorized according to severity level. You can use the severity level to determine which messages are logged for the event type. A low severity level is less restrictive—filters out fewer messages—than a higher level. When you configure a severity level, all messages at that level and all higher (more restrictive) levels are logged.

The following list presents severity levels in order from lowest (least restrictive) to highest (most restrictive). This order also represents the significance of the messages; for example, **error** messages are of greater concern than **info** messages.

- **verbose**
- **info**
- **notice**
- **warning**
- **error**

The severity level that you configure depends on the issue that you are trying to resolve. In some cases you might be interested in seeing all messages relevant to the logged event, so you specify **all**. You can also specify **verbose** with the same result, because **verbose** is the lowest (least restrictive) severity level; it has nothing to do with the terseness or verbosity of the messages. Either choice generates a large amount of output. You can specify a more restrictive severity level, such as **notice** or **info** to filter the messages. By default, the trace operation output includes only messages with a severity level of **error**.

DHCP local server and DHCP relay agent both support the **level** option for the **traceoptions** statement and the **interface-traceoptions** statement. To configure the flags for the events to be logged:

- Specify the severity level for global tracing operations.

```
[edit system processes dhcp-service traceoptions]
user@host# set level severity
```

- Specify the severity level for per-interface tracing operations.

```
[edit system processes dhcp-service interface-traceoptions]  
user@host# set level severity
```

Tracing Extended DHCP Operations for Specific Interfaces

In addition to the global DHCP tracing operations, subscriber management enables you to trace extended DHCP operations for a specific interface or for a range of interfaces.

Configuring per-interface tracing is a two-step procedure. In the first step, you specify the tracing options that you want to use, such as file information and flags. In the second step, you enable the tracing operation on the specific interfaces.

To configure per-interface tracing operations:

1. Specify the tracing options you want to use.



NOTE: Per-interface tracing uses the same default tracing behavior as the global extended DHCP tracing operation. The default behavior is described in [“Tracing Extended DHCP Operations” on page 521](#).

- a. Specify that you want to configure per-interface tracing options.

- For DHCP local server, DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent:

```
[edit system processes dhcp-service]  
user@host# edit interface-traceoptions
```

- b. (Optional) Specify the tracing file options.

- Configure the name for the file used for the trace output.

See [“Configuring the Extended DHCP Log Filename” on page 523](#).

- Configure the number and size of the log files.

See [“Configuring the Number and Size of Extended DHCP Log Files” on page 523](#).

- Configure access to the log file.

See [“Configuring Access to the Extended DHCP Log File” on page 524](#).

- Configure a regular expression to filter logging events.

See [“Configuring a Regular Expression for Extended DHCP Messages to Be Logged” on page 524](#).

- c. (Optional) Specify tracing flag options.

See [“Configuring the Extended DHCP Tracing Flags” on page 524](#).

- d. (Optional) Configure a severity level for messages to specify which event messages are logged.

See [“Configuring the Severity Level to Filter Which Extended DHCP Messages Are Logged” on page 525](#).

2. Enable tracing on an interface or interface range.

The following examples show a DHCP local server configuration. You can also use the **trace** statement at the **[edit forwarding-options dhcp-relay]** hierarchy level and at the **[edit system services dhcp-local-server dhcpv6]** hierarchy level.

- Enable tracing on a specific interface.

```
[edit system services dhcp-local-server]
user@host# set group group-name interface interface-name trace
```

- Enable tracing on a range of interfaces.

```
[edit system services dhcp-local-server]
user@host# set group group-name interface interface-name upto interface
interface-name trace
```

Tracing Extended DHCP Operations for Specific Interfaces

In addition to the global DHCP tracing operations, subscriber management enables you to trace extended DHCP operations for a specific interface or for a range of interfaces.

Configuring per-interface tracing is a two-step procedure. In the first step, you specify the tracing options that you want to use, such as file information and flags. In the second step, you enable the tracing operation on the specific interfaces.

To configure per-interface tracing operations:

1. Specify the tracing options you want to use.



NOTE: Per-interface tracing uses the same default tracing behavior as the global extended DHCP tracing operation. The default behavior is described in [“Tracing Extended DHCP Operations” on page 521](#).

- a. Specify that you want to configure per-interface tracing options.

- For DHCP local server, DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent:

```
[edit system processes dhcp-service]
user@host# edit interface-traceoptions
```

- b. (Optional) Specify the tracing file options.

- Configure the name for the file used for the trace output.

See [“Configuring the Extended DHCP Log Filename” on page 523](#).

- Configure the number and size of the log files.

See [“Configuring the Number and Size of Extended DHCP Log Files” on page 523](#).

- Configure access to the log file.

See [“Configuring Access to the Extended DHCP Log File” on page 524](#).

- Configure a regular expression to filter logging events.

See [“Configuring a Regular Expression for Extended DHCP Messages to Be Logged” on page 524.](#)

- c. (Optional) Specify tracing flag options.

See [“Configuring the Extended DHCP Tracing Flags” on page 524.](#)

- d. (Optional) Configure a severity level for messages to specify which event messages are logged.

See [“Configuring the Severity Level to Filter Which Extended DHCP Messages Are Logged” on page 525.](#)

- 2. Enable tracing on an interface or interface range.

The following examples show a DHCP local server configuration. You can also use the **trace** statement at the **[edit forwarding-options dhcp-relay]** hierarchy level and at the **[edit system services dhcp-local-server dhcpv6]** hierarchy level.

- Enable tracing on a specific interface.

```
[edit system services dhcp-local-server]
user@host# set group group-name interface interface-name trace
```

- Enable tracing on a range of interfaces.

```
[edit system services dhcp-local-server]
user@host# set group group-name interface interface-name upto interface
interface-name trace
```

**Related
Documentation**

- [Tracing Extended DHCP Operations on page 521](#)

CHAPTER 62

Configuring Subscriber Management Database Log Files

- [Configuring the Number and Size of Subscriber Management Database Log Files on page 529](#)
- [Configuring Access to the Subscriber Management Database Log File on page 530](#)
- [Configuring a Regular Expression for Subscriber Management Database Messages to Be Logged on page 530](#)

Configuring the Number and Size of Subscriber Management Database Log Files

You can optionally specify the number of compressed, archived trace log files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB); the default size is 128 kilobytes (KB).

The archived files are differentiated by a suffix in the format *.number.gz*. The newest archived file is *.0.gz* and the oldest archived file is *.(maximum number)-1.gz*. When the current trace log file reaches the maximum size, it is compressed and renamed, and any existing archived files are renamed. This process repeats until the maximum number of archived files is reached, at which point the oldest file is overwritten.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation, *filename*, reaches 2 MB, *filename* is compressed and renamed *filename.0.gz*, and a new file called *filename* is created. When the new *filename* reaches 2 MB, *filename.0.gz* is renamed *filename.1.gz* and *filename* is compressed and renamed *filename.0.gz*. This process repeats until there are 20 trace files. Then the oldest file, *filename.19.gz*, is simply overwritten when the next oldest file, *filename.18.gz* is compressed and renamed to *filename.19.gz*.

To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output.

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

Related Documentation

- [Tracing Subscriber Management Database Operations for Subscriber Access on page 531](#)

Configuring Access to the Subscriber Management Database Log File

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

To specify that all users can read the log file:

- Configure the log file to be world-readable.

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

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

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

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

Related Documentation

- [Tracing Subscriber Management Database Operations for Subscriber Access on page 531](#)

Configuring a Regular Expression for Subscriber Management Database Messages to Be Logged

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

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

To configure regular expressions to be matched:

- Configure the regular expression.

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

Related Documentation

- [Tracing Subscriber Management Database Operations for Subscriber Access on page 531](#)

Configuring Subscriber Management Database Trace Flags and Operations

- [Tracing Subscriber Management Database Operations for Subscriber Access on page 531](#)
- [Configuring the Subscriber Management Database Trace Log Filename on page 532](#)
- [Configuring the Subscriber Management Database Tracing Flags on page 532](#)

Tracing Subscriber Management Database Operations for Subscriber Access

The Junos OS trace feature tracks subscriber management database operations and records events in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

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

1. Important events are logged in a file located in the `/var/log` directory. By default, the router uses the filename **smid**. You can specify a different filename, but you cannot change the directory in which trace files are located.
2. When the trace log file **filename** reaches 128 kilobytes (KB), it is compressed and renamed **filename.0.gz**. Subsequent events are logged in a new file called **filename**, until it reaches capacity again. At this point, **filename.0.gz** is renamed **filename.1.gz** and **filename** is compressed and renamed **filename.0.gz**. This process repeats until the number of archived files reaches the maximum file number. Then the oldest trace file—the one with the highest number—is overwritten.

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

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

To configure all aspects of subscriber management database tracing operations:

1. Configure a trace log filename.

See “Configuring the Subscriber Management Database Trace Log Filename” on page 532.

2. Configure the number and size of trace logs.

See “Configuring the Number and Size of Subscriber Management Database Log Files” on page 529.

3. Configure user access to trace logs.

See “Configuring Access to the Subscriber Management Database Log File” on page 530.

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

See “Configuring a Regular Expression for Subscriber Management Database Messages to Be Logged” on page 530.

5. Configure flags to specify which events are logged.

See “Configuring the Subscriber Management Database Tracing Flags” on page 532.

Configuring the Subscriber Management Database Trace Log Filename

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

To configure the filename for subscriber management database tracing operations:

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

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

Related Documentation

- [Tracing Subscriber Management Database Operations for Subscriber Access on page 531](#)

Configuring the Subscriber Management Database Tracing Flags

By default, only important events are logged. You can specify which events and operations are logged by specifying one or more tracing flags.

To configure the flags for the events to be logged:

- Configure the flags.

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

Related Documentation

- [Tracing Subscriber Management Database Operations for Subscriber Access on page 531](#)

Configuring Subscriber Management Session Database Log Files

- [Configuring the Number and Size of Subscriber Management Session Database Replication Log Files on page 533](#)
- [Configuring Access to the Subscriber Management Session Database Replication Log File on page 534](#)
- [Configuring a Regular Expression for Subscriber Management Session Database Replication Messages to Be Logged on page 534](#)

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

You can optionally specify the number of compressed, archived trace log files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB); the default size is 128 kilobytes (KB).

The archived files are differentiated by a suffix in the format *.number.gz*. The newest archived file is *.0.gz* and the oldest archived file is *.(maximum number)-1.gz*. When the current trace log file reaches the maximum size, it is compressed and renamed, and any existing archived files are renamed. This process repeats until the maximum number of archived files is reached, at which point the oldest file is overwritten.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation, *filename*, reaches 2 MB, *filename* is compressed and renamed *filename.0.gz*, and a new file called *filename* is created. When the new *filename* reaches 2 MB, *filename.0.gz* is renamed *filename.1.gz* and *filename* is compressed and renamed *filename.0.gz*. This process repeats until there are 20 trace files. Then the oldest file, *filename.19.gz*, is simply overwritten when the next oldest file, *filename.18.gz* is compressed and renamed to *filename.19.gz*.

To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output.

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

- Related Documentation**
- [Tracing Subscriber Management Session Database Replication Operations for Subscriber Access on page 535](#)

Configuring Access to the Subscriber Management Session Database Replication Log File

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

To specify that all users can read the log file:

- Configure the log file to be world-readable.

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

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

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

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

- Related Documentation**
- [Tracing Subscriber Management Session Database Replication Operations for Subscriber Access on page 535](#)

Configuring a Regular Expression for Subscriber Management Session Database Replication Messages to Be Logged

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

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

To configure regular expressions to be matched:

- Configure the regular expression.

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

- Related Documentation**
- [Tracing Subscriber Management Session Database Replication Operations for Subscriber Access on page 535](#)

Configuring Subscriber Management Session Database Trace Flags and Operations

- [Tracing Subscriber Management Session Database Replication Operations for Subscriber Access on page 535](#)
- [Configuring the Subscriber Management Session Database Replication Trace Log Filename on page 536](#)
- [Configuring the Subscriber Management Session Database Replication Tracing Flags on page 536](#)

Tracing Subscriber Management Session Database Replication Operations for Subscriber Access

The Junos OS trace feature tracks subscriber management database replication operations and records events in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

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

1. Important events are logged in a file located in the **/var/log** directory. By default, the router uses the filename **bdbrepd**. You can specify a different filename, but you cannot change the directory in which trace files are located.
2. When the trace log file **filename** reaches 128 kilobytes (KB), it is compressed and renamed **filename.0.gz**. Subsequent events are logged in a new file called **filename**, until it reaches capacity again. At this point, **filename.0.gz** is renamed **filename.1.gz** and **filename** is compressed and renamed **filename.0.gz**. This process repeats until the number of archived files reaches the maximum file number. Then the oldest trace file—the one with the highest number—is overwritten.

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

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

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

1. Configure a trace log filename.

See [“Configuring the Subscriber Management Session Database Replication Trace Log Filename” on page 536](#).

2. Configure the number and size of trace logs.

See [“Configuring the Number and Size of Subscriber Management Session Database Replication Log Files” on page 533](#).

3. Configure user access to trace logs.

See [“Configuring Access to the Subscriber Management Session Database Replication Log File” on page 534](#).

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

See [“Configuring a Regular Expression for Subscriber Management Session Database Replication Messages to Be Logged” on page 534](#).

5. Configure flags to specify which events are logged.

See [“Configuring the Subscriber Management Session Database Replication Tracing Flags” on page 536](#).

Configuring the Subscriber Management Session Database Replication Trace Log Filename

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

To configure the filename for subscriber management database tracing operations:

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

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

Related Documentation

- [Tracing Subscriber Management Session Database Replication Operations for Subscriber Access on page 535](#)

Configuring the Subscriber Management Session Database Replication Tracing Flags

By default, only important events are logged. You can specify which events and operations are logged by specifying one or more tracing flags.

To configure the flags for the events to be logged:

- Configure the flags.

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

- Related Documentation**
- [Tracing Subscriber Management Session Database Replication Operations for Subscriber Access on page 535](#)

Configuring Diameter Base Protocol Log Files

- [Configuring the Number and Size of Diameter Base Protocol Log Files on page 539](#)
- [Configuring Access to the Diameter Base Protocol Log File on page 540](#)
- [Configuring a Regular Expression for Diameter Base Protocol Messages to Be Logged on page 540](#)
- [Configuring the Severity Level to Filter Which Diameter Base Protocol Messages Are Logged on page 540](#)

Configuring the Number and Size of Diameter Base Protocol Log Files

You can optionally specify the number of compressed, archived trace log files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB); the default size is 128 kilobytes (KB).

The archived files are differentiated by a suffix in the format *.number.gz*. The newest archived file is *.0.gz* and the oldest archived file is *.(maximum number)-1.gz*. When the current trace log file reaches the maximum size, it is compressed and renamed, and any existing archived files are renamed. This process repeats until the maximum number of archived files is reached, at which point the oldest file is overwritten.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation, *filename*, reaches 2 MB, *filename* is compressed and renamed *filename.0.gz*, and a new file called *filename* is created. When the new *filename* reaches 2 MB, *filename.0.gz* is renamed *filename.1.gz* and *filename* is compressed and renamed *filename.0.gz*. This process repeats until there are 20 trace files. Then the oldest file, *filename.19.gz*, is simply overwritten when the next oldest file, *filename.18.gz* is compressed and renamed to *filename.19.gz*.

To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output. (Diameter base protocol supports the **files** and **size** options for the **traceoptions** statement.)

```
[edit system processes diameter-service traceoptions]  
user@host# set file diam_1_logfile_1 files 20 size 2097152
```

- Related Documentation**
- [Tracing Diameter Base Protocol Processes for Subscriber Access on page 543](#)

Configuring Access to the Diameter Base Protocol Log File

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

To specify that all users can read the log file:

- Configure the log file to be world-readable.

```
[edit system processes diameter-service traceoptions]  
user@host# set file diam_1_logfile_1 world-readable
```

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

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

```
[edit system processes diameter-service traceoptions]  
user@host# set file diam_1_logfile_1 no-world-readable
```

- Related Documentation**
- [Tracing Diameter Base Protocol Processes for Subscriber Access on page 543](#)

Configuring a Regular Expression for Diameter Base Protocol Messages to Be Logged

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

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

To configure regular expressions to be matched:

- Configure the regular expression.

```
[edit system processes diameter-service traceoptions]  
user@host# set file diam_1_logfile_1 match regex
```

- Related Documentation**
- [Tracing Diameter Base Protocol Processes for Subscriber Access on page 543](#)

Configuring the Severity Level to Filter Which Diameter Base Protocol Messages Are Logged

The messages associated with a logged event are categorized according to severity level. You can use the severity level to determine which messages are logged for the event type. The severity level that you configure depends on the issue that you are trying to resolve. In some cases you might be interested in seeing all messages relevant to the logged event, so you specify **all** or **verbose**. Either choice generates a large amount of

output. You can specify a more restrictive severity level, such as **notice** or **info** to filter the messages. By default, the trace operation output includes only messages with a severity level of **error**.

To configure the type of messages to be logged:

- Configure the message severity level.

```
[edit system processes diameter-service traceoptions]  
user@host# set level severity
```

**Related
Documentation**

- [Tracing Diameter Base Protocol Processes for Subscriber Access on page 543](#)

Configuring Diameter Base Protocol Trace Flags and Operations

- [Tracing Diameter Base Protocol Processes for Subscriber Access on page 543](#)
- [Configuring the Diameter Base Protocol Trace Log Filename on page 544](#)
- [Configuring the Diameter Base Protocol Tracing Flags on page 544](#)

Tracing Diameter Base Protocol Processes for Subscriber Access

The Junos OS trace feature tracks Diameter base protocol operations and records events in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

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

1. Important events are logged in a file located in the `/var/log` directory. By default, the router uses the filename `jdiameterd`. You can specify a different filename, but you cannot change the directory in which trace files are located.
2. When the trace log file *filename* reaches 128 kilobytes (KB), it is compressed and renamed *filename.0.gz*. Subsequent events are logged in a new file called *filename*, until it reaches capacity again. At this point, *filename.0.gz* is renamed *filename.1.gz* and *filename* is compressed and renamed *filename.0.gz*. This process repeats until the number of archived files reaches the maximum file number. Then the oldest trace file—the one with the highest number—is overwritten.

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

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

To configure Diameter base protocol tracing operations:

1. (Optional) Configure a trace log filename.
See [“Configuring the Diameter Base Protocol Trace Log Filename” on page 544.](#)
2. (Optional) Configure the number and size of trace logs.
See [“Configuring the Number and Size of Diameter Base Protocol Log Files” on page 539.](#)
3. (Optional) Configure user access to trace logs.
See [“Configuring Access to the Diameter Base Protocol Log File” on page 540.](#)
4. (Optional) Configure a regular expression to filter the information to be included in the trace log.
See [“Configuring a Regular Expression for Diameter Base Protocol Messages to Be Logged” on page 540.](#)
5. (Optional) Configure flags to specify which events are logged.
See [“Configuring the Diameter Base Protocol Tracing Flags” on page 544.](#)
6. (Optional) Configure a severity level for messages to specify which event messages are logged.
See [“Configuring the Severity Level to Filter Which Diameter Base Protocol Messages Are Logged” on page 540.](#)

Configuring the Diameter Base Protocol Trace Log Filename

By default, the name of the file that records trace output for Diameter base protocol is **jdiameterd**. You can specify a different name with the **file** option.

To configure the filename for Diameter base protocol tracing operations:

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

```
[edit system processes diameter-service traceoptions]  
user@host# set file diam_logfile_1
```

Related Documentation

- [Tracing Diameter Base Protocol Processes for Subscriber Access on page 543](#)

Configuring the Diameter Base Protocol Tracing Flags

By default, only important events are logged. You can specify which events and operations are logged by specifying one or more tracing flags.

To configure the flags for the events to be logged:

- Configure the flags.

```
[edit system processes diameter-service traceoptions]  
user@host# set flag dne
```

- Related Documentation**
- [Tracing Diameter Base Protocol Processes for Subscriber Access on page 543](#)

Troubleshooting Diameter Networks

- [Troubleshooting Diameter Network Configuration on page 547](#)
- [Troubleshooting Diameter Network Connectivity on page 547](#)

Troubleshooting Diameter Network Configuration

Problem **Description:** A misconfiguration of the network can prevent Diameter from functioning properly. Configuration options for the Diameter base protocol are simplifying the discovery of a misconfiguration.

Symptoms: The output of the **show diameter peer** command indicates a peer is in the no-activation state. In this case issue the **show diameter peer map** and **show diameter network-element map** commands to determine which network elements use the peer. The output of these commands can indicate why the peer is not activated. For example, all the associated network elements might have higher-priority peers in the open state. The failed-to-forward counters are increasing in the output of the **show diameter function statistics detail** command. this can indicate that the routes to the peer are incorrectly configured. Check the network connectivity, then use the **show diameter routes** command to determine whether application traffic is being correctly forwarded.

Cause Typical misconfigurations appear in the routes, peers, and network element configurations.

Solution Use the appropriate statements to correct the misconfiguration.

Related Documentation

- [show diameter function statistics on page 1130](#)
- [show diameter network-element map on page 1138](#)
- [show diameter peer on page 1141](#)
- [show diameter peer map on page 1146](#)
- [show diameter route on page 1153](#)

Troubleshooting Diameter Network Connectivity

Problem **Description:** In some circumstances, problems can arise with network connectivity to Diameter peers. The problem may originate with the peer or the peer host.

Symptoms: The output of the **show diameter peer** command indicates a peer is in the suspended, rejected, or bad-peer state.

Cause The suspended state indicates that the peer is not responding or has some other malfunction, or the network path to the peer does not exist.

The rejected state indicates that the network connection has been rejected by the peer.

The bad-peer state indicates that the network connection has been rejected by the router on which the peer resides.

Solution Determine how persistent the problem is by issuing the **show diameter peer statistics peer-name brief** command to check the connectivity statistics.

Related Documentation

- [show diameter peer on page 1141](#)
- [show diameter peer statistics on page 1149](#)

Configuring ANCP Log Files

- [Configuring the Number and Size of ANCP Log Files on page 549](#)
- [Configuring Access to the ANCP Log File on page 550](#)
- [Configuring a Regular Expression for ANCP Messages to Be Logged on page 550](#)
- [Configuring the Severity Level to Filter Which ANCP Messages Are Logged on page 550](#)

Configuring the Number and Size of ANCP Log Files

You can optionally specify the number of compressed, archived trace log files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB); the default size is 128 kilobytes (KB).

The archived files are differentiated by a suffix in the format *.number.gz*. The newest archived file is *.0.gz* and the oldest archived file is *.(maximum number)-1.gz*. When the current trace log file reaches the maximum size, it is compressed and renamed, and any existing archived files are renamed. This process repeats until the maximum number of archived files is reached, at which point the oldest file is overwritten.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation, *filename*, reaches 2 MB, *filename* is compressed and renamed *filename.0.gz*, and a new file called *filename* is created. When the new *filename* reaches 2 MB, *filename.0.gz* is renamed *filename.1.gz* and *filename* is compressed and renamed *filename.0.gz*. This process repeats until there are 20 trace files. Then the oldest file, *filename.19.gz*, is simply overwritten when the next oldest file, *filename.18.gz* is compressed and renamed to *filename.19.gz*.

To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output.

```
[edit protocols ancp traceoptions]  
user@host# set file ancp_1_logfile_1 files 20 size 2097152
```

Related Documentation

- [Tracing ANCP Agent Operations for Subscriber Access on page 553](#)

Configuring Access to the ANCP Log File

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

To specify that all users can read the log file:

- Configure the log file to be world-readable.

```
[edit protocols ancp traceoptions]  
user@host# set file ancp_1_logfile_1 world-readable
```

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

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

```
[edit protocols ancp traceoptions]  
user@host# set file ancp_1_logfile_1 no-world-readable
```

Related Documentation

- [Tracing ANCP Agent Operations for Subscriber Access on page 553](#)

Configuring a Regular Expression for ANCP Messages to Be Logged

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

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

To configure regular expressions to be matched:

- Configure the regular expression.

```
[edit protocols ancp traceoptions]  
user@host# set file ancp_1_logfile_1 match regex
```

Related Documentation

- [Tracing ANCP Agent Operations for Subscriber Access on page 553](#)

Configuring the Severity Level to Filter Which ANCP Messages Are Logged

The messages associated with a logged event are categorized according to severity level. You can use the severity level to determine which messages are logged for the event type. The severity level that you configure depends on the issue that you are trying to resolve. In some cases you might be interested in seeing all messages relevant to the logged event, so you specify **all** or **verbose**. Either choice generates a large amount of output. You can specify a more restrictive severity level, such as **notice** or **info** to filter the messages. By default, the trace operation output includes only messages with a severity level of **error**.

To configure the type of messages to be logged:

- Configure the message severity level.

```
[edit protocols ancp traceoptions]  
user@host# set level severity
```

**Related
Documentation**

- [Tracing ANCP Agent Operations for Subscriber Access on page 553](#)
- [Configuring the ANCP Agent on page 368](#)
- [traceoptions on page 954](#)

Configuring ANCP Trace Flags and Operations

- [Tracing ANCP Agent Operations for Subscriber Access on page 553](#)
- [Configuring the ANCP Trace Log Filename on page 554](#)
- [Configuring the ANCP Tracing Flags on page 554](#)

Tracing ANCP Agent Operations for Subscriber Access

The Junos OS trace feature tracks ANCP agent operations and records events in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

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

1. Important events are logged in a file located in the `/var/log` directory. By default, the router uses the filename **ancpd**. You can specify a different filename, but you cannot change the directory in which trace files are located.
2. When the trace log file **filename** reaches 128 kilobytes (KB), it is compressed and renamed **filename.0.gz**. Subsequent events are logged in a new file called **filename**, until it reaches capacity again. At this point, **filename.0.gz** is renamed **filename.1.gz** and **filename** is compressed and renamed **filename.0.gz**. This process repeats until the number of archived files reaches the maximum file number. Then the oldest trace file—the one with the highest number—is overwritten.

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

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

To configure ANCP agent tracing operations:

1. (Optional) Configure a trace log filename.
See [“Configuring the ANCP Trace Log Filename” on page 554.](#)
2. (Optional) Configure the number and size of trace logs.
See [“Configuring the Number and Size of ANCP Log Files” on page 549.](#)
3. (Optional) Configure user access to trace logs.
See [“Configuring Access to the ANCP Log File” on page 550.](#)
4. (Optional) Configure a regular expression to filter the information to be included in the trace log.
See [“Configuring a Regular Expression for ANCP Messages to Be Logged” on page 550.](#)
5. (Optional) Configure flags to specify which events are logged.
See [“Configuring the ANCP Tracing Flags” on page 554.](#)
6. (Optional) Configure a severity level for messages to specify which event messages are logged.
See [“Configuring the Severity Level to Filter Which ANCP Messages Are Logged” on page 550.](#)

Related Documentation • [Configuring the ANCP Agent on page 368](#)

Configuring the ANCP Trace Log Filename

By default, the name of the file that records trace output for ANCP is **ancpd**. You can specify a different name with the **file** option.

To configure the filename for ANCP tracing operations:

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

```
[edit protocols ancp traceoptions]  
user@host# set file ancp_1
```

Related Documentation • [Tracing ANCP Agent Operations for Subscriber Access on page 553](#)

Configuring the ANCP Tracing Flags

By default, only important events are logged. You can specify which events and operations are logged by specifying one or more tracing flags.

To configure the flags for the events to be logged:

- Configure the flags.

```
[edit protocols ancp traceoptions]
```

```
user@host# set flag restart
```

Related Documentation

- [Tracing ANCP Agent Operations for Subscriber Access on page 553](#)

Configuring General Authentication Service Log Files

- [Configuring the Number and Size of General Authentication Service Processes Log Files on page 557](#)
- [Configuring Access to the Log File on page 558](#)
- [Configuring a Regular Expression for Lines to Be Logged on page 558](#)

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

You can optionally specify the number of compressed, archived trace log files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB); the default size is 128 kilobytes (KB).

The archived files are differentiated by a suffix in the format *.number.gz*. The newest archived file is *.0.gz* and the oldest archived file is *.(maximum number)-1.gz*. When the current trace log file reaches the maximum size, it is compressed and renamed, and any existing archived files are renamed. This process repeats until the maximum number of archived files is reached, at which point the oldest file is overwritten.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation, *filename*, reaches 2 MB, *filename* is compressed and renamed *filename.0.gz*, and a new file called *filename* is created. When the new *filename* reaches 2 MB, *filename.0.gz* is renamed *filename.1.gz* and *filename* is compressed and renamed *filename.0.gz*. This process repeats until there are 20 trace files. Then the oldest file, *filename.19.gz*, is simply overwritten when the next oldest file, *filename.18.gz* is compressed and renamed to *filename.19.gz*.

To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output, by including the **files** and **size** options with the **traceoptions** statement.

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

- Related Documentation**
- [Tracing General Authentication Service Processes on page 559](#)

Configuring Access to the Log File

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

To specify that all users can read the log file:

- Configure the log file to be world-readable.

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

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

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

```
[edit system processes general-authentication-service traceoptions]  
user@host# set file aap_logfile_1 no-world-readable
```

- Related Documentation**
- [Tracing General Authentication Service Processes on page 559](#)

Configuring a Regular Expression for Lines to Be Logged

By default, the trace operation output includes all lines relevant to the logged events. You can refine the output by including regular expressions (regex) that will be matched.

To configure regular expressions to match:

- Configure the regular expression.

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

- Related Documentation**
- [Tracing General Authentication Service Processes on page 559](#)

Configuring General Authentication Service Trace Flags and Operations

- [Tracing General Authentication Service Processes on page 559](#)
- [Configuring the General Authentication Service Processes Trace Log Filename on page 563](#)
- [Configuring the Trace Operation on page 564](#)
- [Configuring Subscriber Filtering for General Authentication Service Trace Operations on page 564](#)

Tracing General Authentication Service Processes

The Junos OS trace operations feature tracks general authentication service operations and records events in a log file. By default, the tracing operation is inactive. To trace general authentication service processes, you specify flags in the **traceoptions** statement at the **[edit system processes general-authentication-service]** hierarchy level. The default tracing behavior is the following:

- Important events are logged in a file located in the **/var/log** directory. By default, the router uses the filename, **authd**. You can specify a different filename, but you cannot change the directory (**/var/log**) in which trace files are located.
- When the trace log file **filename** reaches 128 kilobytes (KB), it is compressed and renamed **filename.0.gz**. Subsequent events are logged in a new file called **filename**, until it reaches capacity again. At this point, **filename.0.gz** is renamed **filename.1.gz** and **filename** is compressed and renamed **filename.0.gz**. This process repeats until the number of archived files reaches the maximum file number. Then the oldest trace file—the one with the highest number—is overwritten.

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

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

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

- [Configuring the General Authentication Service Processes Trace Log Filename on page 560](#)
- [Configuring the Number and Size of General Authentication Service Processes Log Files on page 560](#)
- [Configuring Access to the Log File on page 561](#)
- [Configuring a Regular Expression for Lines to Be Logged on page 561](#)
- [Configuring Subscriber Filtering for General Authentication Service Trace Operations on page 561](#)
- [Configuring the Trace Operation on page 562](#)

Configuring the General Authentication Service Processes Trace Log Filename

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

To configure the filename for general authentication service tracing operations:

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

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

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

You can optionally specify the number of compressed, archived trace log files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB); the default size is 128 kilobytes (KB).

The archived files are differentiated by a suffix in the format **.number.gz**. The newest archived file is **.0.gz** and the oldest archived file is **.(maximum number)-1.gz**. When the current trace log file reaches the maximum size, it is compressed and renamed, and any existing archived files are renamed. This process repeats until the maximum number of archived files is reached, at which point the oldest file is overwritten.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation, **filename**, reaches 2 MB, **filename** is compressed and renamed **filename.0.gz**, and a new file called **filename** is created. When the new **filename** reaches 2 MB, **filename.0.gz** is renamed **filename.1.gz** and **filename** is compressed and renamed **filename.0.gz**. This process repeats until there are 20 trace files. Then the oldest file, **filename.19.gz**, is simply overwritten when the next oldest file, **filename.18.gz** is compressed and renamed to **filename.19.gz**.

To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output, by including the **files** and **size** options with the **traceoptions** statement.

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

Configuring Access to the Log File

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

To specify that all users can read the log file:

- Configure the log file to be world-readable.

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

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

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

```
[edit system processes general-authentication-service traceoptions]  
user@host# set file aap_logfile_1 no-world-readable
```

Configuring a Regular Expression for Lines to Be Logged

By default, the trace operation output includes all lines relevant to the logged events. You can refine the output by including regular expressions (regex) that will be matched.

To configure regular expressions to match:

- Configure the regular expression.

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

Configuring Subscriber Filtering for General Authentication Service Trace Operations

You can apply filters to the general authentication service to limit tracing to particular subscribers or domains. Subscriber filtering simplifies troubleshooting in a scaled environment by enabling you to focus on a reduced set of trace results.

For subscriber usernames that have the expected form of **user@domain**, you can filter on the user, the domain, or both. You can use an asterisk (*) as a wildcard to substitute for characters at the beginning or end of either term to match a greater number of subscribers.



NOTE: You cannot filter results using a wildcard in the middle of the user or domain terms. For example, the following uses of the wildcard are not supported: tom*25@example.com, tom125@ex*.com.

When you enable filtering by username, traces that have insufficient information to determine the username are automatically excluded.

To configure subscriber filtering:

- Specify the filter.

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

Consider the following examples of using the wildcard for filtering:

- Filter results for the specific subscriber with the username, tom@example.com.

```
[edit system processes general-authentication-service traceoptions]
user@host# set filter user tom@example.com
```

- Filter results for all subscribers whose username begins with tom.

```
[edit system processes general-authentication-service traceoptions]
user@host# set filter user tom*
```

- Filter results for all subscribers whose username ends with tom.

```
[edit system processes general-authentication-service traceoptions]
user@host# set filter user *tom
```

- Filter results for subscribers with the username tom at all domains beginning with ex.

```
[edit system processes general-authentication-service traceoptions]
user@host# set filter user tom@ex*
```

- Filter results for all subscribers at all domains that end with ample.com.

```
[edit system processes general-authentication-service traceoptions]
user@host# set filter user *ample.com
```

- Filter results for all subscribers whose username begins with tom at domains that end with example.com.

```
[edit system processes general-authentication-service traceoptions]
user@host# set filter user tom*.*example.com
```

Configuring the Trace Operation

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

Flag	Description
address-assignment	Trace all address-assignment pool events

Flag	Description
all	Trace all tracing operations
configuration	Trace configuration events
framework	Trace authentication framework events
gx-plus	Trace Gx-Plus events
jsrc	Trace JSRC events
ldap	Trace LDAP authentication events
local-authentication	Trace local authentication events
radius	Trace RADIUS authentication events
user-access	Trace user access events, such as login, logout, and authenticate

To configure the flags for the event to be logged:

- Configure the flags.

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

Configuring the General Authentication Service Processes Trace Log Filename

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

To configure the filename for general authentication service tracing operations:

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

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

Related Documentation

- [Tracing General Authentication Service Processes on page 559](#)
- [Configuring Address-Assignment Pools on page 316](#)

Configuring the Trace Operation

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

Flag	Description
address-assignment	Trace all address-assignment pool events
all	Trace all tracing operations
configuration	Trace configuration events
framework	Trace authentication framework events
gx-plus	Trace Gx-Plus events
jsrc	Trace JSRC events
ldap	Trace LDAP authentication events
local-authentication	Trace local authentication events
radius	Trace RADIUS authentication events
user-access	Trace user access events, such as login, logout, and authenticate

To configure the flags for the event to be logged:

- Configure the flags.

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

Related Documentation

- [Tracing General Authentication Service Processes on page 559](#)

Configuring Subscriber Filtering for General Authentication Service Trace Operations

You can apply filters to the general authentication service to limit tracing to particular subscribers or domains. Subscriber filtering simplifies troubleshooting in a scaled environment by enabling you to focus on a reduced set of trace results.

For subscriber usernames that have the expected form of **user@domain**, you can filter on the user, the domain, or both. You can use an asterisk (*) as a wildcard to substitute for characters at the beginning or end of either term to match a greater number of subscribers.



NOTE: You cannot filter results using a wildcard in the middle of the user or domain terms. For example, the following uses of the wildcard are not supported: tom*25@example.com, tom125@ex*.com.

When you enable filtering by username, traces that have insufficient information to determine the username are automatically excluded.

To configure subscriber filtering:

- Specify the filter.

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

Consider the following examples of using the wildcard for filtering:

- Filter results for the specific subscriber with the username, tom@example.com.

```
[edit system processes general-authentication-service traceoptions]
user@host# set filter user tom@example.com
```

- Filter results for all subscribers whose username begins with tom.

```
[edit system processes general-authentication-service traceoptions]
user@host# set filter user tom*
```

- Filter results for all subscribers whose username ends with tom.

```
[edit system processes general-authentication-service traceoptions]
user@host# set filter user *tom
```

- Filter results for subscribers with the username tom at all domains beginning with ex.

```
[edit system processes general-authentication-service traceoptions]
user@host# set filter user tom@ex*
```

- Filter results for all subscribers at all domains that end with ample.com.

```
[edit system processes general-authentication-service traceoptions]
user@host# set filter user *ample.com
```

- Filter results for all subscribers whose username begins with tom at domains that end with example.com.

```
[edit system processes general-authentication-service traceoptions]
user@host# set filter user tom*.*example.com
```

Related Documentation

- [Tracing General Authentication Service Processes on page 559](#)

CHAPTER 73

Configuring Static Subscriber Interfaces Log Files

- [Configuring the Number and Size of Static Subscribers Log Files on page 567](#)
- [Configuring Access to the Static Subscribers Log File on page 568](#)
- [Configuring a Regular Expression for Static Subscriber Messages to Be Logged on page 568](#)
- [Configuring the Severity Level to Filter Which Static Subscriber Messages Are Logged on page 568](#)

Configuring the Number and Size of Static Subscribers Log Files

You can optionally specify the number of compressed, archived trace log files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB); the default size is 128 kilobytes (KB).

The archived files are differentiated by a suffix in the format *.number.gz*. The newest archived file is *.0.gz* and the oldest archived file is *.(maximum number)-1.gz*. When the current trace log file reaches the maximum size, it is compressed and renamed, and any existing archived files are renamed. This process repeats until the maximum number of archived files is reached, at which point the oldest file is overwritten.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation, *filename*, reaches 2 MB, *filename* is compressed and renamed *filename.0.gz*, and a new file called *filename* is created. When the new *filename* reaches 2 MB, *filename.0.gz* is renamed *filename.1.gz* and *filename* is compressed and renamed *filename.0.gz*. This process repeats until there are 20 trace files. Then the oldest file, *filename.19.gz*, is simply overwritten when the next oldest file, *filename.18.gz* is compressed and renamed to *filename.19.gz*.

To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output.

```
[edit system processes static-subscribers traceoptions]  
user@host# set file stat-subs_1_logfile_1 files 20 size 2097152
```

- Related Documentation**
- [Tracing Static Subscriber Operations on page 571](#)

Configuring Access to the Static Subscribers Log File

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

To specify that all users can read the log file:

- Configure the log file to be world-readable.

```
[edit system processes static-subscribers traceoptions]  
user@host# set file stat-subs_1_logfile_1 world-readable
```

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

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

```
[edit system processes static-subscribers traceoptions]  
user@host# set file stat-subs_1_logfile_1 no-world-readable
```

- Related Documentation**
- [Tracing Static Subscriber Operations on page 571](#)

Configuring a Regular Expression for Static Subscriber Messages to Be Logged

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

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

To configure regular expressions to be matched:

- Configure the regular expression.

```
[edit system processes static-subscribers traceoptions]  
user@host# set file stat-subs_1_logfile match regex
```

- Related Documentation**
- [Tracing Static Subscriber Operations on page 571](#)

Configuring the Severity Level to Filter Which Static Subscriber Messages Are Logged

The messages associated with a logged event are categorized according to severity level. You can use the severity level to determine which messages are logged for the event type. The severity level that you configure depends on the issue that you are trying to resolve. In some cases you might be interested in seeing all messages relevant to the logged event, so you specify **all** or **verbose**. Either choice generates a large amount of output. You can specify a more restrictive severity level, such as **notice** or **info** to filter the

messages . By default, the trace operation output includes only messages with a severity level of **error**.

To configure the type of messages to be logged:

- Configure the message severity level.

```
[edit system processes static-subscribers traceoptions]  
user@host# set level severity
```

Related Documentation

- [Tracing Static Subscriber Operations on page 571](#)

Configuring Static Subscriber Interfaces Trace Flags and Operations

- [Tracing Static Subscriber Operations on page 571](#)
- [Configuring the Static Subscribers Trace Log Filename on page 572](#)
- [Configuring the Static Subscribers Tracing Flags on page 572](#)

Tracing Static Subscriber Operations

The Junos OS trace feature tracks static subscriber operations and records events in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

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

1. Important events are logged in a file located in the `/var/log` directory. By default, the router uses the filename `jsscd`. You can specify a different filename, but you cannot change the directory in which trace files are located.
2. When the trace log file *filename* reaches 128 kilobytes (KB), it is compressed and renamed *filename.0.gz*. Subsequent events are logged in a new file called *filename*, until it reaches capacity again. At this point, *filename.0.gz* is renamed *filename.1.gz* and *filename* is compressed and renamed *filename.0.gz*. This process repeats until the number of archived files reaches the maximum file number. Then the oldest trace file—the one with the highest number—is overwritten.

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

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

To configure static subscriber tracing operations:

1. (Optional) Configure a trace log filename.
See [“Configuring the Static Subscribers Trace Log Filename”](#) on page 572.
2. (Optional) Configure the number and size of trace logs.
See [“Configuring the Number and Size of Static Subscribers Log Files”](#) on page 567.
3. (Optional) Configure user access to trace logs.
See [“Configuring Access to the Static Subscribers Log File”](#) on page 568.
4. (Optional) Configure a regular expression to filter the information to be included in the trace log.
See [“Configuring a Regular Expression for Static Subscriber Messages to Be Logged”](#) on page 568.
5. (Optional) Configure flags to specify which events are logged.
See [“Configuring the Static Subscribers Tracing Flags”](#) on page 572.
6. (Optional) Configure a severity level for messages to specify which event messages are logged.
See [“Configuring the Severity Level to Filter Which Static Subscriber Messages Are Logged”](#) on page 568.

Configuring the Static Subscribers Trace Log Filename

By default, the name of the file that records trace output for static subscribers is **jsscd**. You can specify a different name with the **file** option.

To configure the filename for static subscribers tracing operations:

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

```
[edit system processes static-subscribers traceoptions]  
user@host# set file stat-subs_1
```

Related Documentation • [Tracing Static Subscriber Operations on page 571](#)

Configuring the Static Subscribers Tracing Flags

By default, only important events are logged. You can specify which events and operations are logged by specifying one or more tracing flags.

To configure the flags for the events to be logged:

- Configure the flags.

```
[edit system processes static-subscribers traceoptions]  
user@host# set flag authentication
```


Related Documentation • [Tracing Static Subscriber Operations on page 571](#)

Configuring PTSP Tracing Operations

- [Tracing Packet-Triggered Subscriber Operations on page 575](#)
- [Configuring a Statistics Profile for PTSP on page 577](#)
- [Tracing PTSP Operations on page 579](#)

Tracing Packet-Triggered Subscriber Operations

Packet-triggered subscriber tracing operations track packet-triggered subscriber operations and record them in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

All log files are located in the `/var/log` directory. You cannot change the directory (`/var/log`) in which trace files are located. When the trace file reaches its maximum size, a `.0` is appended to the filename, then a new file is created with a `.1`, and finally a `.2`. When the maximum number of trace files is reached, the oldest trace file is overwritten.

To configure packet-triggered subscriber tracing operations:

1. Specify that you want to configure tracing options.

```
[edit system services packet-triggered-subscribers]
user@host# edit traceoptions
```

2. (Optional) Configure the name for the file used for the trace output.
3. (Optional) Configure the number and size of the log files.
4. (Optional) Configure flags to filter the operations to be logged.

The packet-triggered subscriber traceoptions operations are described in the following sections:

- [Configuring the Packet-Triggered Subscribers Trace Log Filename on page 576](#)
- [Configuring the Size of Packet-Triggered Subscribers Log Files on page 576](#)
- [Configuring the Packet-Triggered Subscribers Tracing Flags on page 576](#)

Configuring the Packet-Triggered Subscribers Trace Log Filename

By default, the name of the file that records trace output for packet-triggered subscribers is **jptspd**. You can specify a different name with the **file** option.

To configure the filename for packet-triggered subscribers tracing operations:

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

```
[edit system services packet-triggered-subscribers traceoptions]  
user@host# set file ptsp-subsys_1
```

Configuring the Size of Packet-Triggered Subscribers Log Files

You can optionally specify the number of compressed, archived trace log files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB); the default size is 128 kilobytes (KB).

The archived files are differentiated by a suffix in the format **.number.gz**. The newest archived file is **.0.gz** and the oldest archived file is **.(maximum number)-1.gz**. When the current trace log file reaches the maximum size, it is compressed and renamed, and any existing archived files are renamed. This process repeats until the maximum number of archived files is reached, at which point the oldest file is overwritten.

For example, you can set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracing operation, **filename**, reaches 2 MB, **filename** is compressed and renamed **filename.0.gz**, and a new file called **filename** is created. When the new **filename** reaches 2 MB, **filename.0.gz** is renamed **filename.1.gz** and **filename** is compressed and renamed **filename.0.gz**. This process repeats until there are 20 trace files. Then the oldest file, **filename.19.gz**, is simply overwritten when the next oldest file, **filename.18.gz** is compressed and renamed to **filename.19.gz**.

To configure the size of trace files:

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

```
[edit system services packet-triggered-subscribers traceoptions]  
user@host# set file ptsp-subsys_1_logfile_1 size 2097152
```

Configuring the Packet-Triggered Subscribers Tracing Flags

To configure the flags for the events to be logged:

- Configure the flags.

```
[edit system services packet-triggered-subscribers traceoptions]  
user@host# set flag peer  
user@host# set flag session
```

**Related
Documentation**

- [Configuring the PTSP Application on page 486](#)

Configuring a Statistics Profile for PTSP

The local policy decision function (L-PDF) enables you to configure properties for statistics output by creating a statistics profile. The statistics profile configures the files to which statistics records are exported and the format that is exported. You configure the statistics profile so that the statistics records are exported to a flat file. Flat files contain statistics that are collected for each subscriber by application or application group. The statistics in a flat file are not transmitted to the external policy manager using Diameter.

To configure a statistics profile for PTSP:

1. Specify that you want to configure a statistics profile.

```
[edit system services local-policy-decision-function]
user@host# edit statistics
```

2. Configure the file properties used for the trace output.
3. Configure the profile properties.
4. Specify the record type.

Tasks to configure a statistics profile for PTSP are:

- [Configuring the File Properties for Statistics Data Output on page 577](#)
- [Configuring the Profile Properties for Statistics Data Output on page 578](#)
- [Configuring the Record Type for Statistics Data on page 578](#)

Configuring the File Properties for Statistics Data Output

You configure a file to which the statistics data output is exported in a specified format.

To configure the file properties:

1. Specify the unique filename for receiving statistics data output.

```
[edit system services local-policy-decision-function statistics]
user@host# edit file ptsp
```

2. (Optional) Specify the maximum number of files that are maintained at one time and the maximum size of each file. If you configure one of these options, you also must set the other option.

```
[edit system services local-policy-decision-function statistics file ptsp]
user@host# set files 10 size 1g
```

3. Specify the interval for transferring files to archive sites.

```
[edit system services local-policy-decision-function statistics file ptsp]
user@host# set transfer-interval 60
```

4. Specify one or more URLs for archiving the files. Archiving can be done by using FTP or SCP.

```
[edit system services local-policy-decision-function statistics file ptsp]
user@host# set archive-sites "ftp://anonymous@10.227.1.114"
```

Configuring the Profile Properties for Statistics Data Output

You can create an ACL statistics profile, which configures the statistics to collect and write to a file in the `/var/stats/acl` directory.

To configure the profile properties:

1. Specify the name of the profile.

```
[edit system services local-policy-decision-function statistics]
user@host# edit acl-statistics-profile ptsp
```

2. (Optional) Specify the file in the `/var/stats/acl` directory in which statistics are collected. Enclose the name within quotation marks.

```
[edit system services local-policy-decision-function statistics acl-statistics-profile
ptsp]
user@host# set file "pstp"
```

3. Set the interval for reporting statistics.

```
[edit system services local-policy-decision-function statistics acl-statistics-profile
ptsp]
user@host# set report-interval 5
```

4. Set the **interim-active-only** mode for reporting statistics. This mode reports only statistics that have changed in the past report interval.

```
[edit system services local-policy-decision-function statistics acl-statistics-profile
ptsp]
user@host# set record-mode interim-active-only
```

5. Specify the statistics to be collected in the log file.

```
[edit system services local-policy-decision-function statistics acl-statistics-profile
ptsp]
user@host# set acl-fields all-fields
```

Configuring the Record Type for Statistics Data

You must configure the interim record type for recording the ACL statistics.

To configure the record type:

- Specify interim as the record type.

```
[edit system services local-policy-decision-function statistics]
user@host# set record-type interim
```

Related Documentation

- [Tracing PTSP Operations on page 579](#)
- [Configuring PTSP on page 486](#)

Tracing PTSP Operations

Tracing operations track L-PDF operations and record them in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

By default, no events are traced. When you enable the tracing operation, the default tracing behavior is as follows:

1. Important events are logged in a file located in the `/var/log` directory. By default, the router uses the filename, `ptspd`. You can specify a different filename, but you cannot change the directory in which trace files are located.
2. When the trace log file *filename* reaches 128 kilobytes (KB), it is compressed and renamed *filename.0.gz*. Subsequent events are logged in a new file called *filename*, until it reaches capacity again. At this point, *filename.0.gz* is renamed *filename.1.gz* and *filename* is compressed and renamed *filename.0.gz*. This process repeats until the number of archived files reaches the maximum file number. Then the oldest trace file—the one with the highest number—is overwritten.

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

To customize trace file settings:

1. Specify that you want to configure tracing options.

```
[edit system services local-policy-decision-function]
user@host# edit traceoptions
```
2. Configure the filename used for the trace output.

```
[edit system services local-policy-decision-function traceoptions]
user@host# set file lpdfd
```
3. (Optional) Configure the maximum number and size of the log files. If you configure one of these options, you also must set the other option.

```
[edit system services local-policy-decision-function traceoptions]
user@host# set files 10 size 1g
```
4. (Optional) Specify flags to filter the operations to be logged. To specify more than one flag, include multiple **flag** statements.

```
[edit system services local-policy-decision-function traceoptions]
user@host# set flag ptsp-statistics
```

The following table describes the flags that you can include.

Flag	Description
configuration	Trace configuration events
database	Trace database events

Flag	Description
general	Trace general flow
ptsp-statistics	Trace PTSP events
rtsock	Trace routing socket events
statistics	Trace statistics events
subscriber	Trace subscriber events

- Related Documentation**
- [Configuring a Statistics Profile for PTSP on page 577](#)
 - [Configuring PTSP on page 486](#)

Overriding PCRF Session Control to Troubleshoot a Session or Services

- [Disabling PCRF Control of a Subscriber Session on page 581](#)

Disabling PCRF Control of a Subscriber Session

When a subscriber has been provisioned with Gx-Plus, services for that subscriber can be activated and deactivated only by the PCRF. Accordingly, AAA rejects any RADIUS CoA requests for subscribers provisioned by Gx-Plus. Similarly, CLI-based service activation and deactivation do not work while a subscriber is remotely provisioned.

Network administrators without PCRF access or authority may need to override PCRF control on a particular subscriber session to troubleshoot the session or correct the subscriber services. You can disable PCRF control by issuing the **request network-access aaa subscriber set session-id** command. In response, the router sends a termination notice to the PCRF, but does not actually log out the subscriber.

When you have confirmed that provisioning is disabled, you can then activate or deactivate subscriber services for that session with the **request network-access aaa subscriber add session-id** and **request network-access aaa subscriber delete session-id** commands, respectively. These commands fail if provisioning is still enabled.

Another consequence of disabling provisioning for a subscriber session is that RADIUS change of authorization (CoA) messages can modify the session.

Before you begin, determine or verify the ID for the session by displaying the session IDs of all current subscribers with the **show subscribers detail** or **show network-access aaa subscribers** command.

To disable control by the PCRF over a subscriber session:

1. Disable provisioning for the specified subscriber session ID.

```
user@host> request network-access aaa subscriber set session-id subscriber-session-id  
provisioning-state none
```

2. (Optional) Verify that provisioning is disabled for the session.

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

For example, to disable provisioning for subscriber larry:

```
user@host> show network-access aaa subscribers
Username      Logical system/Routing instance  Client type  Session-ID
...
larry         default:default                  dhcp         55
...

user@host> request network-access aaa subscriber set session-id 55 provisioning-state none
user@host> show network-access aaa subscribers session-id 55 detail
Type: dhcp
Username: larry@isp5.net
Stripped username: larry
AAA Logical system/Routing instance: default:default
Target Logical system/Routing instance: default:retail-onlinecompany-ca
Access-profile:retailer-onlinecompany-sjc
Session ID: 55
Accounting Session ID: 55
Multi Accounting Session ID: 0
IP Address: 192.168.44.104
Authentication State: AuthStateActive
Accounting State: Acc-Start-Send
Provisioning-type: none
Service name: basic-service
Service State: SvcActive
Session ID: 56
Session uptime: 00:01:45
```

Related Documentation • [Activating and Deactivating Subscriber Services Locally with the CLI on page 332](#)

CHAPTER 77

Contacting Juniper Technical Support

- [Collecting Subscriber Access Logs Before Contacting Juniper Networks Technical Support on page 583](#)
- [Compressing Troubleshooting Logs from /var/logs to Send to Juniper Networks Technical Support on page 585](#)

Collecting Subscriber Access Logs Before Contacting Juniper Networks Technical Support

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

Solution To collect standard troubleshooting information:

- Redirect the command output to a file.

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

To configure logging to assist Juniper Networks Technical Support:

1. Review the following blocks of statements to determine which apply to your configuration.

[edit]

```
set system syslog archive size 100m files 25
set system auto-configuration traceoptions file filename
set system auto-configuration traceoptions file filename size 100m files 25
set protocols ppp-service traceoptions file filename size 100m files 25
set protocols ppp-service traceoptions level all
set protocols ppp-service traceoptions flag all
set protocols ppp traceoptions file filename size 100m files 25
set protocols ppp traceoptions level all
set protocols ppp traceoptions flag all
set protocols ppp monitor-session all
set interfaces pp0 traceoptions flag all
set demux traceoptions file filename size 100m files 25
set demux traceoptions level all
set demux traceoptions flag all
set system processes dhcp-service traceoptions file filename
set system processes dhcp-service traceoptions file size 100m
set system processes dhcp-service traceoptions file files 25
set system processes dhcp-service traceoptions flag all
set class-of-service traceoptions file filename
set class-of-service traceoptions file size 100m
set class-of-service traceoptions flag all
set class-of-service traceoptions file files 25
set routing-options traceoptions file filename
set routing-options traceoptions file size 100m
set routing-options traceoptions flag all
set routing-options traceoptions file files 25
set interfaces traceoptions file filename
set interfaces traceoptions file size 100m
set interfaces traceoptions flag all
set interfaces traceoptions file files 25
set system processes general-authentication-service traceoptions file filename
set system processes general-authentication-service traceoptions file size 100m
set system processes general-authentication-service traceoptions flag all
set system processes general-authentication-service traceoptions file files 25
```

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



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



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

**Related
Documentation**

- [Compressing Troubleshooting Logs from /var/logs to Send to Juniper Networks Technical Support on page 585](#)

Compressing Troubleshooting Logs from /var/logs to Send to Juniper Networks Technical Support

Problem **Description:** You have collected logs on your device and need to send them to Juniper Networks Technical Support. This topic shows you how to compress the logs into a single file for each Routing Engine to more conveniently send the logs.

Solution You can compress all the log files in the **/var/log** directories of the master and backup (if present) Routing Engines into a single **tgz** file for each Routing Engine, which enables you to send the logs to JTAC in a convenient package. You can use either the CLI or the command shell to perform these tasks; because of its ease of use, only the CLI version is shown here.

1. Access the device through the management IP address or console, typically on the master Routing Engine, RE0.

```
user@host>
```

2. Archive and compress all the log files on RE0 and put them in **/var/tmp**.

```
user@host> file archive compress source /var/log/* destination /var/tmp/re0.tgz
/usr/bin/tar: Removing leading '/' from member names
```

3. Confirm that the compressed archive file has been created.

```
user@host> file list /var/tmp
baseline-config.conf
gres-tp
idp_license_info
install
jinstall-12.2-20120328.0-domestic-signed.tgz
krt_gencfg_filter.txt
preinstall_boot_loader.conf
re0.tgz
rtsdb
sec-download
vi.recover
```

On devices with a single Routing Engine, skip to Step 10.

4. Log in to the backup Routing Engine, RE1, and access the CLI.



NOTE: **1** is appended to the hostname in the prompt to signify that you are on RE1.

```
user@host> request routing-engine login backup
% cli
user@host11>
```

5. Archive and compress all the log files on RE1 and put them in **/var/tmp**.

```
user@host1> file archive compress source /var/log/* destination /var/tmp/re1.tgz
/usr/bin/tar: Removing leading '/' from member names
```

6. Confirm that the compressed archive file has been created.

```
user@host1> file list /var/tmp
baseline-config.conf
gres-tp
idp_license_info
install
jinstall-12.2-20120328.0-domestic-signed.tgz
krt_gencfg_filter.txt
preinstall_boot_loader.conf
re1.tgz
rtsdb
sec-download
vi.recover
%
```

7. Exit the remote login to the backup Routing Engine to return to the master Routing Engine. Note that the previously appended *1* is removed from the hostname in the prompt to signify that you are back on RE0.

```
user@host1> exit
rlogin: connection closed
```

```
user@host1>
```

8. Copy the compressed archive file from RE1 to RE0.

```
user@host> file copy re1:/var/tmp/re1.tgz /var/tmp
```

9. Confirm the presence of the copied file.

```
user@host> file list /var/tmp
baseline-config.conf
gres-tp
idp_license_info
install
jinstall-12.2-20120328.0-domestic-signed.tgz
krt_gencfg_filter.txt
preinstall_boot_loader.conf
re0.tgz
re1.tgz
rtsdb
sec-download
vi.recover
%
```

10. Copy the files directly from the master Routing Engine to any local host using FTP, SCP, JWEB, or (on some devices) a mounted USB.

Related Documentation

- [Collecting Subscriber Access Logs Before Contacting Juniper Networks Technical Support on page 583](#)

PART 10

Configuration Statements and Operational Commands

- [Configuration Statements on page 589](#)
- [Operational Commands on page 997](#)

CHAPTER 78

Configuration Statements

- [\[edit access address-assignment\] Hierarchy Level on page 600](#)
- [\[edit access domain\] Hierarchy Level on page 601](#)
- [\[edit access gx-plus\] Hierarchy Level on page 601](#)
- [\[edit access profile\] Hierarchy Level on page 602](#)
- [\[edit diameter\] Hierarchy Level on page 604](#)
- [\[edit dynamic-profiles\] Hierarchy Level on page 605](#)
- [\[edit forwarding-options dhcp-relay\] Hierarchy Level on page 612](#)
- [\[edit interfaces radius-options\] Hierarchy Level on page 616](#)
- [\[edit jsrc\] Hierarchy Level on page 616](#)
- [\[edit protocols ancp\] Hierarchy Level on page 616](#)
- [\[edit system services dhcp-local-server\] Hierarchy Level on page 617](#)
- [\[edit system services packet-triggered-subscribers\] Hierarchy Level on page 621](#)
- [\[edit system services static-subscribers\] Hierarchy Level on page 621](#)
- [\[edit system services subscriber-management\] Hierarchy Level on page 622](#)
- [aaa-logical-system \(Domain Map\) on page 623](#)
- [aaa-routing-instance \(Domain Map\) on page 624](#)
- [abated-utilization \(Address-Assignment Pools\) on page 625](#)
- [abated-utilization-v6 \(Address-Assignment Pools\) on page 625](#)
- [access-identifier on page 626](#)
- [access-loop-id-local on page 626](#)
- [access-profile \(Domain Map\) on page 627](#)
- [access-profile \(Static Subscribers\) on page 628](#)
- [access-profile-name \(Duplicate Accounting\) on page 629](#)
- [accounting \(Access Profile\) on page 630](#)
- [accounting-backup-options \(Access Profile\) on page 631](#)
- [accounting-order \(Service Accounting\) on page 631](#)
- [accounting-port on page 632](#)
- [accounting-retry \(RADIUS\) on page 633](#)

- [accounting-server](#) on page 633
- [accounting-session-id-format](#) on page 634
- [accounting-stop-on-access-deny](#) on page 634
- [accounting-stop-on-failure](#) on page 635
- [accounting-timeout \(RADIUS\)](#) on page 635
- [active-server-group](#) on page 636
- [address \(Diameter Peer\)](#) on page 637
- [address \(Diameter Transport\)](#) on page 637
- [address-assignment \(Address-Assignment Pools\)](#) on page 638
- [address-pool \(Domain Map\)](#) on page 639
- [adjacency-timer](#) on page 639
- [advisory-options \(Traffic Shaping\)](#) on page 640
- [aggregate-clients \(DHCP Relay Agent\)](#) on page 641
- [aggregate-clients \(Static Subscribers\)](#) on page 642
- [always-write-giaddr](#) on page 643
- [always-write-option-82](#) on page 644
- [ancp](#) on page 645
- [ancp-speed-change-immediate-update \(ANCP\)](#) on page 646
- [application-group-any](#) on page 646
- [application-groups](#) on page 647
- [applications \(Services PTSP\)](#) on page 647
- [attempts \(DHCP Local Server\)](#) on page 648
- [attributes](#) on page 649
- [authentication \(DHCP Local Server\)](#) on page 650
- [authentication \(DHCP Relay Agent\)](#) on page 651
- [authentication \(Static Subscribers\)](#) on page 652
- [authentication-order](#) on page 653
- [authentication-server](#) on page 654
- [authorization-order](#) on page 654
- [autonomous \(Dynamic Router Advertisement\)](#) on page 655
- [boot-file](#) on page 655
- [boot-server](#) on page 656
- [calling-station-id-delimiter \(Subscriber Management\)](#) on page 656
- [calling-station-id-format \(Subscriber Management\)](#) on page 657
- [circuit-id \(Address-Assignment Pools\)](#) on page 658
- [circuit-type \(DHCP Local Server\)](#) on page 659
- [circuit-type \(DHCP Relay Agent\)](#) on page 660

- [clear-on-abort \(DHCP Local Server\) on page 661](#)
- [client-accounting-algorithm on page 662](#)
- [client-authentication-algorithm on page 662](#)
- [client-discover-match \(DHCP Local Server\) on page 663](#)
- [client-discover-match \(DHCP Relay Agent\) on page 664](#)
- [client-id \(DHCP Local Server\) on page 665](#)
- [client-id \(DHCP Relay Agent\) on page 666](#)
- [client-idle-timeout on page 666](#)
- [client-session-timeout on page 667](#)
- [coa-dynamic-variable-validation on page 668](#)
- [coa-immediate-update on page 668](#)
- [coa-no-override service-class-attribute on page 669](#)
- [concurrent-data-sessions on page 669](#)
- [connect-actively on page 670](#)
- [count-type on page 671](#)
- [current-hop-limit \(Dynamic Router Advertisement\) on page 672](#)
- [database-replication \(Subscriber Session Database\) on page 672](#)
- [default-action \(DHCP Relay Agent Option\) on page 673](#)
- [default-lifetime \(Dynamic Router Advertisement\) on page 674](#)
- [delay-authentication \(DHCP Relay Agent\) on page 674](#)
- [delegated-pool \(DHCP Local Server\) on page 675](#)
- [delimiter \(DHCP Local Server\) on page 676](#)
- [delimiter \(Domain Map\) on page 677](#)
- [delimiter \(DHCP Relay Agent\) on page 678](#)
- [demux on page 679](#)
- [destination \(Diameter Network Element\) on page 679](#)
- [destination-host on page 680](#)
- [destination-host \(Gx-Plus\) on page 680](#)
- [destination-host \(PTSP\) on page 681](#)
- [destination-realm \(JSRC\) on page 681](#)
- [destination-realm \(Gx-Plus\) on page 682](#)
- [destination-realm \(PTSP\) on page 682](#)
- [dhcp-attributes \(Address-Assignment Pools\) on page 683](#)
- [dhcp-local-server on page 684](#)
- [dhcp-relay on page 689](#)
- [dhcipv6 \(DHCP Local Server\) on page 695](#)
- [dhcipv6 \(DHCP Relay Agent\) on page 698](#)

- [diameter on page 701](#)
- [diameter-instance \(JSRC\) on page 702](#)
- [diameter-instance \(Gx-Plus\) on page 702](#)
- [diameter-instance \(PTSP\) on page 703](#)
- [disable on page 703](#)
- [disable-relay on page 704](#)
- [dns-server on page 704](#)
- [domain \(Domain Map\) on page 705](#)
- [domain-name \(DHCP Local Server\) on page 706](#)
- [domain-name \(DHCP Relay Agent\) on page 708](#)
- [domain-name \(Address-Assignment Pools\) on page 709](#)
- [domain-name \(Static Subscribers\) on page 710](#)
- [domain-name-server \(Routing Instances and Access Profiles\) on page 711](#)
- [domain-name-server-inet \(Routing Instances and Access Profiles\) on page 712](#)
- [domain-name-server-inet6 \(Routing Instances and Access Profiles\) on page 713](#)
- [downstream-rate \(Traffic Shaping\) on page 714](#)
- [drop \(DHCP Relay Agent Option\) on page 715](#)
- [duplication \(Access Profile\) on page 715](#)
- [duplication-vrf \(Duplicate Accounting\) on page 716](#)
- [dynamic-profile \(DHCP Local Server\) on page 717](#)
- [dynamic-profile \(DHCP Relay Agent\) on page 718](#)
- [dynamic-profile \(Domain Map\) on page 719](#)
- [dynamic-profile \(Static Subscribers\) on page 720](#)
- [enable on page 721](#)
- [equals \(DHCP Relay Agent\) on page 722](#)
- [ethernet-port-type-virtual on page 723](#)
- [exceed-action on page 723](#)
- [exclude \(RADIUS\) on page 724](#)
- [external-authority on page 728](#)
- [family \(Address-Assignment Pools\) on page 729](#)
- [forward-only \(DHCP Relay Agent Option\) on page 730](#)
- [forward-rule \(Configuring\) on page 731](#)
- [forward-rule \(Including in Rule\) on page 732](#)
- [forwarding \(Diameter Network Element\) on page 732](#)
- [from \(Forward Rule\) on page 733](#)
- [from \(Rule\) on page 734](#)
- [function \(Diameter Network Element\) on page 735](#)

- [function \(Diameter Route\) on page 736](#)
- [global \(Gx-Plus\) on page 736](#)
- [grace-period on page 737](#)
- [group \(DHCP Local Server\) on page 738](#)
- [group \(DHCP Relay Agent\) on page 741](#)
- [group \(Static Subscribers\) on page 744](#)
- [gsmp-syn-timeout \(ANCP\) on page 745](#)
- [gsmp-syn-wait \(ANCP\) on page 746](#)
- [gx-plus \(Gx-Plus\) on page 747](#)
- [hardware-address on page 747](#)
- [high-utilization \(Address-Assignment Pools\) on page 748](#)
- [high-utilization-v6 \(Address-Assignment Pools\) on page 748](#)
- [host \(Address-Assignment Pools\) on page 749](#)
- [host \(Diameter Origin\) on page 749](#)
- [ietf-mode on page 750](#)
- [ignore on page 751](#)
- [immediate-update on page 752](#)
- [include-ipv6 \(Gx-Plus\) on page 752](#)
- [include-irb-and-l2 on page 753](#)
- [interface \(DHCP Local Server\) on page 755](#)
- [interface \(DHCP Relay Agent\) on page 757](#)
- [interface \(Dynamic Router Advertisement\) on page 759](#)
- [interface \(Static Subscriber Group\) on page 760](#)
- [interface \(Static Subscriber Username\) on page 761](#)
- [interface-client-limit \(DHCP Local Server\) on page 762](#)
- [interface-client-limit \(DHCP Relay Agent\) on page 764](#)
- [interface-delete \(Subscriber Management or DHCP Client Management\) on page 765](#)
- [interface-delete \(Subscriber Management or DHCP Client Management\) on page 766](#)
- [interface-description-format on page 766](#)
- [interface-name \(DHCP Local Server\) on page 767](#)
- [interface-name \(DHCP Relay Agent\) on page 768](#)
- [interface-set \(ANCP\) on page 769](#)
- [interface-traceoptions \(DHCP\) on page 770](#)
- [interfaces \(ANCP\) on page 772](#)
- [ip-address on page 772](#)
- [ip-address-first on page 773](#)
- [jsrc \(JSRC\) on page 774](#)

- [jsrc-partition](#) on page 774
- [juniper-dsl-attributes](#) on page 775
- [layer2-unicast-replies](#) on page 776
- [lease-time-threshold](#) (DHCP Local Server and DHCP Relay Agent) on page 777
- [lease-time-validation](#) (DHCP Local Server and DHCP Relay Agent) on page 778
- [limit](#) on page 778
- [link](#) (Address-Assignment Pools) on page 779
- [local-address](#) on page 780
- [local-address-range](#) on page 781
- [local-port-range](#) on page 781
- [local-ports](#) on page 782
- [local-prefix-list](#) on page 782
- [local-server-group](#) (DHCP Relay Agent Option) on page 783
- [logical-system](#) (Diameter Peer) on page 784
- [logical-system](#) (Diameter Transport) on page 785
- [logical-system-name](#) (Static Subscribers) on page 786
- [logical-system-name](#) (DHCP Local Server) on page 787
- [logical-system-name](#) (DHCP Relay Agent) on page 788
- [ltv-syslog-interval](#) (System Process) on page 789
- [mac-address](#) (DHCP Local Server) on page 790
- [mac-address](#) (DHCP Relay Agent) on page 791
- [maintain-subscriber](#) (Subscriber Management) on page 792
- [managed-configuration](#) (Dynamic Router Advertisement) on page 793
- [map](#) (Domain Map) on page 794
- [mask](#) (Domain Map) on page 795
- [match-direction](#) (Services PTSP) on page 795
- [max-advertisement-interval](#) (Dynamic Router Advertisement) on page 796
- [max-data-sessions-per-subscriber](#) on page 796
- [max-outstanding-requests](#) on page 797
- [max-outstanding-requests](#) (Gx-Plus) on page 798
- [max-pending-accounting-stops](#) (Access Profile) on page 798
- [max-withhold-time](#) (Access Profile) on page 799
- [maximum-discovery-table-entries](#) on page 799
- [maximum-helper-restart-time](#) on page 800
- [maximum-lease-time](#) on page 800
- [metric](#) (Diameter Route) on page 801
- [metric](#) (Domain Map) on page 801

- [min-advertisement-interval \(Dynamic Router Advertisement\)](#) on page 802
- [multi-address-embedded-option-response \(DHCP Local Server\)](#) on page 803
- [name-server](#) on page 803
- [nas-identifier](#) on page 804
- [nas-port-extended-format \(Access Profile\)](#) on page 805
- [nas-port-extended-format \(Interfaces\)](#) on page 807
- [nas-port-id-delimiter \(Subscriber Management\)](#) on page 808
- [nas-port-id-format \(Subscriber Management\)](#) on page 809
- [nas-port-options \(RADIUS Options\)](#) on page 810
- [nas-port-type \(Subscriber Management\)](#) on page 811
- [nas-port-type \(RADIUS Options\)](#) on page 813
- [neighbor \(Define ANCP\)](#) on page 814
- [neighbor-discovery-router-advertisement \(Address-Assignment Pools\)](#) on page 815
- [netbios-node-type](#) on page 815
- [network](#) on page 816
- [network-element \(Diameter Base Protocol\)](#) on page 817
- [no-bind-on-request \(DHCP Relay Agent\)](#) on page 818
- [on-link \(Dynamic Router Advertisement\)](#) on page 819
- [no-vlan-interface-name](#) on page 820
- [option](#) on page 822
- [option-60 \(DHCP Local Server\)](#) on page 823
- [option-60 \(DHCP Relay Agent\)](#) on page 824
- [option-82 \(DHCP Relay Agent\)](#) on page 825
- [option-82 \(DHCP Local Server Authentication\)](#) on page 826
- [option-82 \(DHCP Local Server Pool Matching\)](#) on page 827
- [option-82 \(Address-Assignment Pools\)](#) on page 828
- [option-match](#) on page 828
- [option-number \(DHCP Relay Agent Option\)](#) on page 829
- [options \(Access Profile\)](#) on page 830
- [order](#) on page 831
- [origin \(Diameter Base Protocol\)](#) on page 832
- [other-stateful-configuration \(Dynamic Router Advertisement\)](#) on page 832
- [overhead-accounting \(ANCP\)](#) on page 833
- [overrides \(DHCP Local Server\)](#) on page 834
- [overrides \(DHCP Relay Agent\)](#) on page 836
- [packet-triggered-subscribers](#) on page 837
- [packet-triggered-subscribers-partition](#) on page 838

- [padn \(Domain Map\) on page 838](#)
- [parse-direction \(Domain Map\) on page 839](#)
- [parse-order \(Domain Map\) on page 840](#)
- [partition on page 841](#)
- [partition \(Gx-Plus\) on page 841](#)
- [partition \(PTSP\) on page 842](#)
- [password \(Static Subscribers\) on page 843](#)
- [password \(DHCP Local Server\) on page 844](#)
- [password \(DHCP Relay Agent\) on page 845](#)
- [peer \(Diameter Base Protocol\) on page 846](#)
- [peer \(Diameter Network Element\) on page 846](#)
- [pool \(Address-Assignment Pools\) on page 847](#)
- [pool \(DHCP Local Server Overrides\) on page 848](#)
- [pool-match-order on page 849](#)
- [port on page 850](#)
- [port \(Diameter Peer\) on page 850](#)
- [pre-ietf-mode on page 851](#)
- [preauthentication-order \(Access Profile\) on page 851](#)
- [preauthentication-server \(Access Profile\) on page 852](#)
- [preferred-lifetime \(Address-Assignment Pools\) on page 853](#)
- [preferred-lifetime \(Dynamic Router Advertisement\) on page 854](#)
- [prefix \(DHCP Relay Agent\) on page 855](#)
- [prefix \(Address-Assignment Pools\) on page 856](#)
- [prefix \(Dynamic Router Advertisement\) on page 856](#)
- [priority \(Diameter Peer\) on page 857](#)
- [profile \(Access\) on page 858](#)
- [process-inform on page 862](#)
- [protocol on page 863](#)
- [protocols \(Dynamic Profiles\) on page 864](#)
- [provisioning-order on page 866](#)
- [proxy-mode on page 867](#)
- [qos-adjust on page 868](#)
- [qos-adjust-adsl on page 868](#)
- [qos-adjust-adsl2 on page 869](#)
- [qos-adjust-adsl2-plus on page 869](#)
- [qos-adjust-sdsl on page 870](#)
- [qos-adjust-vdsl on page 870](#)

- [qos-adjust-vds2](#) on page 871
- [radius \(Access Profile\)](#) on page 872
- [radius-disconnect \(DHCP Local Server\)](#) on page 874
- [radius-options \(Edit Access\)](#) on page 875
- [radius-options \(Interfaces\)](#) on page 876
- [radius-server](#) on page 877
- [range \(Address-Assignment Pools\)](#) on page 878
- [rapid-commit \(DHCPv6 Local Server\)](#) on page 879
- [reachable-time \(Dynamic Router Advertisement\)](#) on page 880
- [realm \(Diameter Origin\)](#) on page 880
- [realm-delimiter \(Domain Map\)](#) on page 881
- [realm-parse-direction \(Domain Map\)](#) on page 881
- [reconfigure \(DHCP Local Server\)](#) on page 882
- [relay-agent-interface-id \(DHCP Local Server\)](#) on page 883
- [relay-agent-interface-id \(DHCPv6 Relay Agent\)](#) on page 884
- [relay-agent-interface-id \(DHCPv6 Relay Agent Username\)](#) on page 885
- [relay-agent-remote-id \(DHCP Local Server\)](#) on page 886
- [relay-agent-remote-id \(DHCPv6 Relay Agent Username\)](#) on page 887
- [relay-agent-remote-id \(DHCPv6 Relay Agent\)](#) on page 888
- [relay-agent-subscriber-id \(DHCP Local Server\)](#) on page 889
- [relay-agent-subscriber-id \(DHCPv6 Relay Agent\)](#) on page 890
- [relay-option \(DHCP Relay Agent\)](#) on page 891
- [relay-option-82](#) on page 892
- [relay-server-group \(DHCP Relay Agent Option\)](#) on page 893
- [remote-address](#) on page 894
- [remote-address-range](#) on page 895
- [remote-id](#) on page 895
- [remote-id \(DHCP Relay Agent\)](#) on page 896
- [remote-port-range](#) on page 898
- [remote-ports](#) on page 898
- [remote-prefix-list](#) on page 899
- [replace-ip-source-with](#) on page 900
- [report-interface-descriptions \(Edit Access\)](#) on page 901
- [request network-access aaa replay pending-accounting-stops](#)
- [request network-access aaa subscriber add session-id](#)
- [request network-access aaa subscriber delete session-id](#)
- [request network-access aaa subscriber modify session-id](#)

- [request-rate](#) on page 908
- [requested-ip-network-match](#) (DHCP Local Server) on page 909
- [retransmit-timer](#) (Dynamic Router Advertisement) on page 910
- [retry](#) on page 910
- [revert-interval](#) on page 911
- [route](#) (Diameter Network Element) on page 912
- [router](#) (Address-Assignment Pools) on page 912
- [router-advertisement](#) (Dynamic Profiles) on page 913
- [routing-instance](#) on page 913
- [routing-instance](#) (Diameter Peer) on page 914
- [routing-instance](#) (Diameter Transport) on page 914
- [routing-instance-name](#) (Static Subscribers) on page 915
- [routing-instance-name](#) (DHCP Relay Agent) on page 916
- [routing-instance-name](#) (DHCP Local Server) on page 917
- [rule](#) (Configuring) on page 918
- [rule](#) (Including in Rule Set) on page 919
- [rule-set](#) (Services PTSP) on page 919
- [secret](#) on page 920
- [send-acct-status-on-config-change](#) (Access Profile) on page 921
- [send-release-on-delete](#) (DHCP Relay Agent) on page 922
- [server-group](#) on page 923
- [server-identifier](#) (Address-Assignment Pools) on page 924
- [server-response-time](#) (DHCP Relay Agent) on page 924
- [service](#) (Service Accounting) on page 925
- [service-profile](#) (DHCP Local Server) on page 926
- [service-profile](#) (DHCP Relay Agent) on page 927
- [services](#) (PTSP) on page 928
- [session-options](#) on page 928
- [sip-server-address](#) on page 929
- [sip-server-domain-name](#) on page 929
- [source-address](#) on page 930
- [stacked-vlan-ranges](#) (RADIUS Options) on page 931
- [starts-with](#) (DHCP Relay Agent Option) on page 932
- [static-subscribers](#) on page 933
- [statistics](#) (Access Profile) on page 934
- [strict](#) (DHCP Local Server) on page 935
- [strip-domain](#) (Domain Map) on page 936

- [subscriber-identification \(PTSP\) on page 937](#)
- [subscriber-packet-idle-timeout on page 938](#)
- [subscriber-management \(Subscriber Management\) on page 939](#)
- [subscriber-profile on page 940](#)
- [t1-percentage \(Address-Assignment Pools\) on page 941](#)
- [t2-percentage \(Address-Assignment Pools\) on page 942](#)
- [target-logical-system \(Domain Map\) on page 943](#)
- [target-routing-instance \(Domain Map\) on page 944](#)
- [term \(Forward Rule\) on page 945](#)
- [term \(Rule\) on page 946](#)
- [terminate-code on page 947](#)
- [tftp-server on page 948](#)
- [then \(Forward Rule\) on page 948](#)
- [then \(Rule\) on page 949](#)
- [timeout \(RADIUS\) on page 950](#)
- [timeout \(DHCP Local Server\) on page 951](#)
- [token \(DHCP Local Server\) on page 952](#)
- [trace \(DHCP Local Server\) on page 953](#)
- [traceoptions \(ANCP\) on page 954](#)
- [traceoptions \(Diameter Base Protocol\) on page 956](#)
- [traceoptions \(DHCP\) on page 958](#)
- [traceoptions \(General Authentication Service\) on page 961](#)
- [traceoptions \(PTSP\) on page 963](#)
- [traceoptions \(Static Subscribers\) on page 965](#)
- [traceoptions \(Subscriber Management\) on page 967](#)
- [traceoptions \(Subscriber Session Database Replication\) on page 969](#)
- [transport \(Diameter Base Protocol\) on page 970](#)
- [transport \(Diameter Peer\) on page 971](#)
- [trigger \(DHCP Local Server\) on page 972](#)
- [trust-option-82 on page 973](#)
- [tunnel-profile \(Domain Map\) on page 974](#)
- [underlying-interface \(ANCP\) on page 974](#)
- [update-interval on page 975](#)
- [upstream-rate \(Traffic Shaping\) on page 976](#)
- [use-interface-description on page 977](#)
- [use-option-82 on page 979](#)
- [use-primary \(DHCP Relay Agent\) on page 980](#)

- [use-vlan-id](#) on page 982
- [user-prefix \(DHCP Relay Agent\)](#) on page 984
- [user-prefix \(Static Subscribers\)](#) on page 985
- [user-prefix \(DHCP Local Server\)](#) on page 986
- [username-include \(Static Subscribers\)](#) on page 987
- [username-include \(DHCP Local Server\)](#) on page 988
- [username-include \(DHCP Relay Agent\)](#) on page 989
- [valid-lifetime \(Dynamic Router Advertisement\)](#) on page 990
- [valid-lifetime \(Address-Assignment Pools\)](#) on page 991
- [violation-action \(DHCP Local Server and DHCP Relay Agent\)](#) on page 992
- [vlan-nas-port-stacked-format](#) on page 993
- [vlan-ranges \(RADIUS Options\)](#) on page 994
- [vrf-name \(Duplicate Accounting\)](#) on page 995
- [wait-for-acct-on-ack \(Access Profile\)](#) on page 995
- [wins-server \(Access\)](#) on page 996

[edit access address-assignment] Hierarchy Level

```
access {
  address-assignment {
    abated-utilization percentage;
    abated-utilization-v6 percentage;
    high-utilization percentage;
    high-utilization-v6 percentage;
    neighbor-discovery-router-advertisement ndra-pool-name;
    pool pool-name {
      family family {
        dhcp-attributes {
          [protocol-specific attributes]
        }
        host hostname {
          hardware-address mac-address;
          ip-address ip-address;
        }
        network ip-prefix /<prefix-length>;
        prefix ipv6-prefix;
        range range-name {
          high upper-limit;
          low lower-limit;
          prefix-length prefix-length;
        }
      }
    }
  }
  link pool-name;
}
```

- Related Documentation**
- [Address-Assignment Pools Overview on page 315](#)
 - [Configuring Address-Assignment Pools on page 316](#)

[edit access domain] Hierarchy Level

```
access {
  domain {
    delimiter [delimiter-character];
    map domain-map-name {
      aaa-logical-system logical-system-name {
        aaa-routing-instance routing-instance-name;
      }
      aaa-routing-instance routing-instance-name;
      access-profile profile-name;
      address-pool pool-name;
      dynamic-profile profile-name;
      padn destination-address {
        mask destination-mask;
        metric route-metric;
      }
      strip-domain;
      target-logical-system logical-system-name {
        target-routing-instance routing-instance-name;
      }
      target-routing-instance routing-instance-name;
      tunnel-profile profile-name;
    }
    parse-direction (left-to-right | right-to-left);
    parse-order (domain | realm);
    realm-delimiter [delimiter-character];
    realm-parse-direction (left-to-right | right-to-left);
  }
}
```

- Related Documentation**
- [Domain Mapping Overview on page 128](#)
 - [Configuring a Domain Map on page 131](#)

[edit access gx-plus] Hierarchy Level

```
access {
  gx-plus {
    global {
      include-ipv6;
      max-outstanding-requests number;
    }
    partition partition-name {
      diameter-instance instance-name;
      destination-host hostname;
      destination-realm realm;
    }
  }
}
```

```
}
```

- Related Documentation**
- [Gx-Plus for Provisioning Subscribers Overview on page 439](#)
 - [Configuring Gx-Plus on page 446](#)

[edit access profile] Hierarchy Level

```
access {
  profile profile-name {
    accounting {
      accounting-stop-on-access-deny;
      accounting-stop-on-failure;
      address-change-immediate-update;
      ancp-speed-change-immediate-update;
      coa-immediate-update;
      coa-no-override service-class-attribute;
      duplication;
      duplication-vrf {
        access-profile-name profile-name;
        vrf-name vrf-name;
      }
      immediate-update;
      order [ accounting-method ];
      statistics (time | volume-time);
      update-interval minutes;
      wait-for-acct-on-ack;
    }
    authentication-order [ authentication-methods ];
    authorization-order jsrc;
    client client-name {
      ...
    }
    domain-name-server;
    domain-name-server-inet;
    domain-name-server-inet6;
    provisioning-order (gx-plus | jsrc);
    radius {
      accounting-server [ ip-address ];
      attributes {
        exclude {
          ...
        }
        ignore {
          framed-ip-netmask;
          input-filter;
          logical-system-routing-instance;
          output-filter;
        }
      }
    }
    authentication-server [ ip-address ];
    options {
      accounting-session-id-format (decimal | description);
      calling-station-id-delimiter delimiter-character;
      calling-station-id-format {
```

```

    agent-circuit-id;
    agent-remote-id;
    interface-description;
    nas-identifier;
}
client-accounting-algorithm (detail | round-robin);
client-authentication-algorithm(detail | round-robin);
coa-dynamic-variable-validation;
ethernet-port-type-virtual;
interface-description-format {
    exclude-adapter;
    exclude-sub-interface;
}
nas-identifier identifier-value;
nas-port-extended-format {
    adapter-width width;
    ae-width width;
    port-width width;
    slot-width width;
    stacked-vlan-width width;
    vlan-width width;
    atm {
        adapter-width width;
        port-width width;
        slot-width width;
        vci-width width;
        vpi-width width;
    }
}
nas-port-id-delimiter delimiter-character;
nas-port-id-format {
    agent-circuit-id;
    agent-remote-id;
    interface-description;
    nas-identifier;
}
nas-port-type {
    ethernet {
        port-type;
    }
}
revert-interval interval;
vlan-nas-port-stacked-format;
}
}
radius-server server-address {
    accounting-port port-number;
    accounting-retry number;
    accounting-timeout seconds;
    port port-number;
    retry attempts;
    routing-instance routing-instance-name;
    secret password;
    max-outstanding-requests value;
    source-address source-address;
    timeout seconds;
}

```

```
    }
    service {
        accounting-order (activation-protocol | radius);
    }
    session-options {
        client-idle-timeout minutes;
        client-session-timeout minutes;
    }
}
}
```

Related Documentation

- [AAA Service Framework Overview on page 3](#)

[edit diameter] Hierarchy Level

```
diameter {
    network-element element-name {
        forwarding {
            route dne-route-name {
                destination realm realm-name <host hostname>;
                function function-name <partition partition-name>;
                metric route-metric;
            }
        }
        function function-name;
        peer peer-name {
            priority priority-number;
        }
    }
    origin {
        host hostname;
        realm realm-name;
    }
    peer peer-name {
        address ip-address;
        connect-actively {
            port port-number;
            transport transport-name;
        }
        logical-system logical-system-name <routing-instance routing-instance-name >;
        routing-instance routing-instance-name;
    }
    transport transport-name {
        address;
        logical-system logical-system-name <routing-instance routing-instance-name>;
        routing-instance routing-instance-name;
    }
}
```

Related Documentation

- [Diameter Base Protocol Overview on page 419](#)
- [Configuring Diameter on page 434](#)

[edit dynamic-profiles] Hierarchy Level

```

dynamic-profiles {
  profile-name {
    class-of-service {
      interfaces {
        interface-name {
          unit logical-unit-number {
            classifiers {
              type (classifier-name | default);
            }
            output-traffic-control-profile (profile-name | $junos-cos-traffic-control-profile);
            rewrite-rules {
              dscp (rewrite-name | default);
              dscp-ipv6 (rewrite-name | default);
              ieee-802.1 (rewrite-name | default) vlan-tag (outer | outer-and-inner);
              inet-precedence (rewrite-name | default);
            }
          }
        }
      }
    }
  }
  scheduler-maps {
    map-name {
      forwarding-class class-name scheduler scheduler-name;
    }
  }
  schedulers {
    (scheduler-name) {
      buffer-size (percent percentage | remainder | temporal microseconds |
        $junos-cos-scheduler-bs);
      drop-profile-map loss-priority (any | low | medium-low | medium-high | high)
        protocol (any | non-tcp | tcp) drop-profile (profile-name | predefined-variable);
      excess-priority (low | high | $junos-cos-scheduler-excess-priority);
      excess-rate (percent percentage | percent $junos-cos-scheduler-excess-rate);
      overhead-accounting (shaping-mode) <bytes (byte-value)>;
      priority (priority-level | $junos-cos-scheduler-priority);
      shaping-rate (rate | predefined-variable);
      transmit-rate (rate | percent percentage | remainder | percent percentage
        $junos-cos-scheduler-tx) <exact | rate-limit>;
    }
  }
  traffic-control-profiles profile-name {
    delay-buffer-rate (percent percentage | rate);
    excess-rate (percent percentage | proportion value | percent
      $junos-cos-excess-rate);
    guaranteed-rate (percent percentage | rate);
    overhead-accounting (shaping-mode) <bytes (byte-value)>;
    scheduler-map map-name;
    shaping-rate (percent percentage | rate | predefined-variable);
  }
}
firewall {
  family family {

```

```
fast-update-filter filter-name {
  interface-specific;
  match-order [match-order];
  term term-name {
    from {
      match-conditions;
    }
    then {
      action;
      action-modifiers;
    }
    only-at-create;
  }
  filter filter-name {
    interface-specific;
    term term-name {
      from {
        match-conditions;
      }
      then {
        action;
        action-modifiers;
      }
    }
  }
}
policer policer-name {
  filter-specific;
  if-exceeding {
    (bandwidth-limit bps | bandwidth-percent percentage);
    burst-size-limit bytes;
  }
  logical-bandwidth-policer;
  logical-interface-policer;
  physical-interface-policer;
  then {
    policer-action;
  }
}
hierarchical-policer policer-name {
  aggregate {
    if-exceeding {
      bandwidth-limit-limit bps;
      burst-size-limit bytes;
    }
    then {
      policer-action;
    }
  }
  premium {
    if-exceeding {
      bandwidth-limit bps;
      burst-size-limit bytes;
    }
    then {
      policer-action;
    }
  }
}
```

```

three-color-policer policer-name {
  action {
    loss-priority high then discard;
  }
  logical-interface-policer;
  single-rate {
    (color-aware | color-blind);
    committed-burst-size bytes;
    committed-information-rate bps;
    excess-burst-size bytes;
  }
  two-rate {
    (color-aware | color-blind);
    committed-burst-size bytes;
    committed-information-rate bps;
    peak-burst-size bytes;
    peak-information-rate bps;
  }
}
}
}
policy-options {
  prefix-listname {
    ip-addresses;
    dynamic-db;
  }
}
}
interfaces {
  interface-name {
    unit logical-unit-number {
      family family {
        access-concentrator name;
        address address;
        direct-connect;
        duplicate-protection;
        dynamic-profile profile-name;
        filter {
          adf {
            counter;
            input-precedence precedence;
            not-mandatory;
            output-precedence precedence;
            rule rule-value;
          }
          input filter-name {
            precedence precedence;
            shared-name filter-shared-name;
          }
          output filter-name {
            precedence precedence;
            shared-name filter-shared-name;
          }
        }
      }
      max-sessions number;
      max-sessions-vs-a-ignore;
      rpf-check {

```

```

        fail-filter filter-name;
        mode loose;
    }
    service {
        input {
            service-set service-set-name {
                service-filter filter-name;
            }
            post-service-filter filter-name;
        }
        output {
            service-set service-set-name {
                service-filter filter-name;
            }
        }
    }
    service-name-table table-name;
    short-cycle-protection <lockout-time-min minimum-seconds lockout-time-max
        maximum-seconds>;
    unnumbered-address interface-name <preferred-source-address address>;
}
ppp-options {
    chap;
    pap;
}
vlan-id number;
}
vlan-tagging;
}
interface-set interface-set-name {
    interface interface-name {
        unit logical-unit-number;
    }
}
}
demux0 {
    unit logical-unit-number {
        demux-options {
            underlying-interface interface-name
        }
        demux-source {
            source-prefix;
        }
        family family {
            access-concentrator name;
            address address;
            direct-connect;
            duplicate-protection;
            dynamic-profile profile-name;
            filter {
                input filter-name;
                output filter-name;
            }
            mac-validate (loose | strict):
            max-sessions number;
            max-sessions-vsa-ignore;
            service-name-table table-name;

```

```

        short-cycle-protection <lockout-time-min minimum-seconds lockout-time-max
            maximum-seconds>;
        unnumbered-address interface-name <preferred-source-address address>;
    }
}
}
pp0 {
    unit logical-unit-number {
        keepalives interval seconds;
        no-keepalives;
        pppoe-options {
            underlying-interface interface-name;
            server;
        }
        ppp-options {
            authentication [ authentication-protocols ];
            chap {
                challenge-length minimum minimum-length maximum maximum-length;
            }
            pap;
        }
    }
    family inet {
        unnumbered-address interface-name;
        address address;
        service {
            input {
                service-set service-set-name {
                    service-filter filter-name;
                }
                post-service-filter filter-name;
            }
            output {
                service-set service-set-name {
                    service-filter filter-name;
                }
            }
        }
        filter {
            input filter-name {
                precedence precedence;
            }
            output filter-name {
                precedence precedence;
            }
        }
    }
}
}
}
protocols {
    igmp {
        interface interface-name {
            accounting;
            disable;
            group-policy;
            immediate-leave

```

```

no-accounting;
promiscuous-mode;
ssm-map ssm-map-name;
static {
    group group {
        source source;
    }
}
version version;
}
mld {
    interface interface-name {
        disable;
        (accounting | no-accounting);
        group-policy;
        immediate-leave;
        oif-map;
        passive;
        ssm-map ssm-map-name;
        static {
            group multicast-group-address {
                exclude;
                group-count number;
                group-increment increment;
                source ip-address {
                    source-count number;
                    source-increment increment;
                }
            }
        }
        version version;
    }
}
}
router-advertisement {
    interface interface-name {
        current-hop-limit number;
        default-lifetime seconds;
        (managed-configuration | no-managed-configuration);
        max-advertisement-interval seconds;
        min-advertisement-interval seconds;
        (other-stateful-configuration | no-other-stateful-configuration);
        prefix prefix {
            (autonomous | no-autonomous);
            (on-link | no-on-link);
            preferred-lifetime seconds;
            valid-lifetime seconds;
        }
        reachable-time milliseconds;
        retransmit-timer milliseconds;
    }
}
}
}
}
routing-instances routing-instance-name {
    interface interface-name;

```

```

routing-options {
  access {
    route prefix {
      next-hop next-hop;
      metric route-cost;
      preference route-distance;
      tag route-tag;
    }
  }
  access-internal {
    route subscriber-ip-address {
      qualified-next-hop underlying-interface {
        mac-address address;
      }
    }
  }
  multicast {
    interface interface-name {
      no-qos-adjust;
    }
  }
}
rib routing-table-name {
  access {
    route prefix {
      next-hop next-hop;
      metric route-cost;
      preference route-distance;
      tag route-tag;
    }
  }
  access-internal {
    route subscriber-ip-address {
      qualified-next-hop underlying-interface {
        mac-address address;
      }
    }
  }
}
}
routing-options {
  access {
    route prefix {
      next-hop next-hop;
      metric route-cost;
      preference route-distance;
      tag route-tag;
    }
  }
  access-internal {
    route subscriber-ip-address {
      qualified-next-hop underlying-interface {
        mac-address address;
      }
    }
  }
}

```

```
multicast {
  interface interface-name {
    no-qos-adjust;
  }
}
variables {
  variable-name {
    default-value default-value;
    equals expression;
    mandatory;
    uid;
    uid-reference;
  }
}
```

**Related
Documentation**

- *Dynamic Profiles Overview*
- *CoS for Subscriber Access Overview*
- *Configuring a Basic Dynamic Profile*
- *Configuring Static Hierarchical Scheduling and Queuing in a Dynamic Profile for Subscriber Access*
- *Two-Color Policer Configuration Overview*
- *Three-Color Policer Configuration Overview*
- *Hierarchical Policer Configuration Overview*
- *Guidelines for Applying Traffic Policers*

[edit forwarding-options dhcp-relay] Hierarchy Level

```
forwarding-options {
  dhcp-relay {
    active-server-group server-group-name;
    authentication {
      password password-string;
      username-include {
        circuit-type;
        delimiter delimiter-character;
        domain-name domain-name-string;
        interface-name;
        logical-system-name;
        mac-address;
        option-60;
        option-82 <circuit-id> <remote-id>;
        routing-instance-name;
        user-prefix user-prefix-string;
      }
    }
  }
  dhcpv6 {
    active-server-group server-group-name;
  }
}
```



```

authentication {
  password password-string;
  username-include {
    circuit-type;
    client-id;
    delimiter delimiter-character;
    domain-name domain-name-string;
    interface-name;
    logical-system-name;
    relay-agent-interface-id;
    relay-agent-remote-id;
    relay-agent-subscriber-id;
    routing-instance-name;
    user-prefix user-prefix-string;
  }
}
dynamic-profile profile-name {
  aggregate-clients (merge | replace);
  use-primary primary-profile-name;
}
group group-name {
  active-server-group server-group-name;
  authentication {
    ...
  }
  dynamic-profile profile-name {
    ...
  }
  interface interface-name {
    exclude;
    overrides {
      ...
    }
    relay-option {
      ...
    }
    service-profile dynamic-profile-name;
    trace;
    upto upto-interface-name;
  }
  route-suppression;
  service-profile dynamic-profile-name;
}
overrides {
  ...
}
relay-agent-interface-id {
  ...
}
relay-option {
  ...
}
server-group {
  server-group-name {
    server-ip-address;
  }
}

```

```

    }
  }
  route-suppression;
  service-profile dynamic-profile-name;
  overrides {
    allow-snooped-clients;
    delay-authentication;
    interface-client-limit number;
    no-allow-snooped-clients;
    no-bind-on-request;
    send-release-on-delete;
  }
  relay-agent-interface-id {
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82;
  }
  server-group {
    server-group-name {
      server-ip-address;
    }
  }
}
duplicate-clients-in-subnet (incoming-interface | option-82);
dynamic-profile profile-name {
  aggregate-clients (merge | replace);
  use-primary primary-profile-name;
}
forward-snooped-clients (all-interfaces | configured-interfaces |
  non-configured-interfaces);
group group-name {
  active-server-group server-group-name;
  authentication {
    ...
  }
  dynamic-profile profile-name {
    ...
  }
  interface interface-name {
    exclude;
    overrides {
      ...
    }
    service-profile dynamic-profile-name;
    trace;
    upto upto-interface-name;
  }
  overrides {
    ...
  }
  relay-option {
    ...
  }
  relay-option-82 {
    ...
  }
}

```

```

route-suppression;
server-response-time seconds;
service-profile dynamic-profile-name;
}
overrides {
allow-snooped-clients;
always-write-giaddr;
always-write-option-82;
client-discover-match (option60-and-option82 | incoming-interface);
delay-authentication;
disable-relay;
interface-client-limit number;
layer2-unicast-replies;
no-allow-snooped-clients;
no-bind-on-request;
proxy-mode;
replace-ip-source-with;
send-release-on-delete;
trust-option-82;
}
relay-option {
option-number option-number;
default-action {
drop;
forward-only;
local-server-group local-server-group;
relay-server-group relay-server-group;
}
equals (ascii ascii-string | hexadecimal hexadecimal-string) {
drop;
forward-only;
local-server-group local-server-group;
relay-server-group relay-server-group;
}
starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
drop;
forward-only;
local-server-group local-server-group;
relay-server-group relay-server-group;
}
}
}
relay-option-82 {
circuit-id {
prefix prefix;
use-interface-description (logical | device);
}
}
server-group {
server-group-name {
server-ip-address;
}
}
}
route-suppression;
server-response-time seconds;
service-profile dynamic-profile-name;
}

```

```
}
```

**Related
Documentation**

- [Extended DHCP Relay Agent Overview on page 194](#)

[edit interfaces radius-options] Hierarchy Level

```
interfaces interface-name {  
  radius-options {  
    nas-port-options nas-port-options-name {  
      nas-port-extended-format {  
        adapter-width width;  
        ae-width width;  
        port-width width;  
        slot-width width;  
        stacked;  
        stacked-vlan-width width;  
        vci-width width;  
        vlan-width width;  
        vpi-width width;  
      }  
      nas-port-type port-type;  
      stacked-vlan-ranges (any | low-outer-tag-high-outer-tag),any;  
      vlan-ranges (any | low-tag-high-tag);  
    }  
  }  
}
```

**Related
Documentation**

- [RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN Overview on page 60](#)
- [Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 63](#)

[edit jsrc] Hierarchy Level

```
jsrc {  
  partition partition-name {  
    diameter-instance instance-name;  
    destination-host hostname;  
    destination-realm realm-name;  
  }  
}
```

**Related
Documentation**

- [Juniper Networks Session and Resource Control \(SRC\) and JSRC Overview on page 451](#)
- [Configuring JSRC on page 455](#)

[edit protocols ancp] Hierarchy Level

```
protocols {  
  ancp {  
    adjacency-timer seconds;
```

```

gsmp-syn-timeout seconds;
gsmp-syn-wait;
interfaces {
  interface-set interface-set-name {
    access-identifier identifier-string;
    underlying-interface underlying-interface-name;
  }
  interface-name {
    access-identifier identifier-string;
  }
}
maximum-discovery-table-entries entry-number;
maximum-helper-restart-time;
neighbor ip-address {
  adjacency-timer;
  ietf-mode;
  maximum-discovery-table-entries entry-number;
  pre-ietf-mode;
}
pre-ietf-mode;
qos-adjust;
qos-adjust-adsl adjustment-factor;
qos-adjust-adsl2 adjustment-factor;
qos-adjust-adsl2-plus adjustment-factor;
qos-adjust-sdsl adjustment-factor;
qos-adjust-vdsl adjustment-factor;
qos-adjust-vdsl2 adjustment-factor;
traceoptions {
  file filename <files number> <match regular-expression > <size maximum-file-size>
    <world-readable | no-world-readable>;
  flag flag;
  level (all | error | info | notice | verbose | warning);
  no-remote-trace;
}
}
}

```

- Related Documentation**
- [ANCP and the ANCP Agent Overview on page 351](#)
 - [Configuring the ANCP Agent on page 368](#)

[edit system services dhcp-local-server] Hierarchy Level

```

system {
  services {
    dhcp-local-server {
      authentication {
        password password-string;
        username-include {
          circuit-type;
          delimiter delimiter-character;
          domain-name domain-name-string;
          interface-name;
          logical-system-name;
          mac-address;

```

```
option-60;
option-82 <circuit-id> <remote-id>;
routing-instance-name;
user-prefix user-prefix-string;
}
}
dhcpv6 {
  authentication {
    password password-string;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name-string;
      interface-name;
      logical-system-name;
      relay-agent-interface-id;
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
}
group group-name {
  authentication {
    password password-string;
    username-include {
      circuit-type;
      client-id;
      delimiter delimiter-character;
      domain-name domain-name-string;
      interface-name;
      logical-system-name;
      relay-agent-interface-id;
      relay-agent-remote-id;
      relay-agent-subscriber-id;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
}
interface interface-name {
  exclude;
  overrides {
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
      pool pool-name;
    }
    rapid-commit;
  }
  service-profile dynamic-profile-name;
  trace;
  upto upto-interface-name;
}
overrides {
  delegated-pool;
```

```

    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
        pool pool-name;
    }
    rapid-commit;
}
reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    timeout timeout-value;
    token token-value;
    trigger {
        radius-disconnect;
    }
}
route-suppression;
service-profile dynamic-profile-name;
}
overrides {
    delegated-pool;
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
        pool pool-name;
    }
    rapid-commit;
}
reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    timeout timeout-value;
    token token-value;
    trigger {
        radius-disconnect;
    }
}
route-suppression;
service-profile dynamic-profile-name;
}
duplicate-clients-in-subnet (incoming-interface | option-82);
dynamic-profile profile-name (aggregate-clients (merge | replace) | use-primary
    primary-profile-name);
forward-snooped-clients (all-interfaces | configured-interfaces |
    non-configured-interfaces);
group group-name {
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
            domain-name domain-name-string;
            interface-name;
            logical-system-name;
        }
    }
}

```

```
    mac-address;
    option-60;
    option-82 <circuit-id> <remote-id>;
    overrides;
    routing-instance-name;
    user-prefix user-prefix-string;
  }
}
dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
primary-profile-name>;
interface interface-name {
  exclude;
  overrides {
    client-discover-match (option60-and-option82 | incoming-interface);
    interface-client-limit number;
    process-inform {
      pool pool-name;
    }
  }
  service-profile dynamic-profile-name;
  trace;
  upto upto-interface-name;
}
overrides {
  client-discover-match (option60-and-option82 | incoming-interface);
  interface-client-limit number;
  process-inform {
    pool pool-name;
  }
}
reconfigure {
  attempts attempt-count;
  clear-on-abort;
  timeout timeout-value;
  token token-value;
  trigger {
    radius-disconnect;
  }
}
requested-ip-network-match subnet-mask;
route-suppression;
service-profile dynamic-profile-name;
}
overrides {
  client-discover-match (option60-and-option82 | incoming-interface);
  interface-client-limit number;
  process-inform {
    pool pool-name;
  }
}
service-profile dynamic-profile-name;
pool-match-order {
  external-authority;
  ip-address-first;
  option-82;
```



```

    }
    reconfigure {
        attempts attempt-count;
        clear-on-abort;
        timeout timeout-value;
        token token-value;
        trigger {
            radius-disconnect;
        }
    }
}
}
}
requested-ip-network-match subnet-mask;
route-suppression;
service-profile dynamic-profile-name;
}

```

Related Documentation • [Extended DHCP Local Server Overview on page 188](#)

[\[edit system services packet-triggered-subscribers\] Hierarchy Level](#)

```

system {
  services {
    packet-triggered-subscribers {
      subscriber-packet-idle-timeout subscriber-packet-idle-timeout
      partition partition-name {
        destination-host hostname;
        destination-realm realm;
        diameter-instance instance-name;
      }
      traceoptions {
        file filename <files number> <match regular-expression> <size maximum-file-size>
          <world-readable | no-world-readable>;
        flag flag;
        no-remote-trace;
      }
    }
  }
}

```

Related Documentation • [Configuring the PTSP Application on page 486](#)

[\[edit system services static-subscribers\] Hierarchy Level](#)

```

system {
  services {
    static-subscribers {
      access-profile profile-name;
      authentication {
        password password-string;
        username-include {
          domain-name domain-name;
        }
        interface;
      }
    }
  }
}

```

```

        logical-system-name;
        routing-instance-name;
        user-prefix user-prefix-string;
    }
}
dynamic-profile profile-name {
    aggregate-clients (merge | replace);
}
group group-name {
    access-profile profile-name;
    authentication {
        password password-string;
        username-include {
            domain-name domain-name;
            interface;
            logical-system-name;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
}
dynamic-profile profile-name {
    aggregate-clients (merge | replace);
}
interface interface-name <exclude> <upto upto-interface-name>;
}
traceoptions {
    file filename <files number> <match regular-expression> <size maximum-file-size>
        <world-readable | no-world-readable>;
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
}
}
}
}

```

- Related Documentation
- [Subscribers on Static Interfaces Overview on page 463](#)
 - [Configuring Subscribers over Static Interfaces on page 466](#)

[edit system services subscriber-management] Hierarchy Level

```

system {
    services {
        subscriber-management {
            enforce-strict-scale-limit-license;
            gres-route-flush-delay;
            maintain-subscriber {
                interface-delete;
            }
        }
        traceoptions {
            file <filename> <files number> <match regular-expression> <size
                maximum-file-size> <world-readable | no-world-readable>;
            flag flag;
        }
    }
}

```

```

    }
  }
}

```

- Related Documentation**
- [Subscriber Binding Retention During Interface Delete Events on page 237](#)
 - [Configuring the Router to Strictly Enforce the Subscriber Scaling License](#)
 - [Delaying Removal of Access Routes and Access-Internal Routes After Graceful Routing Engine Switchover](#)

aaa-logical-system (Domain Map)

Syntax `aaa-logical-system logical-system-name {
 aaa-routing-instance routing-instance-name;
 }`

Hierarchy Level [edit access domain [map](#) *domain-map-name*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure a non-default logical system in which the **authd** daemon sends AAA requests for the domain map.



NOTE: Subscriber management is supported in the default logical system only. The `aaa-logical-system` statement is for future extensions of subscriber management and is not supported in current Junos OS releases.

Default Default logical system for the subscriber.

Options *logical-system-name*—Name of the logical system.

The remaining statement is explained separately.

Required Privilege Level admin—To view this statement in the configuration.
 admin-control—To add this statement to the configuration.

- Related Documentation**
- [Specifying an AAA Logical System/Routing Instance in a Domain Map on page 134](#)

aaa-routing-instance (Domain Map)

Syntax	aaa-routing-instance (<i>routing-instance-name</i> default);
Hierarchy Level	[edit access domain map <i>domain-map-name</i>], [edit access domain map <i>domain-map-name</i> aaa-logical-system <i>logical-system-name</i>]
Release Information	Statement introduced in Junos OS Release 10.4. Option default introduced in Junos OS Release 13.3.
Description	Configure the routing instance in which the authd daemon sends AAA requests for the domain map.



NOTE: Subscriber management is supported in the default logical system only.

Default	Routing instance used for the subscriber context.
Options	<i>routing-instance-name</i> —Name of the routing instance. default —The default (master) routing instance.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding Domain Maps and Logical System/Routing Instance Contexts on page 130• Specifying an AAA Logical System/Routing Instance in a Domain Map on page 134

abated-utilization (Address-Assignment Pools)

Syntax	<code>abated-utilization <i>percentage</i>;</code>
Hierarchy Level	[edit access address-assignment], [edit routing-instances <i>routing-instance-name</i> address-assignment]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	Generate SNMP traps for DHCP address pools or linked set of address pools. No SNMP traps are generated unless a value is configured.
Default	Abated utilization is not set. Delete the abated-utilization value to unset.
Options	<i>percentage</i> —Threshold below which an SNMP trap clear is generated. Range: 1 through 98
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Address-Assignment Pools Overview on page 315 • Configuring Address-Assignment Pool Usage Threshold Traps on page 320

abated-utilization-v6 (Address-Assignment Pools)

Syntax	<code>abated-utilization-v6 <i>percentage</i>;</code>
Hierarchy Level	[edit access address-assignment], [edit routing-instances <i>routing-instance-name</i> address-assignment]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	Generate SNMP traps for DHCPv6 address pools or linked set of address pools. No SNMP traps are generated unless a value is configured.
Default	Abated utilization is not set. Delete the abated-utilization value to unset.
Options	<i>percentage</i> —Threshold below which an SNMP trap clear is generated. Range: 1 through 98
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Address-Assignment Pools Overview on page 315 • Configuring Address-Assignment Pool Usage Threshold Traps on page 320

access-identifier

Syntax	<code>access-identifier <i>identifier-string</i>;</code>
Hierarchy Level	[edit protocols ancp interfaces <i>interface-name</i>], [edit protocols ancp interfaces interface-set]
Release Information	Statement introduced in Junos OS Release 9.4.
Description	Associate an access-loop circuit identifier (ACI) with the VLAN or set of VLANs that carry traffic to the subscriber using that access loop; identify a particular subscriber. This statement requires that the name of the interface or interface set is statically configured or deterministic. This means that it can be used with dynamic or static interface sets, VLAN-tagged interface sets, or static VLAN/VLAN demux interfaces.
Options	<i>identifier-string</i> —Unique identifier string for the access loop circuit; also configured on the access node.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the ANCP Agent on page 368• Associating an Access Node with Subscribers for ANCP Agent Operations on page 370

access-loop-id-local

Syntax	<code>access-loop-id-local;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	Statement introduced in Junos OS Release 13.1.
Description	Specify that the Agent-Remote-Id and Agent-Circuit-Id are generated locally when these values are not present in the client database.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Server Options for Subscriber Access on page 102• Configuring RADIUS Server Parameters for Subscriber Access on page 102

access-profile (Domain Map)

Syntax	<code>access-profile <i>profile-name</i>;</code>
Hierarchy Level	[edit access domain map <i>domain-map-name</i>]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Access profile that defines the AAA services and options for subscribers associated with the domain map.
Options	<i>profile-name</i> —Name of access profile.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Specifying an Access Profile in a Domain Map on page 132

access-profile (Static Subscribers)

Syntax	<code>access-profile <i>profile-name</i>;</code>
Hierarchy Level	<code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> system services static-subscribers],</code> <code>[edit logical-systems <i>logical-system-name</i> system services static-subscribers group <i>group-name</i>],</code> <code>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers],</code> <code>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i>],</code> <code>[edit system services static-subscribers],</code> <code>[edit system services static-subscribers group <i>group-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Specify the access profile that triggers AAA services for all static subscribers on interfaces configured at the <code>[edit system services static-subscribers interface]</code> hierarchy level or for the static subscribers in a specific group. The group version of this statement overrides the global configuration.
Options	<i>profile-name</i> —Name of the static subscriber access profile.
Required Privilege Level	access —To view this statement in the configuration. access-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Subscribers over Static Interfaces on page 466• Specifying the Static Subscriber Global Access Profile on page 471• Specifying the Static Subscriber Group Access Profile on page 476

access-profile-name (Duplicate Accounting)

Syntax	<code>access-profile-name [<i>profile-name</i>];</code>
Hierarchy Level	[edit access profile <i>profile-name</i> accounting duplication-vrf]
Release Information	Statement introduced in Junos OS Release 12.3R3 and supported in later 12.3Rx releases. Statement supported in Junos OS Release 13.2 and later releases.
Description	Specify up to five access profiles, all in the same nondefault VRF (LS:RI combination), each of which lists one or more RADIUS accounting servers to which duplication accounting information is sent.
Options	<i>profile-name</i> —Name of an access profile that lists RADIUS accounting servers for duplicate reporting.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding RADIUS Accounting Duplicate Reporting on page 87• Configuring Authentication and Accounting Parameters for Subscriber Access on page 80

accounting (Access Profile)

Syntax	<pre>accounting { accounting-stop-on-access-deny; accounting-stop-on-failure; address-change-immediate-update; coa-immediate-update; coa-no-override service-class-attribute; duplication; duplication-vrf { access-profile-name <i>profile-name</i>; vrf-name <i>vrf-name</i>; } immediate-update; order [<i>accounting-method</i>]; send-acct-status-on-config-change statistics (time volume-time); update-interval <i>minutes</i>; wait-for-acct-on-ack; }</pre>
Hierarchy Level	[edit access profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.
Description	Configure RADIUS accounting parameters and enable RADIUS accounting for an access profile. The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Authentication and Accounting Parameters for Subscriber Access on page 80• Configuring Per-Subscriber Session Accounting on page 92• Understanding RADIUS Accounting Duplicate Reporting on page 87


accounting-backup-options (Access Profile)

Syntax	<pre>accounting-backup-options { max-pending-accounting-stops <i>number</i>; max-withhold-time <i>hold-time</i>; }</pre>
Hierarchy Level	[edit access]
Release Information	Statement introduced in Junos OS Release 13.1.
Description	<p>Configure options for backing up RADIUS accounting stop requests when all RADIUS accounting servers in the profile are offline.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>access—To view this statement in the configuration.</p> <p>access-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Back-up Options for RADIUS Accounting on page 97

accounting-order (Service Accounting)

Syntax	accounting-order (activation-protocol radius);
Hierarchy Level	[edit access profile <i>profile-name</i> <i>service</i>]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Specify which method is used for reporting subscriber service accounting.
Default	activation-protocol
Options	<p>activation-protocol—Send service accounting reports by means of the application that activates services, such as JSRC.</p> <p>radius—Send service accounting reports by means of the RADIUS protocol.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Service Accounting with JSRC on page 460 • Service Accounting with JSRC on page 459

accounting-port

Syntax	<code>accounting-port <i>port-number</i>;</code>
Hierarchy Level	[edit access radius-server <i>server-address</i>], [edit access profile <i>profile-name</i> radius-server <i>server-address</i>]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches with support for Enhanced Layer 2 software (ELS).</p> <p>Statement introduced on Junos OS without ELS in the following releases:</p> <ul style="list-style-type: none">• Junos OS Release 12.3 for EX Series switches: Release 12.3R10.• Junos OS Release 14.1X53 for EX Series switches: Release 14.1X53-D25. <p>Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.</p>
Description	Configure the port number on which to contact the RADIUS accounting server.
	<div> NOTE: Specifying the accounting port is optional, and port 1813 is the default. However, we recommend that you configure it in order to avoid confusion, as some RADIUS servers might refer to an older default.</div>
Options	<p><i>port-number</i>—Port number on which to contact the RADIUS accounting server. Most RADIUS servers use port 1813, as specified in RFC 2866.</p> <p>Default: 1813</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS System Accounting• Configuring Router or Switch Interaction with RADIUS Servers on page 99• Configuring Authentication and Accounting Parameters for Subscriber Access on page 80• Configuring RADIUS Authentication for L2TP

accounting-retry (RADIUS)

Syntax	<code>accounting-retry <i>number</i>;</code>
Hierarchy Level	[edit access radius-server <i>server-address</i>], [edit access profile <i>profile-name</i> radius-server <i>server-address</i>]
Release Information	Statement introduced in Junos OS Release 14.1.
Description	Configure the number of times the router retransmits RADIUS accounting messages when no response is received from the server.
Options	<i>number</i> —Number of retry attempts. Default: 0 (disabled) Range: 0 through 30
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Router or Switch Interaction with RADIUS Servers on page 99 • Configuring Authentication and Accounting Parameters for Subscriber Access on page 80 • Configuring RADIUS Authentication for L2TP

accounting-server

Syntax	<code>accounting-server [<i>ip-address</i>];</code>
Hierarchy Level	[edit access profile <i>profile-name</i> radius]
Release Information	Statement introduced in Junos OS Release 9.1.
Description	Specify a list of the RADIUS accounting servers used for accounting for DHCP, L2TP, and PPP clients.
Options	<i>ip-address</i> —IP version 4 (IPv4) address.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Authentication and Accounting Parameters for Subscriber Access on page 80

accounting-session-id-format

Syntax	accounting-session-id-format (decimal description);
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	Configure the format the router or switch uses to identify the accounting session.
Default	decimal
Options	decimal —Use the decimal format. description —Use the generic format, in the form: jnpr <i>interface-specifier:subscriber-session-id</i> .
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Server Options for Subscriber Access on page 102• Configuring Authentication and Accounting Parameters for Subscriber Access on page 80

accounting-stop-on-access-deny

Syntax	accounting-stop-on-access-deny;
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	Configure RADIUS accounting to send an Acct-Stop message when the AAA server refuses a client request for access.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Authentication and Accounting Parameters for Subscriber Access on page 80

accounting-stop-on-failure

Syntax	accounting-stop-on-failure;
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	Configure RADIUS accounting to send an Acct-Stop message when client access fails AAA but the AAA server grants access.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Authentication and Accounting Parameters for Subscriber Access on page 80

accounting-timeout (RADIUS)

Syntax	accounting-timeout <i>seconds</i> ;
Hierarchy Level	[edit access radius-server <i>server-address</i>], [edit access profile <i>profile-name</i> radius-server <i>server-address</i>]
Release Information	Statement introduced in Junos OS Release 14.1.
Description	Configure how long the local router waits to receive a response from a RADIUS accounting server before retransmitting the message.
Options	<i>seconds</i> —Duration of timeout period. Default: 0 (disabled) Range: 0 through 900 seconds
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Router or Switch Interaction with RADIUS Servers on page 99 • Configuring Authentication and Accounting Parameters for Subscriber Access on page 80 • Configuring RADIUS Authentication for L2TP

active-server-group

Syntax	<code>active-server-group <i>server-group-name</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay], [edit forwarding-options dhcp-relay dhcpv6], [edit forwarding-options dhcp-relay group <i>group-name</i>], [edit forwarding-options dhcp-relay group <i>group-name</i> dhcpv6], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6], [edit logical-systems <i>logical-system-name</i> forwarding-options group <i>group-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options group <i>group-name</i> dhcpv6], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> dhcpv6], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay] [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i>], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 8.3.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	<p>Apply a DHCP relay agent configuration to the named group of DHCP server addresses. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.</p> <p>A group-specific configuration overrides a global option.</p>
Options	<i>server-group-name</i> —Name of the group of DHCP or DHCPv6 server addresses to which the DHCP or DHCPv6 relay agent configuration applies.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Extended DHCP Relay Agent Overview on page 194 • Configuring Active Server Groups on page 259 • Configuring Group-Specific DHCP Relay Options on page 226 • dhcp-relay on page 689

address (Diameter Peer)

Syntax	<code>address <i>ip-address</i>;</code>
Hierarchy Level	[edit diameter peer <i>peer-name</i>]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Configure the IP address for a Diameter remote peer.
Options	<i>ip-address</i> —IP address of remote Diameter peer.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Diameter on page 434• Configuring Diameter Peers on page 435

address (Diameter Transport)

Syntax	<code>address <i>ip-address</i>;</code>
Hierarchy Level	[edit diameter transport <i>transport-name</i>]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	Configure the source (local) IP address for the Diameter local transport connection.
Options	<i>ip-address</i> —IP address of remote Diameter peer.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Diameter on page 434

address-assignment (Address-Assignment Pools)

```
Syntax  address-assignment {
        abated-utilization percentage;
        abated-utilization-v6 percentage;
        high-utilization percentage;
        high-utilization-v6 percentage;
        neighbor-discovery-router-advertisement ndra-pool-name;
        pool pool-name {
            family family {
                dhcp-attributes {
                    protocol-specific attributes;
                }
            }
            host hostname {
                hardware-address mac-address;
                ip-address ip-address;
            }
            network ip-prefix / <prefix-length>;
            prefix ipv6-prefix;
            range range-name {
                high upper-limit;
                low lower-limit;
                prefix-length prefix-length;
            }
        }
        link pool-name;
    }
```

Hierarchy Level [edit access]

Release Information Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.1 for EX Series switches.
Statement introduced in Junos OS Release 14.1X53-D30 for the QFX Series.

Description Configure address-assignment pools that can be used by different client applications.



NOTE: Support for subordinate statements is platform-specific. See individual statement topics for support information.

Options *pool-name*—Name assigned to an address-assignment pool.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- [Address-Assignment Pools Overview on page 315](#)
- [Configuring Address-Assignment Pools on page 316](#)

- *Configuring an Address-Assignment Pool for L2TP LNS with Inline Services*
- *Configuring a DHCP Server on Switches (CLI Procedure)*

address-pool (Domain Map)

Syntax	<code>address-pool <i>pool-name</i>;</code>
Hierarchy Level	[edit access domain <code>map</code> <i>domain-map-name</i>]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Specify the address pool used to assign addresses to subscribers associated with the domain map.
Options	<i>pool-name</i> —Name of address pool.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Specifying an Address Pool in a Domain Map on page 133

adjacency-timer

Syntax	<code>adjacency-timer <i>seconds</i>;</code>
Hierarchy Level	[edit protocols <code>ancp</code>], [edit protocols <code>ancp neighbor ip-address</code>]
Release Information	Statement introduced in Junos OS Release 9.4.
Description	Specify a value for the interval that the ANCP agent proposes during negotiation to establish an adjacency, for all neighbors or a specific neighbor. The larger of the values proposed by the agent and the neighbor is selected for the interval between subsequent adjacency messages exchanged by the agent and the neighbor.
Options	<i>seconds</i> —Number of seconds between adjacency messages. Range: 1 through 25 seconds Default: 10 seconds
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring the ANCP Agent on page 368 • Specifying the Interval Between ANCP Adjacency Messages on page 371 • Configuring ANCP Neighbors on page 369

advisory-options (Traffic Shaping)

Syntax	<pre>advisory-options { downstream-rate <i>rate</i>; upstream-rate <i>rate</i>; }</pre>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> interfaces \$junos-interface-ifd-name unit \$junos-interface-unit], [edit dynamic-profiles <i>profile-name</i> interfaces interface-set \$junos-interface-set-name interface \$junos-interface-ifd-name], [edit interfaces demux0 unit <i>logical-unit-number</i>], [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]
Release Information	Statement introduced in Junos OS Release 11.4. Support at the [edit interfaces demux0 ...] hierarchy level introduced in Junos OS Release 12.2. Support at the [edit dynamic-profiles ...] hierarchy level introduced in Junos OS Release 13.1.
Description	<p>Specify a recommended shaping rate to be applied to downstream or upstream traffic on an interface.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Setting a Recommended Shaping Rate for Traffic on ANCP Interfaces on page 400• Configuring the ANCP Agent on page 368• Configuring the Method to Set the LAC Connection Speeds to the LNS

aggregate-clients (DHCP Relay Agent)

Syntax	<code>aggregate-clients (merge replace);</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay dhcpv6 dynamic-profile <i>profile-name</i>], [edit forwarding-options dhcp-relay dynamic-profile <i>profile-name</i>], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> dynamic-profile <i>profile-name</i>], [edit forwarding-options dhcp-relay group <i>group-name</i> dynamic-profile <i>profile-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 dynamic-profile <i>profile-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dynamic-profile <i>profile-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> dynamic-profile <i>profile-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> dynamic-profile <i>profile-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 dynamic-profile <i>profile-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dynamic-profile <i>profile-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> dynamic-profile <i>profile-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> dynamic-profile <i>profile-name</i>], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 dynamic-profile <i>profile-name</i>], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dynamic-profile <i>profile-name</i>], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> dynamic-profile <i>profile-name</i>], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> dynamic-profile <i>profile-name</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.3.</p> <p>Options merge and replace introduced in Junos OS Release 9.5.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	<p>Specify that the router merge (chain) client attributes such as firewall filters and CoS attributes or replace them when multiple client sessions exist on the same underlying VLAN. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.</p> <p>M120 and M320 routers do not support DHCPv6.</p> <p>Not supported for IP demux subscriber interfaces.</p>
Options	<p>merge—Aggregate multiple client attributes for the same subscriber (logical interface)</p> <p>replace—Replace the entire logical interface whenever a new client logs in to the network using the same VLAN logical interface</p>

Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• dhcp-relay on page 689• <i>Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces</i>• Configuring Group-Specific DHCP Relay Options on page 226

aggregate-clients (Static Subscribers)

Syntax	aggregate-clients (merge replace);
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers group <i>group-name</i> dynamic-profile <i>profile-name</i>],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers dynamic-profile <i>profile-name</i>],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> dynamic-profile <i>profile-name</i>],</p> <p>[edit system services static-subscribers dynamic-profile <i>profile-name</i>],</p> <p>[edit system services static-subscribers group <i>group-name</i> dynamic-profile <i>profile-name</i>]</p>
Release Information	Statement introduced in Junos OS Release 9.6.
Description	<p>Specify for all static subscribers or for a group of static subscribers that the router merge (chain) subscriber (client) attributes such as firewall filters and CoS attributes or replace them when multiple subscriber sessions exist on the same underlying VLAN. The group version of this statement overrides the global version.</p> <p>This statement is not supported for IP demux subscriber interfaces.</p>
Default	By default, multiple subscribers cannot be on the same logical interface.
Options	<p>merge—Aggregate the attributes of multiple subscribers for the logical interface.</p> <p>replace—Replace the entire logical interface whenever a new client logs in to the network using the same VLAN logical interface.</p>
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Subscribers over Static Interfaces on page 466• Enabling Multiple Subscribers on a VLAN Logical Interface for All Static Subscribers on page 472

always-write-giaddr

Syntax	<code>always-write-giaddr;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay <i>overrides</i>], [edit forwarding-options dhcp-relay group <i>group-name overrides</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay <i>overrides</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name overrides</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay <i>overrides</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name overrides</i>], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay <i>overrides</i>], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name overrides</i>], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name overrides</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 8.3.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	Overwrite the gateway IP address (giaddr) of every DHCP packet with the giaddr of the DHCP relay agent before forwarding the packet to the DHCP server.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Extended DHCP Relay Agent Overview on page 194 • dhcp-relay on page 689

always-write-option-82

Syntax	<code>always-write-option-82;</code>
Hierarchy Level	<code>[edit forwarding-options dhcp-relay overrides],</code> <code>[edit forwarding-options dhcp-relay group <i>group-name</i> overrides],</code> <code>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides],</code> <code>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</code> <code>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides],</code> <code>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</code> <code>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]</code>
Release Information	Statement introduced in Junos OS Release 8.3. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	<p>Override the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server. The use of this option causes the DHCP relay agent to perform one of the following actions, depending on how it is configured:</p> <ul style="list-style-type: none">• If the DHCP relay agent is configured to add option 82 information to DHCP packets, it clears the existing option 82 values from the DHCP packets and inserts the new values before forwarding the packets to the DHCP server.• If the DHCP relay agent is not configured to add option 82 information to DHCP packets, it clears the existing option 82 values from the packets, but does not add any new values before forwarding the packets to the DHCP server.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Extended DHCP Relay Agent Overview on page 194

ancp

```

Syntax  ancp {
        adjacency-timer seconds;
        gsmp-syn-timeout seconds;
        gsmp-syn-wait;
        interfaces {
            interface-set interface-set-name {
                access-identifier identifier-string;
                underlying-interface underlying-interface-name;
            }
            interface-name {
                access-identifier identifier-string;
            }
        }
        maximum-discovery-table-entries entry-number;
        maximum-helper-restart-time;
        neighbor ip-address {
            adjacency-timer;
            ietf-mode;
            maximum-discovery-table-entries entry-number;
            pre-ietf-mode;
        }
        pre-ietf-mode;
        qos-adjust;
        qos-adjust-adsl adjustment-factor;
        qos-adjust-adsl2 adjustment-factor;
        qos-adjust-adsl2-plus adjustment-factor;
        qos-adjust-sdsl adjustment-factor;
        qos-adjust-vdsl adjustment-factor;
        qos-adjust-vdsl2 adjustment-factor;
        traceoptions {
            file filename <files number> <match regular-expression > <size maximum-file-size>
                <world-readable | no-world-readable>;
            flag flag;
            level (all | error | info | notice | verbose | warning);
            no-remote-trace;
        }
    }

```

Hierarchy Level [edit protocols]

Release Information Statement introduced in Junos OS Release 9.4.

Description Configure Junos OS ANCP agent features.

The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- [Configuring the ANCP Agent on page 368](#)

ancp-speed-change-immediate-update (ANCP)

Syntax	ancp-speed-change-immediate-update;
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in Junos OS Release 13.3.
Description	Configure AAA to generate immediate interim accounting updates to the RADIUS server in response to ANCP agent notifications of rate changes on subscriber access lines.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Immediate Interim Accounting Updates to RADIUS in Response to ANCP Notifications on page 408• Configuring Per-Subscriber Session Accounting on page 92• Configuring the ANCP Agent on page 368

application-group-any

Syntax	application-group-any;
Hierarchy Level	[edit services ptsp rule <i>rule-name</i> term <i>precedence</i> from]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Specify that any application group defined in the database is considered a match.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Static PTSP Rules on page 495 in Junos OS Subscriber Management and Services Library

application-groups

Syntax	<code>application-group [<i>application-group-name</i>];</code>
Hierarchy Level	[edit services ptsp forward-rule <i>forward-rule-name</i> term <i>precedence</i> from] [edit services ptsp rule <i>rule-name</i> term <i>precedence</i> from]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Identify one or more application groups defined in the application identification configuration for inclusion as a match condition.
Options	<i>application-group-name</i> —Identifier of the application group.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>

applications (Services PTSP)

Syntax	<code>applications [<i>application-name</i>];</code>
Hierarchy Level	[edit services ptsp forward-rule <i>forward-rule-name</i> term <i>precedence</i> from] [edit services ptsp rule <i>rule-name</i> term <i>precedence</i> from]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Identify one or more applications defined in the application identification configuration for inclusion as a match condition.
Options	<i>application-name</i> —Identifier of the application.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>

attempts (DHCP Local Server)

Syntax	<code>attempts <i>attempt-count</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit system services dhcp-local-server reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.0.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.</p>
Description	Configure how many attempts are made to reconfigure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces before reconfiguration is considered to have failed. A group configuration takes precedence over a DHCP local server configuration.
Options	<p><i>attempt-count</i>—Maximum number of attempts.</p> <p>Range: 1 through 10</p> <p>Default: 8</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Dynamic Client Reconfiguration of Extended Local Server Clients on page 244 • Configuring Dynamic Reconfiguration Attempts for DHCP Clients on page 246

attributes

Syntax	<pre> attributes { exclude { ... } ignore { framed-ip-netmask; input-filter; logical-system-routing-instance; output-filter; } } </pre>
Hierarchy Level	[edit access profile <i>profile-name</i> radius]
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 9.1 for EX Series switches.</p>
Description	<p>Specify how the router or switch processes RADIUS attributes.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring How RADIUS Attributes Are Used for Subscriber Access on page 40

authentication (DHCP Local Server)

Syntax	<pre> authentication { password <i>password-string</i>; username-include { circuit-type; client-id; delimiter <i>delimiter-character</i>; domain-name <i>domain-name-string</i>; interface-name; logical-system-name; mac-address; option-60; option-82 <circuit-id> <remote-id>; relay-agent-interface-id; relay-agent-remote-id; relay-agent-subscriber-id; routing-instance-name; user-prefix <i>user-prefix-string</i>; } } </pre>
Hierarchy Level	<pre> [edit system services dhcp-local-server], [edit system services dhcp-local-server dhcpv6], [edit system services dhcp-local-server dhcpv6 group group-name], [edit system services dhcp-local-server group group-name], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server ...], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...] </pre>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	<p>Configure the parameters the router sends to the external AAA server. A group configuration takes precedence over a global DHCP relay or DHCP local server configuration.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using External AAA Authentication Services with DHCP on page 217


authentication (DHCP Relay Agent)

Syntax	<pre> authentication { password <i>password-string</i>; username-include { circuit-type; client-id; delimiter <i>delimiter-character</i>; domain-name <i>domain-name-string</i>; interface-name; logical-system-name; mac-address; option-60; option-82 <circuit-id> <remote-id>; relay-agent-interface-id; relay-agent-remote-id; relay-agent-subscriber-id; routing-instance-name; user-prefix <i>user-prefix-string</i>; } }</pre>
Hierarchy Level	<pre> [edit forwarding-options dhcp-relay], [edit forwarding-options dhcp-relay dhcpv6], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i>], [edit forwarding-options dhcp-relay group <i>group-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...]</pre>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p>
Description	<p>Configure the parameters the router sends to the external AAA server. A group configuration takes precedence over a global DHCP relay configuration. Use the statement at the [edit...dhcpv6] hierarchy levels to configure DHCPv6 support.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • dhcp-relay on page 689 • Using External AAA Authentication Services with DHCP on page 217

authentication (Static Subscribers)

Syntax	<pre> authentication { password <i>password-string</i>; username-include { domain-name <i>domain-name</i>; interface; logical-system-name; routing-instance-name; user-prefix <i>user-prefix-string</i>; } }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers group <i>group-name</i>],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i>],</p> <p>[edit system services static-subscribers],</p> <p>[edit system services static-subscribers group <i>group-name</i>]</p>
Release Information	Statement introduced in Junos OS Release 9.6.
Description	<p>Specify the authentication parameters that trigger the Access-Request message to AAA for all static subscribers on interfaces configured at the [edit system services static-subscribers interface] hierarchy level, or for the static subscribers in a specific group. The group version of this statement overrides the global configuration.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Subscribers over Static Interfaces on page 466 • Configuring the Static Subscriber Global Authentication Password on page 473 • Configuring the Static Subscriber Group Authentication Password on page 477

authentication-order

Syntax	<code>authentication-order [<i>authentication-methods</i>];</code>
Hierarchy Level	<code>[edit access <i>profile</i> <i>profile-name</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Option none introduced in Junos OS Release 11.2.
Description	Set the order in which the Junos OS tries different authentication methods when verifying that a client can access the router or switch. For each login attempt, the software tries the authentication methods in order, from first to last.
Default	password
Options	<p><i>authentication-methods</i></p> <ul style="list-style-type: none"> • none—Grants authentication without examining the client credentials. Can be used, for example, when the Diameter function Gx-Plus is employed for notification during subscriber provisioning. • password—Verify the client using the information configured at the <code>[edit access profile <i>profile-name</i> client <i>client-name</i>]</code> hierarchy level. • radius—Verify the client using RADIUS authentication services.
<div>  <p>NOTE: For subscriber access management, you must always specify the radius method. Subscriber access management does not support the password option (the default), and authentication fails when no method is specified.</p> </div>	
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Example: Configuring CHAP Authentication with RADIUS</i> • Specifying the Authentication and Accounting Methods for Subscriber Access on page 80 • <i>Configuring Access Profiles for L2TP or PPP Parameters</i>

authentication-server

Syntax	authentication-server [<i>ip-address</i>];
Hierarchy Level	[edit access profile profile-name radius]
Release Information	Statement introduced in Junos OS Release 9.1.
Description	Specify a list of the RADIUS authentication servers used to authenticate DHCP, L2TP, and PPP clients. The servers in the list are also used as RADIUS dynamic-request servers, from which the router accepts and processes RADIUS disconnect requests, CoA requests, and dynamic service activations and deactivations.
Options	<i>ip-address</i> —IPv4 address.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Server Parameters for Subscriber Access on page 102

authorization-order

Syntax	authorization-order (jsrc [<i>authorization-order-data-list</i>]);
Hierarchy Level	[edit access profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 9.6. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Description	Configure AAA to use JSRC in an SRC environment to request authorization from the SAE when verifying that a DHCP subscriber can access the router or switch. When you include this statement, AAA ignores any configured authentication order settings. This statement is ignored for non-DHCP subscribers.
Options	jsrc—Use JSRC application to communicate with the SAE for subscriber authorization. JSRC is the only application that is currently available. [<i>authorization-order-data-list</i>] —Set of data listing the authorization order to be used, enclosed by brackets. This can be any combination of authorization methods, up to and including a list of the entire authorization order.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring JSRC on page 455• Authorizing Subscribers with JSRC on page 457

autonomous (Dynamic Router Advertisement)

Syntax	(autonomous no-autonomous);
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols router-advertisement interface <i>interface-name</i> <i>prefix</i> <i>prefix</i>]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	Specify whether prefixes in the router advertisement messages are used for stateless address autoconfiguration: <ul style="list-style-type: none"> • autonomous—Use prefixes for address autoconfiguration. • no-autonomous—Do not use prefixes for address autoconfiguration.
Default	autonomous
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Example: Configuring IPv6 Interfaces and Enabling Neighbor Discovery</i>

boot-file

Syntax	boot-file <i>filename</i> ;
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet <i>dhcp-attributes</i>]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	Set the boot file advertised to DHCP clients. After the client receives an IP address and the boot file location from the DHCP server, the client uses the boot image stored in the boot file to complete DHCP setup. This configuration is equivalent to DHCP Option 67.
Options	<i>filename</i> —Location of the boot file on the boot server. The filename can include a pathname.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • boot-server on page 656 • Configuring Address-Assignment Pools on page 316 • <i>Configuring a DHCP Server on Switches (CLI Procedure)</i>

boot-server

Syntax	<code>boot-server (address hostname);</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	Configure the name of the boot server advertised to DHCP clients. The client uses a boot file located on the boot server to complete DHCP setup. This configuration is equivalent to DHCP Option 66.
Options	address —IPv4 address of a boot server. hostname —Fully qualified hostname of a boot server.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• boot-file on page 655• Configuring Address-Assignment Pools on page 316• Configuring a DHCP Server on Switches (CLI Procedure)

calling-station-id-delimiter (Subscriber Management)

Syntax	<code>calling-station-id-delimiter <i>delimiter-character</i>;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	Statement introduced in Junos OS Release 13.1.
Description	Specify the character that the router uses as a separator between the concatenated values in the Calling-Station-ID (RADIUS IETF attribute 31) string. The router uses the delimiter when you configure more than one value in the calling-station-id-format statement.
Default	The hash (#) character.
Options	delimiter-character —Character to use for the delimiter. You must enclose the delimiter character in quotation marks (" ").
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring a Calling-Station-ID with Additional Attributes on page 58

calling-station-id-format (Subscriber Management)

Syntax	calling-station-id-format { agent-circuit-id; agent-remote-id; interface-description; nas-identifier; }
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	Statement introduced in Junos OS Release 13.1.
Description	Specify the information that the router includes in the Calling-Station-ID (RADIUS IETF attribute 31) that is passed to the RADIUS server during authentication and accounting. You can include one or more optional values in any combination.
Default	The router displays the Calling-Station-ID set by the client.
Options	<p>agent-circuit-id—Include the agent circuit identifier (ACI) string, which uniquely identifies the subscriber's access node and the digital subscriber line (DSL) on the access node. The ACI string is stored in either the DHCP option 82 field of DHCP messages (for DHCP traffic), or in the DSL Forum Agent-Circuit-ID VSA [26-1] of PPPoE PADI and PADR control packets (for PPPoE traffic).</p> <p>agent-remote-id—Include the agent remote identifier (ARI) string, which identifies the subscriber on the digital subscriber line access multiplexer (DSLAM) interface that initiated the service request. The ARI string is stored in either the DHCP option 82 field of DHCP messages (for DHCP traffic), or in the DSL Forum Agent-Remote-ID VSA [26-2] of PPPoE PADI and PADR control packets (for PPPoE traffic).</p> <p>interface-description—Include the interface description value.</p> <p>nas-identifier—Include the NAS-identifier (RADIUS IETF attribute 32), which specifies the name of the NAS that originated the authentication or accounting request.</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring a Calling-Station-ID with Additional Attributes on page 58

circuit-id (Address-Assignment Pools)

Syntax	<code>circuit-id <i>value</i> range <i>named-range</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes option-match option-82]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	Configure the address-assignment pool <i>named-range</i> to use for a particular option 82 Agent Circuit ID value.
Options	<p><i>value</i>—String for the Agent Circuit ID suboption (suboption 1) of the DHCP relay agent information option (option 82) in DHCP packets.</p> <p><i>range named-range</i>—Name of the address-assignment pool range to use.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Address-Assignment Pools on page 316

circuit-type (DHCP Local Server)

Syntax	circuit-type;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server group group-name authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify that the circuit type is concatenated with the username during the subscriber authentication or client authentication process.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using External AAA Authentication Services with DHCP on page 217

circuit-type (DHCP Relay Agent)

Syntax	circuit-type;
Hierarchy Level	[edit forwarding-options dhcp-relay authentication username-include], [edit forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include], [edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 12.3R2 for EX Series switches. Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Description	Specify that the circuit type is concatenated with the username during the subscriber authentication or client authentication process. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Using External AAA Authentication Services with DHCP on page 217• Creating Unique Usernames for DHCP Clients on page 218

clear-on-abort (DHCP Local Server)

Syntax	clear-on-abort;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit system services dhcp-local-server reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.0.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.</p>
Description	Delete all DHCP clients or only the DHCP clients serviced by the specified group of interfaces when reconfiguration fails; that is, when the maximum number of retry attempts have been made without success. A group configuration takes precedence over a DHCP local server configuration.
Default	Restores the original client configuration when reconfiguration fails.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Dynamic Client Reconfiguration of Extended Local Server Clients on page 244 • Configuring Deletion of the Client When Dynamic Reconfiguration Fails on page 247


client-accounting-algorithm

Syntax	client-accounting-algorithm (direct round-robin);
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	Statement introduced in Junos OS Release 10.0. Statement introduced in Junos OS for EX Series switches Release 13.2X50-D10.
Description	Configure the access method the router uses to access RADIUS accounting servers.
Default	direct
Options	direct —Use the direct method. round-robin —Use the round-robin method.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Server Parameters for Subscriber Access on page 102• Configuring RADIUS Server Options for Subscriber Access on page 102


client-authentication-algorithm

Syntax	client-authentication-algorithm (direct round-robin);
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	Statement introduced in Junos OS Release 10.0. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Description	Configure the access method the router uses to access RADIUS authentication servers.
Default	direct
Options	direct —Use the direct method. round-robin —Use the round-robin method.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Server Parameters for Subscriber Access on page 102• Configuring RADIUS Server Options for Subscriber Access on page 102

client-discover-match (DHCP Local Server)

Syntax	client-discover-match (option60-and-option82 incoming-interface);
Hierarchy Level	<p>[edit system services dhcp-local-server overrides],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i> overrides]</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server ... overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server ...overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...overrides]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.4.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Option incoming-interface introduced in Junos OS Release 13.3.</p>
Description	Configure the match criteria DHCP local server uses to uniquely identify DHCP subscribers or clients when primary identification fails. The options are mutually exclusive.
Options	<p>incoming-interface—Allow only one client device to connect on the interface. If the client device changes, the router deletes the existing client binding and creates a binding for the newly connected device.</p>
<div style="display: flex; align-items: flex-start;"> <div style="flex: 1; text-align: center; margin-right: 10px;">  </div> <div> <p>NOTE: The overrides client-discover-match incoming-interface configuration deletes and replaces the existing binding when a new device connects. This action differs from the overrides interface-client-limit 1 statement, which retains the existing binding and rejects the newly connected client.</p> </div> </div>	
<p>option60-and-option82—Use option 60 and option 82 information to identify subscribers.</p>	
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Extended DHCP Local Server Overview on page 188 • Overriding Default DHCP Local Server Configuration Settings on page 255 • DHCP Auto Logout Overview on page 249 • Allowing Only One DHCP Client Per Interface on page 234

client-discover-match (DHCP Relay Agent)

Syntax	client-discover-match (option60-and-option82 incoming-interface);
Hierarchy Level	<p>[edit forwarding-options dhcp-relay overrides],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay ... overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ... overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group ... overrides]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.4.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Option incoming-interface introduced in Junos OS Release 13.3.</p>
Description	Configure the match criteria DHCP relay uses to uniquely identify DHCP subscribers or clients when primary identification fails. The options are mutually exclusive.
Options	<p>incoming-interface—Allow only one client device to connect on the interface. If the client device changes, the router deletes the existing client binding and creates a binding for the newly connected device.</p>
<div style="display: flex; align-items: flex-start;"> <div style="flex: 1; text-align: center; margin-right: 10px;">  </div> <div> <p>NOTE: The overrides client-discover-match incoming-interface configuration deletes and replaces the existing binding when a new device connects. This action differs from the overrides interface-client-limit 1 statement, which retains the existing binding rejects the newly connected client.</p> </div> </div>	
<p>option60-and-option82—Use option 60 and option 82 information to identify subscribers.</p>	
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Extended DHCP Relay Agent Overview on page 194 • Overriding the Default DHCP Relay Configuration Settings on page 256 • DHCP Auto Logout Overview on page 249 • Allowing Only One DHCP Client Per Interface on page 234

client-id (DHCP Local Server)

Syntax	client-id;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify that the DHCPv6 Client-ID option (option 1) in the client PDU name is concatenated with the username during the subscriber authentication or client authentication process.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Creating Unique Usernames for DHCP Clients on page 218


client-id (DHCP Relay Agent)

Syntax	client-id;
Hierarchy Level	[edit forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 ...], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 ...]
Release Information	Statement introduced in Junos OS Release 11.4. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Specify that the client ID is concatenated with the username during the subscriber authentication or client authentication process.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Using External AAA Authentication Services with DHCP on page 217• Creating Unique Usernames for DHCP Clients on page 218

client-idle-timeout

Syntax	client-idle-timeout <i>minutes</i> ;
Hierarchy Level	[edit access profile <i>profile-name</i> session-options]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	(MX Series and SRX Series devices) Specify the grace period that begins after an authenticated user terminates all sessions and connections. Authentication is not required if a new connection is initiated during the grace period by the same user.
Default	The timeout is not configured.
Options	minutes —Number of minutes of idle time that elapse before the session is terminated. Range: 10 through 1440 minutes
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding Session Options for Subscriber Access on page 109• Configuring Subscriber Session Options on page 111• Removing Inactive Dynamic Subscriber VLANs on page 112

client-session-timeout

Syntax	client-session-timeout <i>minutes</i> ;
Hierarchy Level	[edit access profile <i>profile-name</i> session-options]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	(MX Series and SRX Series devices) Specify the amount of time after which user sessions are terminated, regardless of user activity (also known as a forced or hard authentication timeout).
<div>  <p>NOTE: For all subscriber types other than DHCP (such as L2TP-tunneled and PPP-terminated subscribers), the client-session-timeout value limits the subscriber session. For DHCP subscribers, the client-session-timeout value is used to limit the lease. The lease expires when the timeout value expires. If this value is not supplied by either the CLI or RADIUS, the DHCP lease does not expire.</p> </div>	
Default	The timeout is not configured.
Options	<i>minutes</i> —Number of minutes after which user sessions are terminated. Range: 1 through 527040 minutes
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Understanding Session Options for Subscriber Access on page 109 • Configuring Subscriber Session Options on page 111

coa-dynamic-variable-validation

Syntax	coa-dynamic-variable-validation;
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	Statement introduced in Junos OS Release 12.1. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Description	Specify that when a CoA operation includes a change to a client profile dynamic variable that cannot be applied (such as an update to a non-existent filter), the router does not apply any changes to client profile dynamic variables in the request, and responds with a NACK message.
Default	If you do not configure this statement, the router does not apply any incorrect variable updates but does make any other changes to the client profile dynamic variables, and then responds with an ACK message.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Server Options for Subscriber Access on page 102• RADIUS Server Options for Subscriber Access on page 4• Configuring RADIUS Server Parameters for Subscriber Access on page 102

coa-immediate-update

Syntax	coa-immediate-update;
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in Junos OS Release 10.0.
Description	Configure the router to send an Acct-Update message to the RADIUS accounting server immediately following a CoA operation.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Server Parameters for Subscriber Access on page 102• Configuring Per-Subscriber Session Accounting on page 92

coa-no-override service-class-attribute

Syntax	coa-no-override service-class-attribute;
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Specify that, after a CoA action that changes the RADIUS Class attribute, accounting reports for the subscriber's service sessions continue to use the original Class attribute that was assigned when the service sessions were created. The new Class attribute value is used in accounting reports for the subscriber session only.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring RADIUS Server Parameters for Subscriber Access on page 102 • Configuring Per-Subscriber Session Accounting on page 92

concurrent-data-sessions

Syntax	concurrent-data-sessions <i>max-session-number</i> ;
Hierarchy Level	[edit services service-set <i>services-set-name</i> subscriber-profile <i>profile-name</i> enable <i>service-name</i>]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Specify the maximum number of sessions that are concurrently enabled for the named service. The system randomly selects the number of sessions and enables the named service, whereas other sessions are not allotted the named service. This facilitates to increase the limit on the number of resources a service can use.
Options	<i>max-session-number</i> —Maximum number of sessions concurrently enabled for the named service.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

connect-actively

Syntax	<code>connect-actively { <code>port</code> <i>port-number</i>; <code>transport</code> <i>transport-name</i>; }</code>
Hierarchy Level	[edit diameter <code>peer</code> <i>peer-name</i>]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	<p>Define the destination port and transport connection used to establish active connections to Diameter peer.</p> <p>The remaining statements are explained separately.</p>
Default	Port 3868 and an automatically assigned local address are used to establish active connections to a peer.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Diameter on page 434• Configuring Diameter Peers on page 435

count-type

Syntax	count-type (application rule);
Hierarchy Level	[edit services ptsp rule rule-name]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Specify the statistics aggregation, collection, and reporting style for this rule. Terms and rules cannot mix and match different styles. All service rules attached to a given service set must have the same style.
Options	<p>application—Report statistics in a flat file and aggregate them by application for one of the following:</p> <ul style="list-style-type: none"> • An application, where the count action application is specified in the term. • An application group, where the count action application-group is specified in the term. • All application groups, where the count action application-group-any is specified in the term. <p>rule—Aggregate statistics for the service rule. The statistics are reported by Diameter. All count actions in all terms for the rule must specify rule.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>

current-hop-limit (Dynamic Router Advertisement)

Syntax	<code>current-hop-limit <i>number</i>;</code>
Hierarchy Level	[edit dynamic-profiles protocols router-advertisement interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	Default value placed in the hop count field of the IP header for outgoing packets.
Options	<i>number</i> —Hop limit. A value of 0 means the limit is unspecified by this router. Range: 0 through 255 Default: 64
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Example: Configuring IPv6 Interfaces and Enabling Neighbor Discovery</i>

database-replication (Subscriber Session Database)

Syntax	<pre>database-replication { traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i> > <size <i>maximum-file-size</i>> <world-readable no-world-readable>; flag <i>flag</i>; } }</pre>
Hierarchy Level	[edit system services]
Release Information	Statement introduced in Junos OS Release 9.3.
Description	Define operations for subscriber management session database replication processes. The remaining statements are explained separately.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Tracing Subscriber Management Session Database Replication Operations for Subscriber Access on page 535

default-action (DHCP Relay Agent Option)

Syntax	<pre>default-action { drop; forward-only; local-server-group local-server-group; relay-server-group relay-server-group; }</pre>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay relay-option], [edit forwarding-options dhcp-relay dhcpv6 relay-option], [edit forwarding-options dhcp-relay group group-name relay-option], [edit forwarding-options dhcp-relay dhcpv6 group group-name relay-option], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...]</p>
Release Information	Statement introduced in Junos OS Release 12.3.
Description	<p>Specify the action DHCP relay agent takes when the option string in client traffic does not satisfy any match criteria or when no match criteria are configured.</p> <p>The default-action statement is optional. If the match criteria are not satisfied or not configured and no default-action is specified, DHCP relay processes the traffic in the normal manner.</p> <p>The local-server-group option is not supported for DHCPv6 relay agent.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using DHCP Option Information to Selectively Process DHCP Client Traffic on page 273

default-lifetime (Dynamic Router Advertisement)

Syntax	default-lifetime <i>seconds</i> ;
Hierarchy Level	[edit protocols router-advertisement interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	Lifetime associated with a default router.
Options	seconds —Default lifetime. A value of 0 means this router is not the default router. Range: Maximum advertisement interval value through 9000 seconds Default: Three times the maximum advertisement interval value
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>max-advertisement-interval (Protocols IPv6 Neighbor Discovery)</i>• <i>Example: Configuring IPv6 Interfaces and Enabling Neighbor Discovery</i>

delay-authentication (DHCP Relay Agent)

Syntax	delay-authentication;
Hierarchy Level	[edit forwarding-options dhcp-relay ... overrides], [edit forwarding-options dhcp-relay dhcpv6 ... overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay ... overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ... overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ... overrides]
Release Information	Statement introduced in Junos OS Release 13.3.
Description	Delay authentication of subscribers until the DHCP client sends a Request packet. This conserves managed resources by delaying the authorization process and the creation of an entry in the subscriber database until the DHCP request processing phase.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Extended DHCP Relay Agent Overview on page 194• Overriding the Default DHCP Relay Configuration Settings on page 256

delegated-pool (DHCP Local Server)

Syntax	<code>delegated-pool <i>pool-name</i>;</code>
Hierarchy Level	<p>[edit system services dhcp-local-server dhcpv6 overrides],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name overrides],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name interface <i>interface-name overrides</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 ...],</p> <p>[edit logical-systems <i>logical-system-name</i> system services system services dhcp-local-server dhcpv6 ...],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services system services dhcp-local-server dhcpv6 ...]</p>
Release Information	<p>Statement introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify the address pool that assigns the IA_PD address. A pool specified by RADIUS VSA 26-161 takes precedence over the pool specified by this delegated-pool statement.
Options	<i>pool-name</i> —Name of the address-assignment pool.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Specifying the Delegated Address Pool for IPv6 Prefix Assignment on page 290 • Overriding Default DHCP Local Server Configuration Settings on page 255

delimiter (DHCP Local Server)

Syntax	<code>delimiter <i>delimiter-character</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server group group-name authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify the character used as the delimiter between the concatenated components of the username.
Options	<i>delimiter-character</i> —Character that separates components that make up the concatenated username. You cannot use the semicolon (;) as a delimiter.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

- Related Documentation**
- [Using External AAA Authentication Services with DHCP on page 217](#)

delimiter (Domain Map)

Syntax	<code>delimiter [<i>delimiter-character</i>];</code>
Hierarchy Level	[edit access domain]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Specify the characters that the router uses to separate usernames from domain names.
Default	The @ character.
Options	<i>delimiter-character</i> —One or more characters used as delimiters. You can specify a maximum of eight delimiters. You cannot use the semicolon (;) as a delimiter. Do not include spaces between characters.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Specifying Domain and Realm Name Delimiters on page 136• Configuring Domain and Realm Name Usage for Domain Maps on page 136

delimiter (DHCP Relay Agent)

Syntax	<code>delimiter <i>delimiter-character</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay authentication username-include],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p>
Description	Specify the character used as the delimiter between the concatenated components of the username. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.
Options	<i>delimiter-character</i> —Character that separates components that make up the concatenated username. You cannot use the semicolon (;) as a delimiter.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using External AAA Authentication Services with DHCP on page 217 • Creating Unique Usernames for DHCP Clients on page 218

demux

Syntax	<code>demux (destination-address source-address);</code>
Hierarchy Level	<code>[edit services ptsp rule rule-name]</code>
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Specify the IP address used to establish the subscriber context. Subscriber instantiation is always triggered for ingress packets, so this value indicates which IP address in the ingress packets for the flow is used. If the IP address does not correspond to a known subscriber, then a new subscriber context is created. All service rules attached to a given service set must have the same setting.
Options	<p>destination-address—Use the destination IP address field of the ingress packet header for the flow.</p> <p>source-address—Use the source IP address field of the ingress packet header for the flow.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>

destination (Diameter Network Element)

Syntax	<code>destination realm <i>realm-name</i> <host <i>hostname</i>>;</code>
Hierarchy Level	<code>[edit diameter network-element element-name forwarding route dne-route-name]</code>
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Associate the route with all hosts of the specified realm or with a specific host of the specified realm. Together with the function and metric, defines a route reachable through a Diameter network element.
Options	<p>host <i>hostname</i>—(Optional) Name of the destination host associated with the route.</p> <p>realm <i>realm-name</i>—Name of the destination realm associated with the route.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Diameter on page 434 • Configuring Diameter Network Elements on page 437

destination-host

Syntax	<code>destination-host <i>hostname</i></code>
Hierarchy Level	[edit jsrsrc partition <i>partition-name</i>]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Configure the host on which the SAE application resides.
Options	hostname —Host on which the SAE is installed.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring JSRC on page 455• Configuring the JSRC Partition on page 456

destination-host (Gx-Plus)

Syntax	<code>destination-host <i>hostname</i>;</code>
Hierarchy Level	[edit access gx-plus partition <i>partition-name</i>]
Release Information	Statement introduced in Junos OS Release 11.2. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Description	Configure the host on which the PCRF application resides.
Options	hostname —Host on which the PCRF is installed.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Gx-Plus on page 446• Configuring the Gx-Plus Partition on page 447

destination-host (PTSP)

Syntax	<code>destination-host <i>hostname</i>;</code>
Hierarchy Level	[edit system services packet-triggered-subscribers partition <i>partition-name</i>]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Configure the host on which the SAE application resides.
Options	<i>hostname</i> —Host on which the SAE is installed.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the PTSP Partition on page 491

destination-realm (JSRC)

Syntax	<code>destination-realm <i>realm</i></code>
Hierarchy Level	[edit jsrc partition <i>partition-name</i>]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Configure the realm in which the SAE host resides.
Options	<i>realm</i> —Realm in which the SAE host resides.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring JSRC on page 455• Configuring the JSRC Partition on page 456

destination-realm (Gx-Plus)

Syntax	<code>destination-realm <i>realm</i>;</code>
Hierarchy Level	[edit access gx-plus partition <i>partition-name</i>]
Release Information	Statement introduced in Junos OS Release 11.2. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Description	Configure the realm in which the PCRF host resides.
Options	<i>realm</i> —Realm in which the PCRF host resides.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Gx-Plus on page 446• Configuring the Gx-Plus Partition on page 447

destination-realm (PTSP)

Syntax	<code>destination-realm <i>realm</i></code>
Hierarchy Level	[edit system services packet-triggered-subscribers partition <i>partition-name</i>]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Configure the realm in which the SAE host resides.
Options	<i>realm</i> —Realm in which the SAE host resides.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the PTSP Partition on page 491

dhcp-attributes (Address-Assignment Pools)

Syntax `dhcp-attributes {`
 `boot-file filename;`
 `boot-server (address | hostname);`
 `dns-server [ipv6-address];`
 `domain-name domain-name;`
 `grace-period seconds;`
 `maximum-lease-time seconds;`
 `name-server [server-list];`
 `netbios-node-type node-type;`
 `option {`
 `[(id-number option-type option-value)`
 `(id-number array option-type option-value)];`
 `}`
 `option-match {`
 `option-82 {`
 `circuit-id value range named-range;`
 `remote-id value range named-range;`
 `}`
 `}`
 `preferred-lifetime seconds;`
 `router [router-address];`
 `server-identifier ip4-address;`
 `sip-server-address [ipv6-address];`
 `sip-server-domain-name domain-name;`
 `t1-percentage percentage;`
 `t2-percentage percentage;`
 `tftp-server address;`
 `valid-lifetime seconds;`
 `wins-server [servers];`
 `}`

Hierarchy Level `[edit access address-assignment pool pool-name family family]`

Release Information Statement introduced in Junos OS Release 9.0.
 Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description Configure address pools that can be used by different client applications.
 The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
 admin-control—To add this statement to the configuration.

Related Documentation

- [Address-Assignment Pools Overview on page 315](#)
- [DHCP Attributes for Address-Assignment Pools on page 201](#)
- [Configuring Address-Assignment Pools on page 316](#)
- [Configuring DHCP Client-Specific Attributes Applied When Clients Obtain an Address on page 205](#)
- [Configuring a DHCP Server on Switches \(CLI Procedure\)](#)

dhcp-local-server

```
Syntax  dhcp-local-server {
        authentication {
            password password-string;
            username-include {
                circuit-type;
                delimiter delimiter-character;
                domain-name domain-name-string;
                interface-name;
                logical-system-name;
                mac-address;
                option-60;
                option-82 <circuit-id> <remote-id>;
                routing-instance-name;
                user-prefix user-prefix-string;
            }
        }
        dhcpv6 {
            authentication {
                ...
            }
            group group-name {
                authentication {
                    ...
                }
                interface interface-name {
                    exclude;
                    liveness-detection {
                        failure-action (clear-binding | clear-binding-if-interface-up | log-only);
                        method {
                            bfd {
                                version (0 | 1 | automatic);
                                minimum-interval milliseconds;
                                minimum-receive-interval milliseconds;
                                multiplier number;
                                no-adaptation;
                                transmit-interval {
                                    minimum-interval milliseconds;
                                    threshold milliseconds;
                                }
                            }
                            detection-time {
                                threshold milliseconds;
                            }
                        }
                        session-mode (automatic | multihop | singlehop);
                        holddown-interval milliseconds;
                    }
                }
            }
        }
        overrides {
            interface-client-limit number;
            multi-address-embedded-option-response;
            process-inform {
                pool pool-name;
            }
        }
    }
```



```

    }
    rapid-commit;
}
service-profile dynamic-profile-name;
trace;
upto upto-interface-name;
}
overrides {
    delegated-pool;
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
        pool pool-name;
    }
    rapid-commit;
}
route-suppression;
service-profile dynamic-profile-name;
}
liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
        bfd {
            version (0 | 1 | automatic);
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            detection-time {
                threshold milliseconds;
            }
            session-mode (automatic | multihop | singlehop);
            holddown-interval milliseconds;
        }
    }
}
}
overrides {
    delegated-pool;
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
        pool pool-name;
    }
    rapid-commit;
}
reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    timeout timeout-value;
    token token-value;
    trigger {

```

```

        radius-disconnect;
    }
}
route-suppression;
service-profile dynamic-profile-name;
}
duplicate-clients-in-subnet (incoming-interface | option-82);
dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
    primary-profile-name>;
forward-snooped-clients (all-interfaces | configured-interfaces |
    non-configured-interfaces);
group group-name {
    authentication {
        ...
    }
}
dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
    primary-profile-name>;
interface interface-name {
    exclude;
    liveness-detection {
        failure-action (clear-binding | clear-binding-if-interface-up | log-only);
        method {
            bfd {
                version (0 | 1 | automatic);
                minimum-interval milliseconds;
                minimum-receive-interval milliseconds;
                multiplier number;
                no-adaptation;
                transmit-interval {
                    minimum-interval milliseconds;
                    threshold milliseconds;
                }
                detection-time {
                    threshold milliseconds;
                }
                session-mode (automatic | multihop | singlehop);
                holddown-interval milliseconds;
            }
        }
    }
}
}
overrides {
    client-discover-match (option60-and-option82 | incoming-interface);
    include-option-82 {
        forcerenew;
        nak;
    }
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
}
service-profile dynamic-profile-name;
trace;
upto upto-interface-name;
}
overrides {

```

```

    client-discover-match (option60-and-option82 | incoming-interface);
    include-option-82 {
        forcerenew;
        nak;
    }
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
}
requested-ip-network-match subnet-mask
route-suppression;
service-profile dynamic-profile-name;
}
liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
        bfd {
            version (0 | 1 | automatic);
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            detection-time {
                threshold milliseconds;
            }
            session-mode (automatic | multihop | singlehop);
            holddown-interval milliseconds;
        }
    }
}
overrides {
    client-discover-match (option60-and-option82 | incoming-interface);
    include-option-82 {
        forcerenew;
        nak;
    }
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
}
pool-match-order {
    external-authority;
    ip-address-first;
    option-82;
}
reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    timeout timeout-value;
}

```

```

    token token-value;
    trigger {
        radius-disconnect;
    }
}
requested-ip-network-match subnet-mask;
route-suppression;
service-profile dynamic-profile-name;
}

```

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services],
 [edit logical-systems *logical-system-name* system services],
 [edit routing-instances *routing-instance-name* system services],
 [edit system services]

Release Information Statement introduced in Junos OS Release 9.0.
 Statement introduced in Junos OS Release 12.1 for EX Series switches.
 Statement introduced in Junos OS Release 13.2X51 for the QFX Series.
 Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Configure Dynamic Host Configuration Protocol (DHCP) local server options on the router or switch and enable the router or switch to function as an extended DHCP local server. The DHCP local server receives DHCP request and reply packets from DHCP clients and then responds with an IP address and other optional configuration information to the client.

The DHCP local server and the DHCP/BOOTP relay server, which are configured under the **[edit forwarding-options helpers]** hierarchy level, cannot both be enabled on the router or switch at the same time. The extended DHCP local server is fully compatible with the extended DHCP relay feature.

The **dhcpx6** stanza configures the router or switch to support Dynamic Host Configuration Protocol for IPv6 (DHCPv6). The DHCPv6 local server is fully compatible with the extended DHCP local server and the extended DHCP relay feature.



NOTE: When you configure the **dhcp-local-server** statement at the routing instance hierarchy level, you must use a routing instance type of **virtual-router**.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

Related Documentation

- [Extended DHCP Local Server Overview on page 188](#)
- [DHCPv6 Local Server Overview on page 287](#)
- [Configuring a DHCP Server on Switches \(CLI Procedure\)](#)

dhcp-relay

```
Syntax  dhcp-relay {
    active-server-group server-group-name;
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
            domain-name domain-name-string;
            interface-name;
            logical-system-name;
            mac-address;
            option-60;
            option-82 <circuit-id> <remote-id>;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
    dhcpv6 {
        active-server-group server-group-name;
        authentication {
            password password-string;
            username-include {
                circuit-type;
                client-id;
                delimiter delimiter-character;
                domain-name domain-name-string;
                interface-name;
                logical-system-name;
                relay-agent-interface-id;
                relay-agent-remote-id;
                relay-agent-subscriber-id;
                routing-instance-name;
                user-prefix user-prefix-string;
            }
        }
        dynamic-profile profile-name {
            aggregate-clients (merge | replace);
            use-primary primary-profile-name;
        }
        group group-name {
            active-server-group server-group-name;
            authentication {
                ...
            }
            dynamic-profile profile-name {
                ...
            }
            interface interface-name {
                exclude;
                liveness-detection {
                    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
                    method {

```

```
bfd {
  version (0 | 1 | automatic);
  minimum-interval milliseconds;
  minimum-receive-interval milliseconds;
  multiplier number;
  no-adaptation;
  transmit-interval {
    minimum-interval milliseconds;
    threshold milliseconds;
  }
  detection-time {
    threshold milliseconds;
  }
  session-mode(automatic | multihop | singlehop);
  holddown-interval milliseconds;
}
}
}
overrides {
  ...
}
relay-option {
  ...
}
service-profile dynamic-profile-name;
trace;
upto upto-interface-name;
}
route-suppression:
service-profile dynamic-profile-name;
overrides {
  ...
}
relay-agent-interface-id {
  ...
}
relay-agent-remote-id {
  ...
}
relay-option {
  ...
}
route-suppression;
server-response-time seconds;
service-profile dynamic-profile-name;
}
liveness-detection {
  failure-action (clear-binding | clear-binding-if-interface-up | log-only);
  method {
    bfd {
      version (0 | 1 | automatic);
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      transmit-interval {
```

```

        minimum-interval milliseconds;
        threshold milliseconds;
    }
    detection-time {
        threshold milliseconds;
    }
    session-mode(automatic | multihop | singlehop);
    holddown-interval milliseconds;
}
}
}
overrides {
    allow-snooped-clients;
    delay-authentication;
    interface-client-limit number;
    no-allow-snooped-clients;
    no-bind-on-request;
    send-release-on-delete;
}
relay-agent-interface-id {
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82;
}
relay-agent-remote-id {
    prefix prefix;
    use-interface-description (logical | device);
}
server-group {
    server-group-name {
        server-ip-address;
    }
}
duplicate-clients-in-subnet (incoming-interface | option-82):
dynamic-profile profile-name {
    aggregate-clients (merge | replace);
    use-primary primary-profile-name;
}
forward-snooped-clients (all-interfaces | configured-interfaces |
non-configured-interfaces);
group group-name {
    active-server-group server-group-name;
    authentication {
        ...
    }
    dynamic-profile profile-name {
        ...
    }
    interface interface-name {
        exclude;
        liveness-detection {
            failure-action (clear-binding | clear-binding-if-interface-up | log-only);
            method {
                bfd {
                    version (0 | 1 | automatic);
                    minimum-interval milliseconds;

```

```

        minimum-receive-interval milliseconds;
        multiplier number;
        no-adaptation;
        transmit-interval {
            minimum-interval milliseconds;
            threshold milliseconds;
        }
        detection-time {
            threshold milliseconds;
        }
        session-mode(automatic | multihop | singlehop);
        holddown-interval milliseconds;
    }
}
overrides {
    ...
}
service-profile dynamic-profile-name;
trace;
upto upto-interface-name;
}
overrides {
    ...
}
relay-option {
    ...
}
relay-option-82 {
    ...
}
route-suppression:
service-profile dynamic-profile-name;
}
liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
        bfd {
            version (0 | 1 | automatic);
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            detection-time {
                threshold milliseconds;
            }
            session-mode(automatic | multihop | singlehop);
            holddown-interval milliseconds;
        }
    }
}
overrides {

```



```

allow-snooped-clients;
always-write-giaddr;
always-write-option-82;
client-discover-match (option60-and-option82 | incoming-interface);
delay-authentication;
disable-relay;
interface-client-limit number;
layer2-unicast-replies;
no-allow-snooped-clients;
no-bind-on-request;
proxy-mode;
replace-ip-source-with;
send-release-on-delete;
trust-option-82;
}
relay-option {
  option-number option-number;
  default-action {
    drop;
    forward-only;
    relay-server-group group-name;
  }
  equals (ascii ascii-string | hexadecimal hexadecimal-string) {
    drop;
    forward-only;
    relay-server-group relay-server-group;
  }
  starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
    drop;
    forward-only;
    local-server-group local-server-group;
    relay-server-group relay-server-group;
  }
}
}
relay-option-82 {
  circuit-id {
    prefix prefix;
    use-interface-description (logical | device);
  }
  remote-id {
    prefix prefix;
    use-interface-description (logical | device);
  }
}
}
server-group {
  server-group-name {
    server-ip-address;
  }
}
}
route-suppression:
server-response-time seconds;
service-profile dynamic-profile-name;
}

```

Hierarchy Level	[edit forwarding-options], [edit logical-systems <i>logical-system-name</i> forwarding-options], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options], [edit routing-instances <i>routing-instance-name</i> forwarding-options]
Release Information	Statement introduced in Junos OS Release 8.3. Statement introduced in Junos OS Release 12.1 for EX Series switches. Statement introduced in Junos OS Release 13.2X51 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	<p>Configure extended Dynamic Host Configuration Protocol (DHCP) relay and DHCPv6 relay options on the router or switch and enable the router (or switch) to function as a DHCP relay agent. A DHCP relay agent forwards DHCP request and reply packets between a DHCP client and a DHCP server.</p> <p>DHCP relay supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide subscriber authentication or client authentication. You can attach dynamic profiles and configure authentication support on a global basis or for a specific group of interfaces.</p> <p>The extended DHCP and DHCPv6 relay agent options configured with the dhcp-relay and dhcpv6 statements are incompatible with the DHCP/BOOTP relay agent options configured with the bootp statement. As a result, the extended DHCP or DHCPv6 relay agent and the DHCP/BOOTP relay agent cannot both be enabled on the router (or switch) at the same time.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Extended DHCP Relay Agent Overview on page 194• DHCPv6 Relay Agent Overview• DHCP Relay Proxy Overview on page 197• Using External AAA Authentication Services with DHCP on page 217

dhcpv6 (DHCP Local Server)

```
Syntax  dhcpv6 {
    authentication {
        password password-string;
        username-include {
            circuit-type;
            client-id;
            delimiter delimiter-character;
            domain-name domain-name-string;
            logical-system-name;
            relay-agent-interface-id;
            relay-agent-remote-id;
            relay-agent-subscriber-id;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
    group group-name {
        authentication {
            ...
        }
        interface interface-name {
            exclude;
            liveness-detection {
                failure-action (clear-binding | clear-binding-if-interface-up | log-only);
                method {
                    bfd {
                        version (0 | 1 | automatic);
                        minimum-interval milliseconds;
                        minimum-receive-interval milliseconds;
                        multiplier number;
                        no-adaptation;
                        transmit-interval {
                            minimum-interval milliseconds;
                            threshold milliseconds;
                        }
                        detection-time {
                            threshold milliseconds;
                        }
                    }
                    session-mode (automatic | multihop | singlehop);
                    holddown-interval milliseconds;
                }
            }
        }
    }
    overrides {
        include-option-82;
        interface-client-limit number;
        multi-address-embedded-option-response;
        process-inform {
            pool pool-name;
        }
        rapid-commit;
    }
    service-profile dynamic-profile-name;
}
```

```

    trace;
    upto upto-interface-name;
}
overrides {
    delegated-pool;
    include-option-82;
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
        pool pool-name;
    }
    rapid-commit;
}
route-suppression;
service-profile dynamic-profile-name;
}
liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
        bfd {
            version (0 | 1 | automatic);
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            detection-time {
                threshold milliseconds;
            }
            session-mode (automatic | multihop | singlehop);
            holddown-interval milliseconds;
        }
    }
}
overrides {
    delegated-pool;
    include-option-82;
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
        pool pool-name;
    }
    rapid-commit;
    reconfigure {
        attempts attempt-count;
        clear-on-abort;
        strict;
        timeout timeout-value;
        token token-value;
        trigger {
            radius-disconnect;
        }
    }
}

```

```

}
reconfigure {
  attempts attempt-count;
  clear-on-abort;
  strict;
  timeout timeout-value;
  token token-value;
  trigger {
    radius-disconnect;
  }
}
requested-ip-network-match subnet-mask;
route-suppression;
service-profile dynamic-profile-name;
}

```

Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server],</p> <p>[edit system services dhcp-local-server]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 12.3 for EX Series switches.</p>
Description	<p>Configure DHCPv6 local server options on the router or switch and enable the router or switch to function as a server for the DHCP protocol for IP version 6 (IPv6). The DHCPv6 local server sends and receives packets using the IPv6 protocol and informs IPv6 of the routing requirements of router clients. The local server works together with the AAA service framework to control subscriber access (or DHCP client access) and accounting.</p> <p>The DHCPv6 local server is fully compatible with the extended DHCP local server and DHCP relay agent.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • DHCPv6 Local Server Overview on page 287

dhcpx6 (DHCP Relay Agent)

```
Syntax dhcpx6 {
    active-server-group server-group-name;
    authentication {
        password password-string;
        username-include {
            circuit-type;
            client-id;
            delimiter delimiter-character;
            domain-name domain-name-string;
            logical-system-name;
            relay-agent-interface-id;
            relay-agent-remote-id;
            relay-agent-subscriber-id;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
    dynamic-profile profile-name {
        aggregate-clients (merge | replace);
        use-primary primary-profile-name;
    }
    group group-name {
        active-server-group server-group-name;
        authentication {
            ...
        }
        dynamic-profile profile-name {
            ...
        }
    }
    interface interface-name {
        exclude;
        liveness-detection {
            failure-action (clear-binding | clear-binding-if-interface-up | log-only);
            method {
                bfd {
                    version (0 | 1 | automatic);
                    minimum-interval milliseconds;
                    minimum-receive-interval milliseconds;
                    multiplier number;
                    no-adaptation;
                    transmit-interval {
                        minimum-interval milliseconds;
                        threshold milliseconds;
                    }
                    detection-time {
                        threshold milliseconds;
                    }
                }
                session-mode (automatic | multihop | singlehop);
                holddown-interval milliseconds;
            }
        }
    }
}
```

```

    overrides {
        ...
    }
    service-profile dynamic-profile-name;
    trace;
    upto upto-interface-name;
}
}
overrides {
    ...
}
relay-agent-interface-id {
    ...
}
relay-agent-remote-id {
    ...
}
relay-option {
    ...
}
route-suppression;
service-profile dynamic-profile-name;
}
liveness-detection {
    ...
}
}
overrides {
    allow-snooped-clients;
    delay-authentication;
    interface-client-limit number;
    no-allow-snooped-clients;
    no-bind-on-request;
    send-release-on-delete;
}
relay-agent-interface-id {
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82;
}
relay-agent-remote-id {
    prefix prefix;
    use-interface-description (logical | device);
}
relay-option {
    option-number option-number;
    default-action {
        drop;
        forward-only;
        relay-server-group relay-server-group;
    }
}
equals (ascii ascii-string | hexadecimal hexadecimal-string) {
    drop;
    forward-only;
    relay-server-group relay-server-group;
}
starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {

```

```

    drop;
    forward-only;
    relay-server-group relay-server-group;
  }
}
server-group {
  server-group-name {
    server-ip-address;
  }
}
route-suppression;
server-response-time seconds;
service-profile dynamic-profile-name;
}

```

Hierarchy Level [edit forwarding-options dhcp-relay],
 [edit logical-systems *logical-system-name* forwarding-options **dhcp-relay**],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*
 forwarding-options dhcp-relay],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay]

Release Information Statement introduced in Junos OS Release 11.4.
 Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description Configure DHCPv6 relay options on the router or switch and enable the router or switch to function as a DHCPv6 relay agent. A DHCPv6 relay agent forwards DHCPv6 request and reply packets between a DHCPv6 client and a DHCPv6 server.

The DHCPv6 relay agent server is fully compatible with the extended DHCP local server and DHCP relay agent. However, the options configured with the **dhcpv6** statement are incompatible with the DHCP/BOOTP relay agent options configured with the **bootp** statement. As a result, the DHCPv6 relay agent and the DHCP/BOOTP relay agent cannot be enabled on the router or switch at the same time.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Documentation

- [dhcp-relay on page 689](#)
- [DHCPv6 Relay Agent Overview](#)
- [Using External AAA Authentication Services with DHCP on page 217](#)

diameter

```
Syntax diameter {
    network-element element-name {
        forwarding {
            route dne-route-name {
                destination realm realm-name <host hostname>;
                function function-name <partition partition-name>;
                metric route-metric;
            }
        }
        function function-name;
        peer peer-name {
            priority priority-number;
        }
    }
    origin {
        host hostname;
        realm realm-name;
    }
    peer peer-name {
        address ip-address;
        connect-actively {
            port port-number;
            transport transport-name;
        }
        logical-system logical-system-name <routing-instance routing-instance-name>;
        routing-instance routing-instance-name;
    }
    transport transport-name {
        address;
        logical-system logical-system-name <routing-instance routing-instance-name>;
        routing-instance routing-instance-name;
    }
}
```

Hierarchy Level [\[edit\]](#)

Release Information Statement introduced in Junos OS Release 9.6.

Description Configure the Diameter base protocol for subscriber management.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- [Configuring Diameter on page 434](#)

diameter-instance (JSRC)

Syntax	diameter-instance <i>instance-name</i>
Hierarchy Level	[edit jsrc partition <i>partition-name</i>]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Specify the Diameter instance associated with the JSRC partition.
Options	<i>instance-name</i> —Name of the Diameter instance. Currently, only master is supported.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring JSRC on page 455• Configuring the JSRC Partition on page 456

diameter-instance (Gx-Plus)

Syntax	diameter-instance <i>instance-name</i> ;
Hierarchy Level	[edit access gx-plus partition <i>partition-name</i>]
Release Information	Statement introduced in Junos OS Release 11.2. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Description	Specify the Diameter instance associated with the Gx-Plus partition.
Options	<i>instance-name</i> —Name of the Diameter instance. Currently, only master is supported.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Gx-Plus on page 446• Configuring the Gx-Plus Partition on page 447

diameter-instance (PTSP)

Syntax	<code>diameter-instance <i>instance-name</i></code>
Hierarchy Level	[edit system services packet-triggered-subscribers partition <i>partition-name</i>]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Specify the Diameter instance associated with the PTSP partition.
Options	<i>instance-name</i> —Name of the Diameter instance. Currently, only master is supported.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring the PTSP Partition on page 491

disable

Syntax	<code>disable <i>service-name</i>;</code>
Hierarchy Level	[edit services service-set <i>services-set-name</i> subscriber-profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Disable the service name of the subscriber profile.
Options	<i>service-name</i> —Name of the disabled service.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

disable-relay

Syntax	<code>disable-relay;</code>
Hierarchy Level	[edit forwarding-options dhcp-relay overrides], [edit forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]
Release Information	Statement introduced in Junos OS Release 8.3. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Disable DHCP relay on specific interfaces in a group.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Extended DHCP Relay Agent Overview on page 194

dns-server

Syntax	<code>dns-server <i>ipv6-address</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet6 dhcp-attributes]
Release Information	Statement introduced in Junos OS Release 10.0.
Description	Specify a DNS server to which clients can send DNS queries. This is equivalent to DHCPv6 option 23. To specify multiple DNS servers, add multiple dns-server statements in order of preference.
Options	<i>ipv6-address</i> —IPv6 address of a DNS server.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Address-Assignment Pools Overview on page 315• Configuring Address-Assignment Pools on page 316

domain (Domain Map)

```
Syntax  domain {
        delimiter [delimiter-character];
        map domain-map-name {
            aaa-logical-system logical-system-name {
                aaa-routing-instance routing-instance-name;
            }
            aaa-routing-instance routing-instance-name;
            access-profile profile-name;
            address-pool pool-name;
            dynamic-profile profile-name;
            padn destination-address {
                mask destination-mask;
                metric route-metric;
            }
            strip-domain;
            target-logical-system logical-system-name {
                target-routing-instance routing-instance-name;
            }
            target-routing-instance routing-instance-name;
            tunnel-profile profile-name;
        }
        parse-direction (left-to-right | right-to-left);
        parse-order (domain-first | realm-first);
        realm-delimiter [delimiter-character];
        realm-parse-direction (left-to-right | right-to-left);
    }
```

Hierarchy Level [edit access]

Release Information Statement introduced in Junos OS Release 10.4.

Description Configure a domain map, which is used to map access options and session parameters for subscriber sessions.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- [Configuring a Domain Map on page 131](#)

domain-name (DHCP Local Server)

Syntax	<code>domain-name <i>domain-name-string</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit system services dhcp],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server group group-name authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify the domain name that is concatenated with the username during the subscriber authentication or DHCP client authentication process.
Options	<i>domain-name-string</i> —Domain name formatted string.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

- Related Documentation**
- [Using External AAA Authentication Services with DHCP on page 217](#)

domain-name (DHCP Relay Agent)

Syntax	<code>domain-name <i>domain-name-string</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay authentication username-include],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p>
Description	Specify the domain name that is concatenated with the username during the subscriber authentication or client authentication process. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.
Options	<i>domain-name-string</i> —Domain name formatted string.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using External AAA Authentication Services with DHCP on page 217 • Creating Unique Usernames for DHCP Clients on page 218

domain-name (Address-Assignment Pools)

Syntax	<code>domain-name <i>domain-name</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	Configure the name of the domain in which clients search for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified. This is equivalent to DHCP option 15.
Options	<i>domain-name</i> —Name of the domain.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Address-Assignment Pools on page 316

domain-name (Static Subscribers)

Syntax	<code>domain-name <i>domain-name</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers authentication username-include],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication username-include],</p> <p>[edit system services static-subscribers authentication username-include],</p> <p>[edit system services static-subscribers group <i>group-name</i> authentication username-include]</p>
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Specify the domain name that is included at the end of the username created for all static subscribers or for the static subscribers in a specified group. The group version of the statement takes precedence over the global version.
Options	<p><i>domain-name</i>—Domain name that ends the username created for all static subscribers. The username is also sent to RADIUS in the Access-Request message. The string can include the following characters: a through z, A through Z, 0 through 9, “-”, or “.”.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Subscribers over Static Interfaces on page 466• Configuring the Static Subscriber Global Username on page 473• Configuring the Static Subscriber Group Username on page 478

domain-name-server (Routing Instances and Access Profiles)


Syntax	<code>domain-name-server <i>dns-address</i>;</code>
Hierarchy Level	[edit access], [edit access <i>profile</i>]
Release Information	Statement introduced in Junos OS Release 12.3. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Description	Configure an IPv4 address for a DNS name server. You can configure an address globally for a routing instance at the [edit access] hierarchy level or for an access profile at the [edit access <i>profile profile-name</i>] hierarchy level. You can configure more than one address by including the statement multiple times.



NOTE: A DNS name server address configured with this statement is lower in preference than one configured with the `domain-name-server-inet` statement.

Options	<i>dns-address</i> —IPv4 address of the DNS name server.
Required Privilege Level	admin—To view this statement in the configuration admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring DNS Name Server Addresses for Subscriber Management on page 325 • DNS Name Server Address Overview

domain-name-server-inet (Routing Instances and Access Profiles)

Syntax	domain-name-server-inet <i>dns-address</i> ;
Hierarchy Level	[edit access], [edit access <i>profile</i>]
Release Information	Statement introduced in Junos OS Release 12.3. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Description	Configure an IPv4 address for a DNS name server. You can configure an address globally for a routing instance at the [edit access] hierarchy level or for an access profile at the [edit access <i>profile profile-name</i>] hierarchy level. You can configure more than one address by including the statement multiple times.
<div> NOTE: A DNS name server address configured with this statement is higher in preference than one configured with the domain-name-server statement.</div>	
Options	<i>dns-address</i> —IPv4 address of the DNS name server.
Required Privilege Level	admin—To view this statement in the configuration admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring DNS Name Server Addresses for Subscriber Management on page 325• DNS Name Server Address Overview

domain-name-server-inet6 (Routing Instances and Access Profiles)

Syntax	<code>domain-name-server-inet6 <i>dns-address</i>;</code>
Hierarchy Level	[edit access], [edit access <i>profile</i>]
Release Information	Statement introduced in Junos OS Release 12.3. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Description	Configure an IPv6 address for a DNS name server. You can configure an address globally for a routing instance at the [edit access] hierarchy level or for an access profile at the [edit access <i>profile profile-name</i>] hierarchy level. You can configure more than one address by including the statement multiple times.
Options	<i>dns-address</i> —IPv6 address of the DNS name server.
Required Privilege Level	admin—To view this statement in the configuration admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring DNS Name Server Addresses for Subscriber Management on page 325• <i>DNS Name Server Address Overview</i>

downstream-rate (Traffic Shaping)

Syntax	<code>downstream-rate rate;</code>
Hierarchy Level	<code>[edit dynamic-profiles <i>profile-name</i> interfaces \$junos-interface-ifd-name unit \$junos-interface-unit advisory-options],</code> <code>[edit dynamic-profiles <i>profile-name</i> interfaces interface-set \$junos-interface-set-name interface \$junos-interface-ifd-name advisory-options],</code> <code>[edit interfaces demux0 unit <i>logical-unit-number</i> advisory-options],</code> <code>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> advisory-options]</code>
Release Information	Statement introduced in Junos OS Release 11.4. Support at the <code>[edit interfaces demux0 ...]</code> hierarchy level introduced in Junos OS Release 12.2. Support at the <code>[edit dynamic-profiles ...]</code> hierarchy level introduced in Junos OS Release 13.1.
Description	<p>Specify a recommended shaping rate to be applied to downstream traffic on an interface.</p> <p>For ANCP interfaces, this configured rate is used as the default value for the Juniper VSA Downstream-Calculated-Qos-Rate (26–141) when the router has not received and processed the attributes from the access node.</p> <p>For L2TP, the rate is configured on an underlying PPPoE logical interface for a subscriber on an MX Series router acting as a LAC. When the subscriber is tunneled, this rate, referred to as speed for L2TP, is sent to the LNS in the ICCN message as AVP 24.</p>
Options	rate —Traffic rate in bits per second. Range: 1000 through 4,294,967,295 bits per second
Required Privilege Level	interface —To view this statement in the configuration. interface-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Setting a Recommended Shaping Rate for Traffic on ANCP Interfaces on page 400• Configuring the ANCP Agent on page 368• Configuring the Method to Set the LAC Connection Speeds to the LNS

drop (DHCP Relay Agent Option)

Syntax	drop;
Hierarchy Level	[edit forwarding-options dhcp-relay relay-option (default-action equals starts-with)], [edit forwarding-options dhcp-relay dhcpv6 relay-option (default-action equals starts-with)], [edit forwarding-options dhcp-relay group <i>group-name</i> relay-option (default-action equals starts-with)], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> relay-option (default-action equals starts-with)], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...]
Release Information	Statement introduced in Junos OS Release 12.3.
Description	Drop (discard) specified DHCP client packets when you use DHCP relay agent selective processing. You can configure the drop operation globally or for a group of interfaces, and for either DHCP or DHCPv6 relay agent.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Using DHCP Option Information to Selectively Process DHCP Client Traffic on page 273

duplication (Access Profile)

Syntax	duplication;
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Configure the router to send accounting reports to both the RADIUS accounting server configured in the access profile for the wholesaler and the RADIUS accounting server configured in the access profile for the retailer.
Default	The router sends accounting reports to the accounting servers that are in the context in which the subscriber is authenticated.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Authentication and Accounting Parameters for Subscriber Access on page 80 • Understanding RADIUS Accounting Duplicate Reporting on page 87

duplication-vrf (Duplicate Accounting)

Syntax	<pre>duplication-vrf { access-profile-name <i>profile-name</i>; vrf-name <i>vrf-name</i>; }</pre>
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in Junos OS Release 12.3R3 and supported in later 12.3Rx releases. Statement supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)
Description	<p>Configure the router to send duplicate accounting information to the RADIUS accounting servers defined in up to five access profiles all in the same nondefault VRF (LS:RI combination).</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding RADIUS Accounting Duplicate Reporting on page 87• Configuring Authentication and Accounting Parameters for Subscriber Access on page 80

dynamic-profile (DHCP Local Server)

Syntax	<pre>dynamic-profile <i>profile-name</i> { aggregate-clients (merge replace); use-primary <i>primary-profile-name</i>; }</pre>
Hierarchy Level	<pre>[edit system services dhcp-local-server], [edit system services dhcp-local-server dhcpv6], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i>], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>], [edit system services dhcp-local-server group <i>group-name</i>], [edit system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...]</pre>
Release Information	<p>Statement introduced in Junos OS Release 9.2.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Options aggregate-clients and use-primary introduced in Junos OS Release 9.3.</p> <p>Support at the [edit ... interface] hierarchy levels introduced in Junos OS Release 11.2.</p>
Description	Specify the dynamic profile that is attached to all interfaces, a named group of interfaces, or a specific interface.
Options	<p><i>profile-name</i>—Name of the dynamic profile.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces • Configuring a Default Subscriber Service on page 200


dynamic-profile (DHCP Relay Agent)

Syntax	<pre>dynamic-profile <i>profile-name</i> { aggregate-clients (merge replace); use-primary <i>primary-profile-name</i>; }</pre>
Hierarchy Level	<pre>[edit forwarding-options dhcp-relay], [edit forwarding-options dhcp-relay dhcpv6], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i>], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> interface <i>interface-name</i>], [edit forwarding-options dhcp-relay group <i>group-name</i>], [edit forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...]</pre>
Release Information	<p>Statement introduced in Junos OS Release 9.2.</p> <p>Support at the <code>[edit ... dhcpv6]</code> hierarchy levels introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	<p>Specify the dynamic profile that is attached to all interfaces, to a named group of interfaces, or to a specific interface.</p> <p>M120 and M320 routers do not support DHCPv6.</p>
Options	<p><i>profile-name</i>—Name of the dynamic profile.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• dhcp-relay on page 689• Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces• Grouping Interfaces with Common DHCP Configurations on page 223• Configuring a Default Subscriber Service on page 200

dynamic-profile (Domain Map)

Syntax	<code>dynamic-profile <i>profile-name</i>;</code>
Hierarchy Level	[edit access domain map <i>domain-map-name</i>]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Dynamic profile that is used for subscriber sessions associated with the domain map.
Options	<i>profile-name</i> —Name of dynamic profile.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Specifying a Dynamic Profile in a Domain Map on page 133

dynamic-profile (Static Subscribers)

Syntax	<code>dynamic-profile <i>profile-name</i> { <i>aggregate-clients</i> (merge replace); }</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services <i>static-subscribers</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers <i>group group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services <i>static-subscribers</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers <i>group group-name</i>],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services <i>static-subscribers</i>],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers <i>group group-name</i>],</p> <p>[edit system services <i>static-subscribers</i>],</p> <p>[edit system services static-subscribers <i>group group-name</i>]</p>
Release Information	Statement introduced in Junos OS Release 9.6.
Description	<p>Specify the dynamic client profile that is instantiated at login and de-instantiated at logout for all static subscribers on interfaces configured at the [edit system services static-subscribers interface] hierarchy level or for the static subscribers in a specific group. The group version of the statement takes precedence over the global version.</p>
<div>  NOTE: Do not specify a dynamic profile that creates a dynamic interface. </div>	
Default	By default, the <i>junos-default-profile</i> is used when you do not specify a global dynamic profile with this statement.
Options	<p><i>profile-name</i>—Name of the dynamic client profile profile.</p> <p>The remaining statement is explained separately.</p>
Required Privilege Level	<p>access—To view this statement in the configuration.</p> <p>access-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Subscribers over Static Interfaces on page 466 • Specifying the Static Subscriber Global Dynamic Profile on page 471 • Specifying the Static Subscriber Group Dynamic Profile on page 476


enable

Syntax	<code>enable <i>service-name</i> { concurrent-data-sessions <i>max-session-number</i>; }</code>
Hierarchy Level	[edit services service-set <i>services-set-name</i> subscriber-profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Enable the service name for the subscriber profile.
Options	<i>service-name</i> —Name of the enabled service. The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

equals (DHCP Relay Agent)

Syntax	<pre>equals (ascii <i>ascii-string</i> hexadecimal <i>hexadecimal-string</i>) { drop; forward-only; local-server-group <i>local-server-group</i>; relay-server-group <i>relay-server-group</i>; }</pre>
Hierarchy Level	<pre>[edit forwarding-options dhcp-relay <i>relay-option</i>], [edit forwarding-options dhcp-relay dhcpv6 <i>relay-option</i>], [edit forwarding-options dhcp-relay group <i>group-name</i> <i>relay-option</i>], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> <i>relay-option</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...]</pre>
Release Information	Statement introduced in Junos OS Release 12.3.
Description	<p>Configure the exact match criteria used with the DHCP relay agent selective processing feature. DHCP relay agent compares the configured match string with the option-specific string received in DHCP client packets. If there is an exact left-to-right match, DHCP performs the action you define for the match criteria.</p> <p>You can configure an unlimited number of match strings. Match strings do not support wildcard attributes.</p> <p>The local-server-group option is not supported for DHCPv6 relay agent.</p>
Options	<p><i>ascii-string</i>—ASCII string of 1 through 255 alphanumeric characters.</p> <p><i>hexadecimal-string</i>—Hexadecimal string of 1 through 255 hexadecimal characters (0 through 9, a through f, A through F).</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Using DHCP Option Information to Selectively Process DHCP Client Traffic on page 273

ethernet-port-type-virtual

Syntax	ethernet-port-type-virtual;
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	Specify the physical port type the router or switch uses to authenticate clients. The router or switch passes a port type of ethernet in RADIUS attribute 61 (NAS-Port-Type) by default. This statement specifies a port type of virtual .
<div>  NOTE: This statement takes precedence over the nas-port-type statement if you include both statements in the same access profile. </div>	
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring RADIUS Server Options for Subscriber Access on page 102 • Configuring RADIUS Server Parameters for Subscriber Access on page 102

exceed-action

Syntax	<pre>exceed-action { drop; syslog; }</pre>
Hierarchy Level	[edit services service-set <i>services-set-name</i> subscriber-profile <i>profile-name</i> max-data-sessions-per-subscriber]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Specify the action if the maximum data sessions per subscriber exceed the maximum limit. You must also specify the drop rate of the packets for drop and system log details for syslog .
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

exclude (RADIUS)

Syntax `exclude {`

- `acc-aggr-cir-id-asc [access-request | accounting-start | accounting-stop];`
- `acc-aggr-cir-id-bin [access-request | accounting-start | accounting-stop];`
- `acc-loop-cir-id [access-request | accounting-start | accounting-stop];`
- `accounting-authentic [accounting-on | accounting-off];`
- `accounting-delay-time [accounting-on | accounting-off];`
- `accounting-session-id [access-request | accounting-on | accounting-off | accounting-stop];`
- `accounting-terminate-cause [accounting-off];`
- `act-data-rate-dn [access-request | accounting-start | accounting-stop];`
- `act-data-rate-up [access-request | accounting-start | accounting-stop];`
- `act-interlv-delay-dn [access-request | accounting-start | accounting-stop];`
- `act-interlv-delay-up [access-request | accounting-start | accounting-stop];`
- `att-data-rate-dn [access-request | accounting-start | accounting-stop];`
- `att-data-rate-up [access-request | accounting-start | accounting-stop];`
- `called-station-id [access-request | accounting-start | accounting-stop];`
- `calling-station-id [access-request | accounting-start | accounting-stop];`
- `class [accounting-start | accounting-stop];`
- `cos-shaping-rate [accounting-start | accounting-stop];`
- `dhcp-gi-address [access-request | accounting-start | accounting-stop];`
- `dhcp-mac-address [access-request | accounting-start | accounting-stop];`
- `dhcp-options [access-request | accounting-start | accounting-stop];`
- `downstream-calculated-qos-rate [access-request | accounting-start | accounting-stop];`
- `dsl-forum-attributes [access-request | accounting-start | accounting-stop];`
- `dsl-line-state [access-request | accounting-start | accounting-stop];`
- `dsl-type [access-request | accounting-start | accounting-stop];`
- `event-timestamp [accounting-on | accounting-off | accounting-start | accounting-stop];`
- `filter-id [accounting-start | accounting-stop];`
- `framed-ip-address [accounting-start | accounting-stop];`
- `framed-ip-netmask [accounting-start | accounting-stop];`
- `input-filter [accounting-start | accounting-stop];`
- `input-gigapackets [accounting-stop];`
- `input-gigawords [accounting-stop];`
- `interface-description [access-request | accounting-start | accounting-stop];`
- `max-data-rate-dn [access-request | accounting-start | accounting-stop];`
- `max-data-rate-up [access-request | accounting-start | accounting-stop];`
- `max-interlv-delay-dn [access-request | accounting-start | accounting-stop];`
- `max-interlv-delay-up [access-request | accounting-start | accounting-stop];`
- `min-data-rate-dn [access-request | accounting-start | accounting-stop];`
- `min-data-rate-up [access-request | accounting-start | accounting-stop];`
- `min-lp-data-rate-dn [access-request | accounting-start | accounting-stop];`
- `min-lp-data-rate-up [access-request | accounting-start | accounting-stop];`
- `nas-identifier [access-request | accounting-on | accounting-off | accounting-start | accounting-stop];`
- `nas-port [access-request | accounting-start | accounting-stop];`
- `nas-port-id [access-request | accounting-start | accounting-stop];`
- `nas-port-type [access-request | accounting-start | accounting-stop];`
- `output-filter [accounting-start | accounting-stop];`
- `output-gigapackets [accounting-stop];`
- `output-gigawords [accounting-stop];`

`}`


```
    upstream-calculated-qos-rate [ access-request | accounting-start | accounting-stop ];  
}
```

Hierarchy Level [edit access profile *profile-name* radius [attributes](#)]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.
Options **downstream-calculated-qos-rate**, **dsl-forum-attributes**, and
upstream-calculated-qos-rate introduced in Junos OS Release 11.4.
Options **cos-shaping-rate** and **filter-id** introduced in Junos OS Release 13.2.

Description Configure the router or switch to exclude the specified attributes from the specified type of RADIUS message.

Not all attributes are available in all types of RADIUS messages. By default, the router or switch includes the specified attributes in RADIUS Access-Request, Acct-On, Acct-Off, Acct-Start, and Acct-Stop messages.

Options RADIUS attribute type—RADIUS attribute, Juniper Networks (vendor ID 4874) VSA number and name, or DSL Forum (vendor ID 3561) VSA number and name.

- **acc-aggr-cir-id-asc**—Juniper Networks VSA 26-112, Acc-Aggr-Cir-Id-Asc.
- **acc-aggr-cir-id-bin**—Juniper Networks VSA 26-111, Acc-Aggr-Cir-Id-Bin.
- **acc-loop-cir-id**—Juniper Networks VSA 26-110, Acc-Loop-Cir-Id.
- **accounting-authentic**—RADIUS attribute 45, Acct-Authentic.
- **accounting-delay-time**—RADIUS attribute 41, Acct-Delay-Time.
- **accounting-session-id**—RADIUS attribute 44, Acct-Session-Id.
- **accounting-terminate-cause**—RADIUS attribute 49, Acct-Terminate-Cause.
- **act-data-rate-dn**—Juniper Networks VSA 26-114, Act-Data-Rate-Dn
- **act-data-rate-up**—Juniper Networks VSA 26-113, Act-Data-Rate-Up
- **act-interlv-delay-dn**—Juniper Networks VSA 26-126, Act-Interlv-Delay-Dn
- **act-interlv-delay-up**—Juniper Networks VSA 26-124, Act-Interlv-Delay-Up
- **att-data-rate-dn**—Juniper Networks VSA 26-118, Att-Data-Rate-Dn
- **att-data-rate-up**—Juniper Networks VSA 26-117, Att-Data-Rate-Up
- **called-station-id**—RADIUS attribute 30, Called-Station-Id.
- **calling-station-id**—RADIUS attribute 31, Calling-Station-Id.
- **class**—RADIUS attribute 25, Class.
- **cos-shaping-rate**—Juniper Networks VSA 26-177, Cos-Shaping-Rate.
- **dhcp-gi-address**—Juniper Networks VSA 26-57, DHCP-GI-Address.
- **dhcp-mac-address**—Juniper Networks VSA 26-56, DHCP-MAC-Address.
- **dhcp-options**—Juniper Networks VSA 26-55, DHCP-Options.
- **downstream-calculated-qos-rate**—Juniper Networks VSA 26-141
- **dsl-forum-attributes**—DSL Forum VSA (vendor ID 3561) as described in RFC 4679, *DSL Forum Vendor-Specific RADIUS Attributes*
- **dsl-line-state**—Juniper Networks VSA 26-127, DSL-Line-State
- **dsl-type**—Juniper Networks VSA 26-128, DSL-Type
- **event-timestamp**—RADIUS attribute 55, Event-Timestamp.
- **filter-id**—RADIUS attribute 11, Filter-Id.
- **framed-ip-address**—RADIUS attribute 8, Framed-IP-Address.
- **framed-ip-netmask**—RADIUS attribute 9, Framed-IP-Netmask.
- **input-filter**—Juniper Networks VSA 26-10, Ingress-Policy-Name.
- **input-gigapackets**—Juniper Networks VSA 26-42, Acct-Input-Gigapackets.

- **input-gigawords**—RADIUS attribute 52, Acct-Input-Gigawords.
- **interface-description**—Juniper Networks VSA 26-53, Interface-Desc.
- **max-data-rate-dn**—Juniper Networks VSA 26-120, Max-Data-Rate-Dn
- **max-data-rate-up**—Juniper Networks VSA 26-119, Max-Data-Rate-Up
- **max-interlv-delay-dn**—Juniper Networks VSA 26-125, Max-Interlv-Delay-Dn
- **max-interlv-delay-up**—Juniper Networks VSA 26-123, Max-Interlv-Delay-Up
- **min-data-rate-dn**—Juniper Networks VSA 26-116, Min-Data-Rate-Dn
- **min-data-rate-up**—Juniper Networks VSA 26-115, Min-Data-Rate-Up
- **min-lp-data-rate-dn**—Juniper Networks VSA 26-122, Min-Lp-Data-Rate-Dn
- **min-lp-data-rate-up**—Juniper Networks VSA 26-121, Min-Lp-Data-Rate-Up
- **nas-identifier**—RADIUS attribute 32, NAS-Identifier.
- **nas-port**—RADIUS attribute 5, NAS-Port.
- **nas-port-id**—RADIUS attribute 87, NAS-Port-Id.
- **nas-port-type**—RADIUS attribute 61, NAS-Port-Type.
- **output-filter**—Juniper Networks VSA 26-11, Egress-Policy-Name.
- **output-gigapackets**—Juniper Networks VSA 26-43, Acct-Output-Gigapackets.
- **output-gigawords**—RADIUS attribute 53, Acct-Output-Gigawords.
- **upstream-calculated-qos-rate**—Juniper Networks VSA 26-142

RADIUS message type

- **access-request**—RADIUS Access-Accept messages.
- **accounting-off**—RADIUS Accounting-Off messages.
- **accounting-on**—RADIUS Accounting-On messages.
- **accounting-start**—RADIUS Accounting-Start messages.
- **accounting-stop**—RADIUS Accounting-Stop messages.

Required Privilege Level admin—To view this statement in the configuration.
 admin-control—To add this statement to the configuration.

Related Documentation • [Configuring RADIUS Server Parameters for Subscriber Access on page 102](#)

external-authority

Syntax	external-authority;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server pool-match-order], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server pool-match-order], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server pool-match-order], [edit system services dhcp-local-server pool-match-order]
Release Information	Statement introduced in Junos OS Release 10.0. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	<p>Specify that an external authority (for example, RADIUS or Diameter) provides the address assignment.</p> <p>When RADIUS is the external authority, the router uses the Framed-IPv6-Pool attribute (RADIUS attribute 100) to select the pool. When Diameter is the external authority, the router uses the Diameter counterpart of RADIUS Framed-IPv6-Pool attribute.</p>
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 203• Extended DHCP Local Server Overview on page 188• Address-Assignment Pools Overview on page 315

family (Address-Assignment Pools)

Syntax

```
family family {
    dhcp-attributes {
        [protocol-specific attributes]
    }
    host hostname {
        hardware-address mac-address;
        ip-address ip-address;
    }
    network ip-prefix / <prefix-length>;
    prefix ipv6-prefix;
    range range-name {
        high upper-limit;
        low lower-limit;
        prefix-length prefix-length;
    }
}
```

Hierarchy Level [edit access address-assignment **pool** *pool-name*]

Release Information Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description Configure the protocol family for the address-assignment pool.



NOTE: Subordinate statement support depends on the platform. See individual statement topics for more detailed support information.

Options *family*—Protocol family:

- **inet**—Internet Protocol version 4 suite
- **inet6**—Internet Protocol version 6 suite


The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- [Address-Assignment Pools Overview on page 315](#)
- [Configuring Address-Assignment Pools on page 316](#)

forward-only (DHCP Relay Agent Option)

Syntax	forward-only;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay relay-option (default-action equals starts-with)],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 relay-option (default-action equals starts-with)],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> relay-option (default-action equals starts-with)],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> relay-option (default-action equals starts-with)],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay ...],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...]</p>
Release Information	Statement introduced in Junos OS Release 12.3.
Description	Forward specified DHCP client packets, without creating a new subscriber session, when you use DHCP relay selective processing feature. You can configure the forwarding operation globally or for a group of interfaces, and for either DHCP or DHCPv6 relay agent.
<div style="display: flex; align-items: center;">  <p>NOTE: When you use the forward-only action, the only configured overrides operation supported is the trust-option-82 option. DHCP relay agent ignores all other configured overrides options.</p> </div>	
Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Using DHCP Option Information to Selectively Process DHCP Client Traffic on page 273

forward-rule (Configuring)

Syntax	<pre> forward-rule <i>forward-rule-name</i> { term <i>precedence</i> { from { application-groups [<i>application-group-name</i>]; applications [<i>application-name</i>]; local-address <i>address</i> <except>; local-address-range low <i>low-value</i> high <i>high-value</i> <except >; local-prefix-list <i>prefix-list-name</i> <except >; } then { forwarding-instance <i>forwarding-instance</i>; unit-number <i>unit-number</i>; } } } </pre>
Hierarchy Level	[edit services ptsp]
Release Information	Statement introduced in Junos OS Release 10.2. IPv6 support introduced in Junos OS Release 12.2
Description	Specify the forwarding instance for a specific subscriber or set of subscribers based on the IP address, network, or prefix list. The rule match is applied on the input side.
Options	<p><i>forward-rule-name</i>—Identifier for the collection of terms that constitute this rule.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>

forward-rule (Including in Rule)

Syntax	<code>forward-rule <i>forward-rule-name</i>;</code>
Hierarchy Level	<code>[edit services ptsp rule <i>rule-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Identify the forwarding instance for inclusion in a rule.
Options	<i>forward-rule-name</i> —Identifier for the forward rule that specifies the forwarding instance. The remaining statements are explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>

forwarding (Diameter Network Element)

Syntax	<pre>forwarding { route <i>dne-route-name</i> { destination realm <i>realm-name</i> <host <i>hostname</i>>; function <i>function-name</i> <partition <i>partition-name</i>>; metric <i>route-metric</i>; } }</pre>
Hierarchy Level	<code>[edit diameter network-element <i>element-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Define the criteria that specify which destinations are reachable through the Diameter network element. The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Diameter on page 434• Configuring Diameter Network Elements on page 437

from (Forward Rule)

Syntax	<pre> from { application-groups [application-group-name]; applications [application-name]; local-address address <except >; local-address-range low low-value high high-value <except >; local-prefix-list prefix-list-name <except >; } </pre>
Hierarchy Level	[edit services ptsp forward-rule <i>forward-rule-name</i> term <i>precedence</i>]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Specify match conditions for the PTSP term.
Options	<p>For information on match conditions, see the description of firewall filter match conditions in the <i>Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices</i>.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>

from (Rule)

Syntax	<pre>from { application-group-any; application-groups [application-group-name]; applications [application-name]; local-port-range low low-value high high-value; local-ports [value-list]; protocol protocol-number; remote-address address <except >; remote-address-range low low-value high high-value <except >; remote-port-range low low-value high high-value; remote-ports [value-list]; remote-prefix-list prefix-list-name <except >; }</pre>
Hierarchy Level	[edit services ptsp rule <i>rule-name</i> term <i>precedence</i>]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Specify match conditions for the PTSP term.
Options	<p>For information on match conditions, see the description of firewall filter match conditions in the <i>Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices</i>.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>

function (Diameter Network Element)

Syntax	<code>function <i>function-name</i>;</code>
Hierarchy Level	[edit diameter <code>network-element</code> <i>element-name</i>]
Release Information	Statement introduced in Junos OS Release 10.1. Support for PTSP introduced in Junos OS Release 10.2. Support for Gx-Plus introduced in Junos OS Release 11.2.
Description	Specify the application (function) associated with a Diameter network element.
Default	By default, all functions are associated with (supported by) the network element.
Options	<i>function-name</i> —Application (function) associated with the route. Gx-Plus, JSRC, and packet-triggered subscribers are the applications currently supported.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Diameter on page 434• Configuring Diameter Network Elements on page 437

function (Diameter Route)

Syntax	<code>function <i>function-name</i> <partition <i>partition-name</i>>;</code>
Hierarchy Level	[edit diameter network-element <i>element-name</i> forwarding route <i>dne-route-name</i>]
Release Information	Statement introduced in Junos OS Release 9.6. Support for PTSP introduced in Junos OS Release 10.2. Support for Gx-Plus introduced in Junos OS Release 11.2.
Description	Specify the application (function) associated with a destination and metric. Together, these three elements define a route reachable through a Diameter network element.
Default	All functions are associated with the route.
Options	<i>function-name</i> —Application (function) associated with the route. Gx-Plus, JSRC, and packet-triggered-subscribers are the applications currently supported. <i>partition partition-name</i> —(Optional) Partition associated with the application (function).
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Diameter on page 434• Configuring Diameter Network Elements on page 437

global (Gx-Plus)

Syntax	<pre>global { include-ipv6; max-outstanding-requests <i>number</i>; }</pre>
Hierarchy Level	[edit access gx-plus]
Release Information	Statement introduced in Junos OS Release 11.2. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Description	Configure global attributes for the Gx-Plus application. The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Gx-Plus on page 446

grace-period

Syntax	<code>grace-period <i>seconds</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family (inet inet6) dhcp-attributes]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	Configure the amount of time that the client retains the address lease after the lease expires. The address cannot be reassigned to another client during the grace period.
Options	<p><i>seconds</i>—Number of seconds the lease is retained.</p> <p>Range: 0 through 4,294,967,295 seconds</p> <p>Default: 0 (no grace period)</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Address-Assignment Pools on page 316

group (DHCP Local Server)

```
Syntax  group group-name {
        authentication {
            password password-string;
            username-include {
                circuit-type;
                client-id;
                delimiter delimiter-character;
                domain-name domain-name-string;
                logical-system-name;
                mac-address;
                option-60;
                option-82 <circuit-id> <remote-id>;
                relay-agent-interface-id
                relay-agent-remote-id;
                relay-agent-subscriber-id;
                routing-instance-name;
                user-prefix user-prefix-string;
            }
        }
        dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
            primary-profile-name>;
        interface interface-name {
            exclude;
            overrides {
                client-discover-match (option60-and-option82 | incoming-interface);
                interface-client-limit number;
                process-inform {
                    pool pool-name;
                }
                rapid-commit;
            }
            service-profile dynamic-profile-name;
            trace;
            upto upto-interface-name;
        }
        liveness-detection {
            failure-action (clear-binding | clear-binding-if-interface-up | log-only);
            method {
                bfd {
                    version (0 | 1 | automatic);
                    minimum-interval milliseconds;
                    minimum-receive-interval milliseconds;
                    multiplier number;
                    no-adaptation;
                    transmit-interval {
                        minimum-interval milliseconds;
                        threshold milliseconds;
                    }
                }
                detection-time {
                    threshold milliseconds;
                }
            }
            session-mode (automatic | multihop | singlehop);
        }
    }
```

```

        holddown-interval milliseconds;
    }
}
}
overrides {
    client-discover-match (option60-and-option82 | incoming-interface);
    delegated-pool;
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
    rapid-commit;
}
reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    timeout timeout-value;
    token token-value;
    trigger {
        radius-disconnect;
    }
}
route-suppression;
service-profile dynamic-profile-name;
}

```

Hierarchy Level	<p>[edit system services dhcp-local-server],</p> <p>[edit system services dhcp-local-server dhcpv6],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server ...],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.0.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	Configure a group of interfaces that have a common configuration, such as authentication parameters. A group must contain at least one interface.
Options	<p><i>group-name</i>—Name of the group.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

**Related
Documentation**

- [Extended DHCP Local Server Overview on page 188](#)
- [Grouping Interfaces with Common DHCP Configurations on page 223](#)
- [Using External AAA Authentication Services with DHCP on page 217](#)
- *Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*
- *Configuring a DHCP Server on Switches (CLI Procedure)*

group (DHCP Relay Agent)

```
Syntax  group group-name {
    active-server-group server-group-name;
    authentication {
        password password-string;
        username-include {
            circuit-type;
            client-id;
            delimiter delimiter-character;
            domain-name domain-name-string;
            logical-system-name;
            mac-address;
            option-60;
            option-82 [circuit-id] [remote-id];
            relay-agent-interface-id;
            relay-agent-remote-id;
            relay-agent-subscriber-id;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
    dynamic-profile profile-name {
        aggregate-clients (merge | replace);
        use-primary primary-profile-name;
    }
    interface interface-name {
        exclude;
        liveness-detection {
            failure-action (clear-binding | clear-binding-if-interface-up | log-only);
            method {
                bfd {
                    version (0 | 1 | automatic);
                    minimum-interval milliseconds;
                    minimum-receive-interval milliseconds;
                    multiplier number;
                    no-adaptation;
                    transmit-interval {
                        minimum-interval milliseconds;
                        threshold milliseconds;
                    }
                }
                detection-time {
                    threshold milliseconds;
                }
            }
            session-mode (automatic | multihop | singlehop);
            holddown-interval milliseconds;
        }
    }
    overrides {
        ...
    }
    service-profile dynamic-profile-name;
    trace;
```

```
    upto upto-interface-name;
}
overrides {
    allow-snooped-clients;
    always-write-giaddr;
    always-write-option-82;
    client-discover-match (option60-and-option82 | incoming-interface);
    disable-relay;
    interface-client-limit number;
    layer2-unicast-replies;
    no-allow-snooped-clients;
    no-bind-on-request;
    proxy-mode;
    replace-ip-source-with;
    send-release-on-delete;
    trust-option-82;
}
relay-agent-interface-id {
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82;
}
relay-agent-remote-id {
    prefix prefix;
    use-interface-description (logical | device);
}
relay-option {
    option-number option-number;
    default-action {
        drop;
        forward-only;
        local-server-group local-server-group;
        relay-server-group relay-server-group;
    }
    equals (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
        forward-only;
        local-server-group local-server-group;
        relay-server-group relay-server-group;
    }
    starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
        forward-only;
        local-server-group local-server-group;
        relay-server-group relay-server-group;
    }
}
relay-option-82 {
    circuit-id {
        prefix prefix;
        use-interface-description (logical | device);
        use-option-82;
    }
    remote-id {
        prefix prefix;
        use-interface-description (logical | device);
    }
}
```

```

    }
  }
  route-suppression;
  service-profile dynamic-profile-name;
}

```

Hierarchy Level	[edit forwarding-options dhcp-relay], [edit forwarding-options dhcp-relay dhcpv6], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...]
Release Information	Statement introduced in Junos OS Release 8.3. Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4. Statement introduced in Junos OS Release 12.1 for EX Series switches.
Description	Specify the name of a group of interfaces that have a common DHCP or DHCPv6 relay agent configuration. A group must contain at least one interface. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.
Options	<p>group-name—Name of a group of interfaces that have a common DHCP or DHCPv6 relay agent configuration.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • dhcp-relay on page 689 • Extended DHCP Relay Agent Overview on page 194 • Configuring Group-Specific DHCP Relay Options on page 226 • Grouping Interfaces with Common DHCP Configurations on page 223 • Using External AAA Authentication Services with DHCP on page 217 • Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces

group (Static Subscribers)

Syntax

```
group group-name {
  access-profile profile-name;
  dynamic-profile profile-name {
    aggregate-clients (merge | replace);
  }
  authentication {
    password password-string;
    username-include {
      domain-name domain-name;
      interface;
      logical-system-name;
      routing-instance-name;
      user-prefix user-prefix-string;
    }
  }
  interface interface-name <exclude> <upto upto-interface-name>;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* system services [static-subscribers](#)],
[edit logical-systems *logical-system-name* routing-instances *routing-instances-name* system services [static-subscribers](#)],
[edit routing-instances *routing-instances-name* system services [static-subscribers](#)],
[edit system services [static-subscribers](#)]

Release Information Statement introduced in Junos OS Release 9.6.

Description Configure a static subscriber group with values that override the values configured at the **[edit system services static-subscribers]** hierarchy level for subscribers outside the group. Includes the subscriber access and dynamic profiles, the authentication parameters that trigger the Access-Request message to AAA for static subscribers in the group, and the statically configured interfaces that form the group.



NOTE: The logical system and routing instance in which the group is configured must match the logical system and routing instance where the static interfaces are configured.

Options *group-name*—Name of a group that defines authentication parameters for static subscribers to override the global authentication configuration.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring Subscribers over Static Interfaces on page 466](#)
- [Creating a Static Subscriber Group on page 475](#)

gsmp-syn-timeout (ANCP)

Syntax	<code>gsmp-syn-timeout <i>seconds</i>;</code>
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 13.3.
Description	Configure the maximum period that the ANCP agent waits before sending a SYN message to an ANCP neighbor to negotiate the adjacency. If the neighbor sends a SYN message during this period, the ANCP agent uses the partition information in the neighbor's message when generating its own initial SYN message to the neighbor. The agent does not wait for the period to expire if it receives a SYN message from the neighbor.
Options	<i>seconds</i> —Number of seconds the ANCP agent waits. Range: 1 through 60 seconds Default: 60 seconds
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the ANCP Agent on page 368• Configuring the ANCP Agent to Learn ANCP Partition IDs on page 373

gsmp-syn-wait (ANCP)

Syntax	gsmp-syn-wait;
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 13.3
Description	Enable the ANCP agent to learn partition ID information from neighbors, in support of nonzero ANCP partition IDs. This statement forces the ANCP agent to delay sending a SYN message during adjacency negotiation for a configurable period. When the neighbor sends a SYN message to the ANCP agent during that period, the agent learns the partition ID information from the neighbor and uses that information when it sends its own SYN message. If the agent does not receive the message during the period, then it sends a SYN message to the neighbor when the period times out.
Default	This statement is disabled. The ANCP agent does not wait before sending the initial SYN message and does not support nonzero partition IDs.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the ANCP Agent on page 368• Configuring the ANCP Agent to Learn ANCP Partition IDs on page 373

gx-plus (Gx-Plus)

Syntax	<pre> gx-plus { global { include-ipv6; max-outstanding-requests <i>number</i>; } partition <i>partition-name</i> { diameter-instance <i>instance-name</i>; destination-host <i>hostname</i>; destination-realm <i>realm</i>; } } </pre>
Hierarchy Level	[edit access]
Release Information	<p>Statement introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p>
Description	<p>Configure the Gx-Plus application to interact with a PCRF to authorize and provision subscribers.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Gx-Plus on page 446

hardware-address

Syntax	hardware-address <i>mac-address</i> ;
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family (inet inet6) <i>host</i> <i>hostname</i>]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	Specify the MAC address of the client. This is the hardware address that identifies the client on the network.
Options	<i>mac-address</i> —MAC address of the client.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Address-Assignment Pools on page 316

high-utilization (Address-Assignment Pools)

Syntax	<code>high-utilization <i>percentage</i>;</code>
Hierarchy Level	[edit access address-assignment], [edit routing-instances <i>routing-instance-name</i> address-assignment]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	Generate an SNMP trap when the DHCP address pool or linked set of address pools use surpasses the specified percentage.
Default	High utilization is not set. Delete the high-utilization value to unset.
Options	<i>percentage</i> —Percentage used to generate a trap. Range: 2 through 99
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Address-Assignment Pools Overview on page 315• Configuring Address-Assignment Pool Usage Threshold Traps on page 320

high-utilization-v6 (Address-Assignment Pools)

Syntax	<code>high-utilization-v6 <i>percentage</i>;</code>
Hierarchy Level	[edit access address-assignment], [edit routing-instances <i>routing-instance-name</i> address-assignment]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	Generate an SNMP trap when the DHCPv6 address pool or linked set of address pools use surpasses the specified percentage.
Default	High utilization is not set. Delete the high-utilization value to unset.
Options	<i>percentage</i> —Percentage used to generate a trap. Range: 2 through 99
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Address-Assignment Pools Overview on page 315• Configuring Address-Assignment Pool Usage Threshold Traps on page 320

host (Address-Assignment Pools)

Syntax	<pre>host <i>hostname</i> { hardware-address <i>mac-address</i>; ip-address <i>ip-address</i>; }</pre>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family (inet inet6)]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	Configure a static binding for the specified client.
Options	<p>hostname—Name of the client.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Address-Assignment Pools Overview on page 315 • Configuring Address-Assignment Pools on page 316

host (Diameter Origin)

Syntax	host <i>hostname</i> ;
Hierarchy Level	[edit diameter origin]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Specify the name of the host that originates the Diameter message.
Options	<p>hostname—Name of the message origin host. Supplied as the value of Origin-Host AVP for all messages sent by the Diameter master instance.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Diameter on page 434 • Configuring the Origin Attributes of the Diameter Instance on page 435

ietf-mode

Syntax	ietf-mode
Hierarchy Level	[edit protocols ancp neighbor ip-address]
Release Information	Statement introduced in Junos OS Release 9.5.
Description	Configure the ANCP agent to run in a mode that is not backward compatible with Internet draft-wadhwa-gsmp-l2control-configuration-00.txt, <i>GSMP extensions for layer2 control (L2C)</i> . Include this statement when pre-ietf mode has been configured globally for the ANCP agent, but you want one or more neighbors to run in the default mode.
Default	ANCP does not run in a backward-compatible mode.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the ANCP Agent on page 368• Configuring ANCP Neighbors on page 369

ignore

Syntax	<pre>ignore { dynamic-iflset-name; framed-ip-netmask; input-filter; logical-system-routing-instance; output-filter; }</pre>
Hierarchy Level	[edit access profile <i>profile-name</i> radius attributes]
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 9.1 for EX Series switches.</p>
Description	Configure the router or switch to ignore the specified attributes in RADIUS Access-Accept messages. By default, the router or switch processes the attributes it receives from the external server.
Options	<p>dynamic-iflset-name—Ignore Interface-Set/Dynamic-Ifset-Name (VSA 26-130).</p> <p>framed-ip-netmask—Ignore Framed-IP-Netmask (RADIUS attribute 9).</p> <p>input-filter—Ignore Ingress-Policy-Name (VSA 26-10).</p> <p>logical-system-routing-instance—Ignore Virtual-Router (VSA 26-1).</p> <p>output-filter—Ignore Egress-Policy-Name (VSA 26-11).</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring RADIUS Server Parameters for Subscriber Access on page 102

immediate-update

Syntax	immediate-update;
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	Configure the router or switch to send an Acct-Update message to the RADIUS accounting server on receipt of a response (for example, an ACK or timeout) to the Acct-Start message.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Server Parameters for Subscriber Access on page 102• Configuring Per-Subscriber Session Accounting on page 92

include-ipv6 (Gx-Plus)

Syntax	include-ipv6;
Hierarchy Level	[edit access gx-plus global]
Release Information	Statement introduced in Junos OS Release 12.3. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Description	Include IPv6 subscribers in Gx-Plus provisioning requests.
Default	By default, IPv6 subscribers are not included.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Gx-Plus Global Attributes on page 448• Configuring Gx-Plus on page 446

include-irb-and-l2

Syntax include-irb-and-l2;

Hierarchy Level [edit forwarding-options dhcp-relay **dhcpv6** (**relay-agent-interface-id** | **relay-agent-remote-id**)],
 [edit forwarding-options dhcp-relay **dhcpv6** group *group-name* (**relay-agent-interface-id** | **relay-agent-remote-id**)],
 [edit forwarding-options dhcp-relay relay-option-82 (circuit-id | **remote-id**)],
 [edit forwarding-options dhcp-relay group *group-name* relay-option-82 (circuit-id | **remote-id**)],
 [edit logical-systems *logical-system-name* ... forwarding-options dhcp-relay dhcpv6 (**relay-agent-interface-id** | **relay-agent-remote-id**)],
 [edit logical-systems *logical-system-name* ... forwarding-options dhcp-relay ... relay-option-82 (circuit-id | **remote-id**)],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay dhcpv6 (**relay-agent-interface-id** | **relay-agent-remote-id**)],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay ... relay-option-82 (circuit-id | **remote-id**)],
 [edit vlans *vlan-name* forwarding-options dhcp-security dhcpv6-options option-18],
 [edit vlans *vlan-name* forwarding-options dhcp-security dhcpv6-options option-37]

Release Information Statement introduced in Junos OS Release 14.1.



NOTE: The EX Series switches that support the include-irb-and-l2 statement are the EX4300, EX4600, and EX9200 switches.

Description Include both the integrated routing and bridging (IRB) interface name and Layer 2 interface name in the **circuit-id** or **remote-id** value in the DHCP option 82 information. VLAN tags are global.

When you configure the **include-irb-and-l2** statement without including the **no-vlan-interface** statement, the format is as follows:

- Bridge domain:

(fe | ge)-fpc/pic/port.subunit:bridge-domain-name+irb.subunit

- VLAN:

(fe | ge)-fpc/pic/port.subunit:vlan-name+irb.subunit



NOTE: For remote systems, the *subunit* is required and is used to differentiate an interface.

When you configure both the **include-irb-and-l2** statement and the **use-vlan-id** statement, the format is as follows:

(fe | ge)-fpc/pic/port.subunit:svlan-id-vlan-id+irb.subunit



NOTE: The *svlan-id-vlan-id* represents the VLANs associated with the bridge domain.

When you configure both the **include-irb-and-l2** and **no-vlan-interface-name** statements, the format is as follows:

(fe | ge)-fpc/pic/port.subunit+irb.subunit

When you configure both the **include-irb-and-l2** and **use-interface-description** statements, the format displays the description for the Layer 2 interface:

l2_descr:vlan-name+irb.subunit

If you configure both the **include-irb-and-l2** and **use-interface-description** statements, and no description for the Layer 2 interface is found, the format displays the Layer 2 logical interface name:

(fe | ge)-fpc/pic/port.subunit:vlan-name+irb.subunit

When you configure the **include-irb-and-l2** statement with both the **no-vlan-interface-name** and **use-interface-description** statements, the format displays as follows:

l2_descr+irb.subunit

If you configure the **include-irb-and-l2** statement with both the **no-vlan-interface-name** and **use-interface-description** statements, and no description is found for the Layer 2 interface, the format displays as follows:

(fe | ge)-fpc/pic/port.subunit+irb.subunit

Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
---------------------------------	---

Related Documentation	<ul style="list-style-type: none">• Including a Textual Description in DHCP Options on page 271• Using DHCP Relay Agent Option 82 Information on page 266• Configuring DHCPv6 Relay Agent Options on page 296
------------------------------	---

interface (DHCP Local Server)

Syntax `interface interface-name {
 exclude;
 overrides {
 client-discover-match (option60-and-option82 | incoming-interface);
 interface-client-limit number;
 rapid-commit;
 }
 service-profile dynamic-profile-name;
 trace;
 upto upto-interface-name;
}`

Hierarchy Level [edit system services dhcp-local-server *group group-name*],
 [edit system services dhcp-local-server *dhcpv6 group group-name*],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system
 services *dhcp-local-server ...*],
 [edit logical-systems *logical-system-name* system services *dhcp-local-server ...*],
 [edit routing-instances *routing-instance-name* system services *dhcp-local-server ...*]

Release Information Statement introduced in Junos OS Release 9.0.
 Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
 Options **upto** and **exclude** introduced in Junos OS Release 9.1.

Description Specify one or more interfaces, or a range of interfaces, that are within a specified group on which the DHCP local server is enabled. You can repeat the **interface *interface-name*** statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group. Also, you cannot use an interface that is being used by the DHCP relay agent.



NOTE: DHCP values are supported in Integrated Routing and Bridging (IRB) configurations. When you configure an IRB interface in a network that is using DHCP, the DHCP information (for example, authentication, address assignment, and so on) is propagated in the associated bridge domain. This enables the DHCP server to configure client IP addresses residing within the bridge domain. IRB currently only supports static DHCP configurations. For additional information about how to configure IRB, see *Configuring Integrated Routing and Bridging for Bridge Domains*.

Options **exclude**—Exclude an interface or a range of interfaces from the group. This option and the **overrides** option are mutually exclusive.

interface-name—Name of the interface. You can repeat this option multiple times.

upto-interface-name—Upper end of the range of interfaces; the lower end of the range is the interface-name entry. The interface device name of the ***upto-interface-name*** must be the same as the device name of the ***interface-name***.

The remaining statements are explained separately.

Required Privilege	system—To view this statement in the configuration.
Level	system-control—To add this statement to the configuration.

- | | |
|------------------------------|--|
| Related Documentation | <ul style="list-style-type: none">• Extended DHCP Local Server Overview on page 188• Grouping Interfaces with Common DHCP Configurations on page 223• Using External AAA Authentication Services with DHCP on page 217 |
|------------------------------|--|

interface (DHCP Relay Agent)

Syntax	<pre> interface <i>interface-name</i> { exclude; overrides { allow-snooped-clients; always-write-giaddr; always-write-option-82; client-discover-match (option60-and-option82 incoming-interface); disable-relay; interface-client-limit <i>number</i>; layer2-unicast-replies; no-allow-snooped-clients; proxy-mode; replace-ip-source-with; send-release-on-delete; trust-option-82; } service-profile <i>dynamic-profile-name</i>; trace; upto <i>upto-interface-name</i>; } </pre>
Hierarchy Level	<pre> [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i>], [edit forwarding-options dhcp-relay group <i>group-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...] </pre>
Release Information	<p>Statement introduced in Junos OS Release 8.3.</p> <p>Options upto and exclude introduced in Junos OS Release 9.1.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	<p>Specify one or more interfaces, or a range of interfaces, that are within a specified group on which the DHCP or DHCPv6 relay agent is enabled. You can repeat the interface <i>interface-name</i> statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group. Also, you cannot use an interface that is being used by the DHCP local server. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.</p> <p>EX Series switches do not support DHCPv6.</p>



NOTE: DHCP values are supported in Integrated Routing and Bridging (IRB) configurations. When you configure an IRB interface in a network that is using DHCP, the DHCP information (for example, authentication, address assignment, and so on) is propagated in the associated bridge domain. This enables the DHCP server to configure client IP addresses residing within the bridge domain. IRB currently only supports static DHCP configurations. For

additional information about how to configure IRB, see *Configuring Integrated Routing and Bridging for Bridge Domains*.

.....

Options **exclude**—Exclude an interface or a range of interfaces from the group. This option and the **overrides** option are mutually exclusive.

interface-name—Name of the interface. You can repeat this option multiple times.

overrides—Override the specified default configuration settings for the interface. The **overrides** statement is described separately.

upto-interface-name—Upper end of the range of interfaces; the lower end of the range is the interface-name entry. The interface device name of the **upto-interface-name** must be the same as the device name of the **interface-name**.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Documentation

- [Extended DHCP Relay Agent Overview on page 194](#)
- [dhcp-relay on page 689](#)
- *dhcp-relay (EX Series Switches only)*
- *Understanding the Extended DHCP Relay Agent for EX Series Switches*
- *Configuring an Extended DHCP Relay Server on EX Series Switches (CLI Procedure)*
- [Grouping Interfaces with Common DHCP Configurations on page 223](#)
- [Using External AAA Authentication Services with DHCP on page 217](#)

interface (Dynamic Router Advertisement)

Syntax interface *interface-name* {
 current-hop-limit *number*;
 default-lifetime *seconds*;
 dns-server-address
 (*managed-configuration* | *no-managed-configuration*);
 max-advertisement-interval *seconds*;
 min-advertisement-interval *seconds*;
 (*other-stateful-configuration* | *no-other-stateful-configuration*);
 prefix *prefix* {
 (*autonomous* | *no-autonomous*);
 (*on-link* | *no-on-link*);
 preferred-lifetime *seconds*;
 valid-lifetime *seconds*;
 }
 reachable-time *milliseconds*;
 retransmit-timer *milliseconds*;
 }

Hierarchy Level [edit dynamic-profiles protocols router-advertisement]

Release Information Statement introduced in Junos OS Release 10.1.

Description Dynamically configure router advertisement properties on an interface. To dynamically configure interface properties, include the *\$junos-interface-name* dynamic variable for the interface name.

Options *interface-name*—Name of an interface. Specify the *\$junos-interface-name* dynamic variable or the full, static interface name, including the physical and logical address components.




NOTE: Even though you can specify a static interface name when defining the interface, we recommend using dynamic variable when configuring this statement.

The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
 routing-control—To add this statement to the configuration.

Related Documentation • *Example: Configuring IPv6 Interfaces and Enabling Neighbor Discovery*

interface (Static Subscriber Group)

Syntax	<code>interface <i>interface-name</i> <exclude> <upto <i>upto-interface-name</i>>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers group <i>group-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i>],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i>],</p> <p>[edit system services static-subscribers group <i>group-name</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.6.</p> <p>Support for IPv6 and IPv4 demux static interfaces introduced in Junos OS Release 11.2.</p>
Description	Specify one or more interfaces, or a range of interfaces, that are within a specified group on which static subscribers are created. You can repeat the interface <i>interface-name</i> statement to specify multiple interfaces within a group. You must configure each interface in only one group.
<div style="display: flex; align-items: center;">  <div> <p>NOTE: The logical system and routing instance in which the static interfaces are configured must match the logical system and routing instance where the group is configured.</p> </div> </div>	
Options	<p>exclude—(Optional) Exclude an interface or a range of interfaces from the group.</p> <p><i>interface-name</i>—Name of the interface on which static subscribers are created. If you do not specify a unit number for the interface, then .0 is assumed. For example, ge-0/1/0 is interpreted as ge-0/1/0.0.</p> <p><i>upto-interface-name</i>—(Optional) The upper end of the range of interfaces; the lower end of the range is the <i>interface-name</i> entry. The interface device name of <i>upto-interface-name</i> must be the same as the device name of <i>interface-name</i>.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Subscribers over Static Interfaces on page 466 • Creating a Static Subscriber Group on page 475

interface (Static Subscriber Username)

Syntax	interface;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers authentication username-include],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication username-include],</p> <p>[edit system services static-subscribers authentication username-include],</p> <p>[edit system services static-subscribers group <i>group-name</i> authentication username-include]</p>
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Specify that a modified version of the interface name is included as part of the username created for all static subscribers or for the static subscribers in a specified group. The group version of the statement takes precedence over the global version. The username is also sent to RADIUS in the Access-Request message. The interface name is modified by replacing the "/" character with the "-" character. For example, ge-0/1/2.50 is converted to ge-0-1-2.50.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Subscribers over Static Interfaces on page 466 • Configuring the Static Subscriber Global Username on page 473 • Configuring the Static Subscriber Group Username on page 478

interface-client-limit (DHCP Local Server)

Syntax	<code>interface-client-limit <i>number</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group group-name overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit system services dhcp-local-server overrides],</p> <p>[edit system services dhcp-local-server dhcpv6 overrides],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name overrides],</p> <p>[edit system services dhcp-local-server dhcpv6 group interface <i>interface-name</i> <i>group-name</i> overrides],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i> overrides]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.2.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Set the maximum number of DHCP subscribers or DHCP clients per interface allowed for a specific group or for all groups. A group specification takes precedence over a global specification for the members of that group.
Default	No limit
Options	<i>number</i> —Maximum number of clients allowed.

Range: 1 through 500,000

Required Privilege system—To view this statement in the configuration.
Level system-control—To add this statement to the configuration.

Related Documentation

- [Specifying the Maximum Number of DHCP Clients Per Interface on page 233](#)
- [Overriding Default DHCP Local Server Configuration Settings on page 255](#)

interface-client-limit (DHCP Relay Agent)

Syntax	<code>interface-client-limit <i>number</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay dhcpv6 overrides], [edit forwarding-options dhcp-relay overrides], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides], [edit forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.2. Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4. Statement introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	<p>Set the maximum number of DHCP (or DHCPv6) subscribers or clients per interface allowed for a specific group or for all groups. A group specification takes precedence over a global specification for the members of that group. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.</p> <p>M120 and M320 routers do not support DHCPv6.</p>
Default	No limit
Options	<p><i>number</i>—Maximum number of clients allowed. Range: 1 through 500,000</p>
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</p>

- Related Documentation**
- [dhcp-relay on page 689](#)
 - [Extended DHCP Relay Agent Overview on page 194](#)
 - [Configuring Group-Specific DHCP Relay Options on page 226](#)
 - [Overriding the Default DHCP Relay Configuration Settings on page 256](#)

interface-delete (Subscriber Management or DHCP Client Management)

Syntax	interface-delete;
Hierarchy Level	[edit system services subscriber-management maintain-subscriber]
Release Information	Statement introduced in Junos OS Release 11.1. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	<p>On router—Configure the router to maintain, rather than log out, subscribers when the subscriber interface is deleted. By default, the router logs out subscribers when the subscriber interface is deleted.</p> <p>On switch—Configure the switch to maintain rather than log out DHCP clients when the client interface is deleted. By default, the switch logs out DHCP clients when the client interface is deleted.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events on page 238

interface-delete (Subscriber Management or DHCP Client Management)

Syntax	interface-delete;
Hierarchy Level	[edit system services subscriber-management maintain-subscriber]
Release Information	Statement introduced in Junos OS Release 11.1. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	<p>On router—Configure the router to maintain, rather than log out, subscribers when the subscriber interface is deleted. By default, the router logs out subscribers when the subscriber interface is deleted.</p> <p>On switch—Configure the switch to maintain rather than log out DHCP clients when the client interface is deleted. By default, the switch logs out DHCP clients when the client interface is deleted.</p>
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events on page 238

interface-description-format

Syntax	interface-description-format { exclude-adapter; exclude-sub-interface; }
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches. Options exclude-adapter and exclude-sub-interface introduced in Junos OS Release 10.4.
Description	Specify the information that is excluded from the interface description that the device passes to RADIUS for inclusion in the RADIUS attribute 87 (NAS-Port-Id). By default, the device includes both the subinterface and the adapter in the interface description.
Options	<p>exclude-adapter—Exclude the adapter from the interface description.</p> <p>exclude-sub-interface—Exclude the subinterface from the interface description.</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Server Options for Subscriber Access on page 102• RADIUS Server Options for Subscriber Access on page 4

interface-name (DHCP Local Server)

Syntax	interface-name;
Hierarchy Level	<p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server group group-name authentication username-include]</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server ...],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...]</p>
Release Information	<p>Statement introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify that the interface name is concatenated with the username during the subscriber authentication or DHCP client authentication process. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Creating Unique Usernames for DHCP Clients on page 218

interface-name (DHCP Relay Agent)

Syntax	interface-name;
Hierarchy Level	[edit forwarding-options dhcp-relay authentication username-include], [edit forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include], [edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...]
Release Information	Statement introduced in Junos OS Release 11.4 Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Specify that the interface name is concatenated with the username during the subscriber authentication or client authentication process. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Creating Unique Usernames for DHCP Clients on page 218

interface-set (ANCP)

Syntax	<pre>interface-set <i>interface-set-name</i> { <i>access-identifier</i> <i>identifier-string</i>; <i>underlying-interface</i> <i>underlying-interface-name</i>; }</pre>
Hierarchy Level	[edit protocols ancp interfaces]
Release Information	Statement introduced in Junos OS Release 9.4.
Description	Identify a group of VLANs on which traffic is sent to a subscriber identified by the access-loop circuit identifier.
Options	<p><i>interface-set-name</i>—Name of a group of VLANs that carry traffic to the subscriber identified by the access loop circuit identifier.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring the ANCP Agent on page 368 • Associating an Access Node with Subscribers for ANCP Agent Operations on page 370

interface-traceoptions (DHCP)

Syntax	<pre>interface-traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i> > <size <i>maximum-file-size</i>> <world-readable no-world-readable>; flag <i>flag</i>; level (all error info notice verbose warning); no-remote-trace; }</pre>
Hierarchy Level	[edit system processes dhcp-service]
Release Information	Statement introduced in Junos OS Release 11.4. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	<p>Configure extended DHCP tracing operations that can be enabled on a specific interface or group of interfaces.</p> <p>Replaces deprecated interface-traceoptions statements at the [edit forwarding-options dhcp-relay] and [edit system services dhcp-local-server] hierarchy levels.</p> <p>To enable the tracing operation on the specific interfaces, you use the interface <i>interface-name</i> trace statement.</p>
Options	<p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the size option.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements</p> <ul style="list-style-type: none">• all—Trace all events• packet—Trace packet and option decoding operations• state—Trace changes in state <p>level—Level of tracing to perform; also known as severity level. The option you configure enables tracing of events at that level and all higher (more restrictive) levels. You can specify any of the following levels:</p> <ul style="list-style-type: none">• all—Match messages of all levels.• error—Match error messages.• info—Match informational messages.• notice—Match notice messages about conditions requiring special handling.

- **verbose**—Match verbose messages. This is the lowest (least restrictive) severity level; when you configure **verbose**, messages at all higher levels are traced. Therefore, the result is the same as when you configure **all**.
- **warning**—Match warning messages.

Default: error

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: *sizek* to specify KB, *sizem* to specify MB, or *sizeg* to specify GB

Range: 10240 through 1073741824

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level	trace—To view this statement in the configuration.
	trace-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Tracing Extended DHCP Operations for Specific Interfaces on page 526

interfaces (ANCP)

Syntax	<pre>interfaces { interface-set <i>interface-set-name</i> { access-identifier <i>identifier-string</i>; underlying-interface <i>underlying-interface-name</i>; } interface-name { access-identifier <i>identifier-string</i> } }</pre>
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 9.4.
Description	Identify the subscribers whose traffic is reported and shaped by the ANCP agent.
Options	<p>interface-name—Name of a logical interface supporting a single VLAN that carries traffic to the subscriber identified by the access-loop circuit identifier.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the ANCP Agent on page 368• Associating an Access Node with Subscribers for ANCP Agent Operations on page 370

ip-address

Syntax	<pre>ip-address <i>ip-address</i>;</pre>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet host <i>hostname</i>]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	Specify the reserved IP address assigned to the client.
Options	ip-address —IP version 4 (IPv4) address.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Address-Assignment Pools on page 316• Configuring Static Address Assignment on page 321

ip-address-first

Syntax	ip-address-first;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server pool-match-order],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server pool-match-order],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server pool-match-order],</p> <p>[edit system services dhcp-local-server pool-match-order]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.0.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	<p>Configure the extended DHCP local server to use the IP address method to determine which address-assignment pool to use. The local server uses the IP address in the gateway IP address if one is present in the DHCP client PDU. If no gateway IP address is present, the local server uses the IP address of the receiving interface to find the address-assignment pool. The DHCP local server uses this method by default when no method is explicitly specified.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 203 • Extended DHCP Local Server Overview on page 188 • Address-Assignment Pools Overview on page 315 • <i>Configuring a DHCP Server on Switches (CLI Procedure)</i>

jsrc (JSRC)

Syntax	<pre>jsrc { partition <i>partition-name</i> { diameter-instance <i>instance-name</i>; destination-host <i>hostname</i>; destination-realm <i>realm-name</i>; } }</pre>
Hierarchy Level	[edit]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	<p>Configure JSRC to interact with an SAE in an SRC environment to authorize and provision subscribers.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring JSRC on page 455

jsrc-partition

Syntax	<pre>jsrc-partition <i>partition-name</i>;</pre>
Hierarchy Level	[edit]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Specify the JSRC partition to use.
Options	<i>partition-name</i> —Name of the JSRC partition that you want JSRC to use. The name is defined with the partition statement at the [edit jsrc] hierarchy level.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring JSRC on page 455• Configuring the JSRC Partition on page 456

juniper-dsl-attributes

Syntax	juniper-dsl-attributes;
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	<p>Configure AAA to add Juniper Networks DSL VSAs to the RADIUS authentication and accounting request messages for subscribers. If the router has not received and processed the corresponding ANCP attributes from the access node, then AAA provides only the following in these RADIUS messages:</p> <ul style="list-style-type: none"> Downstream-Calculated-QoS-Rate (IANA 4874, 26-141)—Default configured advisory transmit speed. Upstream-Calculated-QoS-Rate (IANA 4874, 26-142)—Default configured advisory receive speed.
Default	The Juniper Networks DSL VSAs are not added to the RADIUS authentication and accounting request messages. However, the DSL Forum VSA—if available—is added to RADIUS messages by default.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring AAA to Include Juniper Networks DSL VSAs in RADIUS Messages on page 407 Configuring the ANCP Agent on page 368

layer2-unicast-replies

Syntax	layer2-unicast-replies;
Hierarchy Level	[edit forwarding-options dhcp-relay overrides], [edit forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]
Release Information	Statement introduced in Junos OS Release 8.3. Statement introduced in Junos OS Release 12.1 for EX Series switches.
Description	Override the setting of the broadcast bit in DHCP request packets and instead use the Layer 2 unicast transmission method to transmit DHCP Offer reply packets and DHCP ACK reply packets from the DHCP server to DHCP clients during the discovery process.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Extended DHCP Relay Agent Overview on page 194• dhcp-relay on page 689

lease-time-threshold (DHCP Local Server and DHCP Relay Agent)

Syntax	<code>lease-time-threshold <i>seconds</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay lease-time-validation],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 lease-time-validation],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> lease-time-validation],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> lease-time-validation],</p> <p>[edit logical-systems <i>logical-system-name</i> ...],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>...],</p> <p>[edit routing-instances <i>routing-instance-name</i> ...],</p> <p>[edit system services dhcp-local-server lease-time-validation],</p> <p>[edit system services dhcp-local-server dhcpv6 lease-time-validation],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> lease-time-validation],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> lease-time-validation]</p>
Release Information	Statement introduced in Junos OS Release 14.1.
Description	Configure the minimum DHCP lease time allowed in your subscriber access network. If a third-party DHCP server or address pool provides a client lease that is less than the configured threshold, the router performs the action specified by the violation-action statement.
Options	<p><i>seconds</i>—Minimum client lease time allowed.</p> <p>Range: 60 through 2,147,483,647 seconds</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring a DHCP Lease-Time Threshold on page 209

lease-time-validation (DHCP Local Server and DHCP Relay Agent)

Syntax	<code>lease-time-validation { lease-time-threshold <i>seconds</i>; violation-action <i>action</i>; }</code>
Hierarchy Level	<code>[edit forwarding-options dhcp-relay], [edit forwarding-options dhcp-relay dhcpv6], [edit forwarding-options dhcp-relay group <i>group-name</i>], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i>], [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>...], [edit routing-instances <i>routing-instance-name</i> ...], [edit system services dhcp-local-server], [edit system services dhcp-local-server dhcpv6], [edit system services dhcp-local-server group <i>group-name</i>], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 14.1.
Description	<p>Enable the lease-time validation feature on the router. You can then configure the lease-time threshold and an optional action to take when a lease-time violation occurs.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring a DHCP Lease-Time Threshold on page 209

limit

Syntax	<code>limit <i>max-sub-sessions</i>;</code>
Hierarchy Level	<code>[edit services service-set <i>services-set-name</i> subscriber-profile <i>profile-name</i> max-data-sessions-per-subscriber]</code>
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Specify the limit for the maximum number of subscriber sessions.
Options	<i>max-sub-sessions</i> —Maximum number of subscriber sessions.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>

link (Address-Assignment Pools)

Syntax	link <i>pool-name</i> ;
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i>]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Configure the name of the secondary address-assignment pool that is linked to a primary address-assignment pool. The secondary pool provides backup pool for local address assignment.
Options	<i>pool-name</i> —Name assigned to the address-assignment pool.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Address-Assignment Pools Overview on page 315• Configuring Address-Assignment Pools on page 316• Configuring Address-Assignment Pool Linking on page 320

local-address

Syntax	<code>local-address (address any-unicast) <except>;</code>
Hierarchy Level	[edit services ptsp forward-rule <i>forward-rule-name</i> term <i>precedence</i> from]
Release Information	Statement introduced in Junos OS Release 10.2. IPv6 support introduced in Junos OS Release 12.2
Description	Specify the address for rule matching. Local address values are matched against a source or destination IP address for the flow depending on the configured value for the demux statement. If you do not specify an address, then any local address matches this term. If you do not specify a prefix value, then a host mask is the default.
Options	address —IPv4 or IPv6 address or prefix value. any-unicast —Match all unicast addresses. except —(Optional) Exclude the specified address, prefix, or unicast packets from rule matching.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>• demux on page 679

local-address-range

Syntax	<code>local-address-range low <i>low-value</i> high <i>high-value</i> <except>;</code>
Hierarchy Level	[edit services ptsp forward-rule <i>forward-rule-name</i> term <i>precedence</i> from]
Release Information	Statement introduced in Junos OS Release 10.2. IPv6 support introduced in Junos OS Release 12.2
Description	Specify the address range for rule matching. Local address values are matched against a source or destination IP address for the flow depending on the configured value for the demux statement. If you do not specify an address, then any local address matches this term.
Options	<p>low-value—Lower boundary for the IPv4 or IPv6 address range.</p> <p>high-value—Upper boundary for the IPv4 or IPv6 address range.</p> <p>except—(Optional) Exclude the specified address range from rule matching.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i> • demux on page 679

local-port-range

Syntax	<code>local-port-range low <i>low-value</i> high <i>high-value</i>;</code>
Hierarchy Level	[edit services ptsp rule <i>rule-name</i> term <i>precedence</i> from]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Specify the port range for rule matching.
Options	<p>low-value—Lower boundary for the port range.</p> <p>high-value—Upper boundary for the port range.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>

local-ports

Syntax	<code>local-ports [<i>port-numbers</i>];</code>
Hierarchy Level	[edit services ptsp rule <i>rule-name</i> term <i>precedence</i> from]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Identify one or more ports for inclusion as a match condition.
Options	<i>port-numbers</i> —Port number.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>

local-prefix-list

Syntax	<code>local-prefix-list <i>prefix-list-name</i> <except>;</code>
Hierarchy Level	[edit services ptsp forward-rule <i>forward-rule-name</i> term <i>precedence</i> from]
Release Information	Statement introduced in Junos OS Release 10.2. IPv6 support introduced in Junos OS Release 12.2
Description	Specify the prefix list for rule matching. You configure the prefix list by including the prefix-list statement at the [edit policy-options] hierarchy level.
Options	<i>prefix-list-name</i> —Prefix list. except —(Optional) Exclude the specified prefix list from rule matching.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>

local-server-group (DHCP Relay Agent Option)

Syntax	<code>local-server-group <i>local-server-group</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay relay-option (default-action equals starts-with)],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> relay-option (default-action equals starts-with)],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay ...],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...]</p>
Release Information	<p>Statement introduced in Junos OS Release 12.3.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	<p>Forward DHCP client packets to the specified group of DHCP local servers when you use the DHCP relay selective processing feature. You can configure the forwarding operation globally or for a group of interfaces.</p> <p>The local-server-group option is not supported for DHCPv6 relay agent.</p>
Options	<i>local-server-group</i> —Name of DHCP local server group.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using DHCP Option Information to Selectively Process DHCP Client Traffic on page 273

logical-system (Diameter Peer)

Syntax	<code>logical-system <i>logical-system-name</i> [<routing-instance <i>routing-instance-name</i> > ;</code>
Hierarchy Level	[edit diameter peer <i>peer-name</i>]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Specify a logical system and optionally a routing instance for a Diameter peer. Alternatively, you can include the routing-instance statement at the [edit diameter peer <i>peer-name</i>] hierarchy level to configure only a routing instance.
Options	<p><i>logical-system-name</i>— Name of the logical system. Default: Default logical system</p> <p><i>routing-instance routing-instance-name</i>—(Optional) Name of the routing instance. Default: Master routing instance</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Diameter on page 434• Configuring Diameter Peers on page 435

logical-system (Diameter Transport)

Syntax	<code>logical-system <i>logical-system-name</i> <routing-instance <i>routing-instance-name</i> >;</code>
Hierarchy Level	[edit diameter transport <i>transport-name</i>]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	Specify a logical system and optionally a routing instance for the transport layer connection.



NOTE: The logical system and routing instance must match that for the peer or a configuration error is reported.

Options	<p><i>logical-system-name</i>—Name of the logical system.</p> <p>Default: Default logical system</p> <p><i>routing-instance <i>routing-instance-name</i></i>—(Optional) Name of the routing instance.</p> <p>Default: Master routing instance</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Diameter on page 434 • Configuring the Diameter Transport on page 436

logical-system-name (Static Subscribers)

Syntax	logical-system-name;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers authentication username-include],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication username-include],</p> <p>[edit system services static-subscribers authentication username-include],</p> <p>[edit system services static-subscribers group <i>group-name</i> authentication username-include]</p>
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Specify that the name of the logical system is included as part of the username created for all static subscribers or for the static subscribers in a specified group. The group version of the statement takes precedence over the global version. The username is also sent to RADIUS in the Access-Request message.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Subscribers over Static Interfaces on page 466• Configuring the Static Subscriber Global Username on page 473• Configuring the Static Subscriber Group Username on page 478

logical-system-name (DHCP Local Server)

Syntax	logical-system-name;
Hierarchy Level	<p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server group group-name authentication username-include]</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...]</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server ...],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify that the logical system name be concatenated with the username during the subscriber authentication or DHCP client process. No logical system name is concatenated if the configuration is in the default logical system.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using External AAA Authentication Services with DHCP on page 217

logical-system-name (DHCP Relay Agent)

Syntax	logical-system-name;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay authentication username-include],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p>
Description	<p>Specify that the logical system name is concatenated with the username during the subscriber authentication or client authentication process. No logical system name is concatenated if the configuration is in the default logical system. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using External AAA Authentication Services with DHCP on page 217 • Creating Unique Usernames for DHCP Clients on page 218

ltv-syslog-interval (System Process)

Syntax	ltv-syslog-interval <i>seconds</i> ;
Hierarchy Level	[edit system processes dhcp-service]
Release Information	Statement introduced in Junos OS Release 14.1.
Description	Configure how often the router logs consolidated syslog messages for DHCP lease-time violations.
Options	<i>seconds</i> —Time interval that specifies how often the router logs syslog messages. Range: 600 through 86,400 seconds
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring a DHCP Lease-Time Threshold on page 209• <i>processes</i>


mac-address (DHCP Local Server)

Syntax	mac-address;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server group group-name authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify that the MAC address from the client PDU be concatenated with the username during the subscriber authentication or DHCP client authentication process.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Using External AAA Authentication Services with DHCP on page 217

mac-address (DHCP Relay Agent)

Syntax	mac-address;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay authentication username-include],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify that the MAC address from the client PDU be concatenated with the username during the subscriber authentication or client authentication process.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using External AAA Authentication Services with DHCP on page 217

maintain-subscriber (Subscriber Management)

Syntax	<code>maintain-subscriber { interface-delete; }</code>
Hierarchy Level	[edit system services subscriber-management]
Release Information	Statement introduced in Junos OS Release 11.1.
Description	Configure the router to maintain, rather than log out, subscribers when the specified type of event occurs (such as when an interface is deleted).
<div> NOTE: The <code>maintain-subscriber</code> statement and <code>remove-when-no-subscribers</code> statement are mutually exclusive. You cannot specify that dynamically configured VLAN interfaces are removed when no subscribers exist when the router is also configured to maintain subscribers.</div>	
The remaining statement is explained separately.	
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events on page 238

managed-configuration (Dynamic Router Advertisement)

Syntax	(managed-configuration no-managed-configuration);
Hierarchy Level	[edit dynamic-profiles protocols router-advertisement interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	<p>Specify whether to enable the dynamic host to use a stateful autoconfiguration protocol for address autoconfiguration, along with any stateless autoconfiguration already configured:</p> <ul style="list-style-type: none">• managed-configuration—Enable host to use stateful autoconfiguration.• no-managed-configuration—Disable host from using stateful autoconfiguration.
Default	The configured object is disabled unless explicitly enabled.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Example: Configuring IPv6 Interfaces and Enabling Neighbor Discovery</i>

map (Domain Map)

```
Syntax  map domain-map-name {
        aaa-logical-system logical-system-name {
            aaa-routing-instance routing-instance-name;
        }
        aaa-routing-instance (routing-instance-name | default);
        access-profile profile-name;
        address-pool pool-name;
        dynamic-profile profile-name;
        padn destination-address {
            mask destination-mask;
            metric route-metric;
        }
        strip-domain;
        target-logical-system logical-system-name {
            target-routing-instance routing-instance-name;
        }
        target-routing-instance (routing-instance-name | default);
        tunnel-profile profile-name;
        tunnel-switch-profile profile-name;
    }
```

Hierarchy Level [edit access [domain](#)]

Release Information Statement introduced in Junos OS Release 10.4.

Description Specify the domain map to use to map options and parameters to subscriber sessions based on the subscriber domain.

Options *domain-map-name*—Name of the domain map. The name is the same as the subscriber domain to which it will apply. For example, for the username `user1@xyz.com`, the domain map name is `xyz.com`.



NOTE: Use a domain map name of `default` to specify the domain map that the router uses when there is no match for the domain or realm name in the subscriber username.

Use a domain map name of `none` to specify the domain map the router uses when a subscriber username does not have a domain or realm name.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- [Configuring a Domain Map on page 131](#)

mask (Domain Map)

Syntax	<code>mask destination-mask;</code>
Hierarchy Level	[edit access domain map <i>domain-map-name</i> padn <i>destination-address</i>]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Configure the IP mask of the destination used in the PADN parameters for a domain map.
Options	destination-mask —Subnet mask of the destination.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring PADN Parameters for a Domain Map on page 140

match-direction (Services PTSP)

Syntax	<code>match-direction (input input-output output);</code>
Hierarchy Level	[edit services ptsp rule <i>rule-name</i>]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Specify the direction in which the rule match is applied.
Options	input —Apply the rule match on the input side of the interface. input-output —Apply the rule match bidirectionally. output —Apply the rule match on the output side of the interface.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>

max-advertisement-interval (Dynamic Router Advertisement)

Syntax	<code>max-advertisement-interval <i>seconds</i>;</code>
Hierarchy Level	[edit dynamic-profiles protocols router-advertisement interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	Maximum interval between each router advertisement message.
Options	<i>seconds</i> —Maximum interval. Range: 4 through 1800 seconds Default: 600 seconds
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>min-advertisement-interval (Protocols IPv6 Neighbor Discovery)</i>• <i>Example: Configuring IPv6 Interfaces and Enabling Neighbor Discovery</i>

max-data-sessions-per-subscriber

Syntax	<pre>max-data-sessions-per-subscriber { limit <i>max-sub-sessions</i>; exceed-action { drop; syslog; } }</pre>
Hierarchy Level	[edit services service-set <i>services-set-name</i> subscriber-profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Specify the maximum number of sessions that are concurrently enabled for the named service. The system randomly selects a number of sessions and enables the named service for them. To limit the service's use of resources, other sessions cannot access these named services.
Options	The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.

max-outstanding-requests

Syntax	<code>max-outstanding-requests requests;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> radius-server <i>server-address</i>], [edit access radius-server <i>server-address</i>]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	(M120, M320, MX Series routers) Configure the maximum number of outstanding requests for this RADIUS server. An increase in this value is immediate while a decrease is more gradual if the current number of outstanding requests exceeds the new value.
Options	requests —Maximum number of outstanding requests for this RADIUS server. Range: 0 through 2000 outstanding requests per server Default: 1000 outstanding requests per server
Required Privilege Level	system —To view this statement in the configuration. system-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Router or Switch Interaction with RADIUS Servers on page 99• Configuring RADIUS Server Options for Subscriber Access on page 102• show network-access aaa statistics on page 1164• clear network-access aaa statistics on page 1027

max-outstanding-requests (Gx-Plus)

Syntax	max-outstanding-requests <i>number</i> ;
Hierarchy Level	[edit access gx-plus global]
Release Information	Statement introduced in Junos OS Release 11.2. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Description	Limit the number of outstanding requests to the PCRF that Gx-Plus can retry when the requests are improperly answered. Too many requests risks overloading the PCRF and increases the chance of losing messages.
Options	<i>number</i> —Number of outstanding requests from Gx-Plus to the PCRF that can exist at any time. Default: 40 Range: 2 through 40
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Gx-Plus Global Attributes on page 448• Configuring Gx-Plus on page 446

max-pending-accounting-stops (Access Profile)

Syntax	max-pending-accounting-stops <i>number</i> ;
Hierarchy Level	[edit access accounting-backup-options]
Release Information	Statement introduced in Junos OS Release 13.1.
Description	Set the maximum number of pending accounting stop requests that the router backs up while all the RADIUS accounting servers in the profile are offline.
Options	<i>number</i> —Number of stops to hold. Range: 1 through 168,000 Default: 168,000
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Back-up Options for RADIUS Accounting on page 97

max-withhold-time (Access Profile)

Syntax	<code>max-withhold-time <i>hold-time</i>;</code>
Hierarchy Level	[edit access accounting-backup-options]
Release Information	Statement introduced in Junos OS Release 13.1.
Description	Set the timer that determines how long the router holds pending accounting stop requests. Any remaining accounting stop messages are flushed when the timer expires, even if the accounting server is again online.
Options	<i>hold-time</i> —Number of minutes. Range: 1 through 1440 Default: 60
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Back-up Options for RADIUS Accounting on page 97

maximum-discovery-table-entries

Syntax	<code>maximum-discovery-table-entries <i>entry-number</i>;</code>
Hierarchy Level	[edit protocols ancp], [edit protocols ancp neighbor ip-address]
Release Information	Statement introduced in Junos OS Release 9.5.
Description	Specify the maximum number of discovery table entries accepted from all ANCP neighbors or from a particular ANCP neighbor. The number of entries configured for an individual neighbor supersedes the global value. The neighbor can continue to update previously created entries when the maximum has been exceeded, but no new entries are accepted.
Default	No limit on the number of table entries
Options	<i>entry-number</i> —Maximum number of discovery table entries. Range: 1 through 100,000 Default: 100,000
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring the ANCP Agent on page 368 • Configuring ANCP Neighbors on page 369

maximum-helper-restart-time

Syntax	maximum-helper-restart-time <i>seconds</i> ;
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 9.4.
Description	Specify how long other router processes wait for the ANCP agent to restart before considering it to be down.
Options	seconds —Number of seconds other processes wait for ANCP to restart. Range: 45 through 600 seconds Default: 45 seconds
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the ANCP Agent on page 368• Specifying How Long Processes Wait for the ANCP Agent Restart to Complete on page 373

maximum-lease-time

Syntax	maximum-lease-time <i>seconds</i> ;
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family (inet inet6) dhcp-attributes]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	Specify the maximum length of time, in seconds, that the lease is held for a client if the client does not renew the lease. This is equivalent to DHCP option 51. The maximum-lease-time is mutually exclusive with both the preferred-lifetime and the valid-lifetime , and cannot be configured with either timer.
Options	seconds —Maximum number of seconds the lease can be held. Range: 30 through 4,294,967,295 seconds Default: 86,400 (24 hours)
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Address-Assignment Pools on page 316• DHCP Attributes for Address-Assignment Pools on page 201• preferred-lifetime (Address-Assignment Pools) on page 853• valid-lifetime (Address-Assignment Pools) on page 991

metric (Diameter Route)

Syntax	<code>metric route-metric;</code>
Hierarchy Level	[edit diameter network-statement <i>element-name</i> forwarding route <i>dne-route-name</i>]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Specify the metric associated with a destination and function. Together, these three elements define a route reachable through a Diameter network element. A lower metric makes a route more preferred.
Options	route-metric —Metric assigned to the route. Range: 0 through 255
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Diameter on page 434 • Configuring Diameter Network Elements on page 437

metric (Domain Map)

Syntax	<code>metric route-metric;</code>
Hierarchy Level	[edit access domain map <i>domain-map-name</i> padn <i>destination-address</i>]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Configure the route metric PADN parameter for a domain map.
Options	route-metric —Value assigned to the route. Range: 0 through 255
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring PADN Parameters for a Domain Map on page 140

min-advertisement-interval (Dynamic Router Advertisement)

Syntax	min-advertisement-interval <i>seconds</i> ;
Hierarchy Level	[edit dynamic-profiles protocols router-advertisement interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	Minimum interval between each router advertisement message.
Options	<p><i>seconds</i>—Minimum interval.</p> <p>Range: 3 seconds through three-quarter times the maximum advertisement interval value</p> <p>Default: One-third the maximum advertisement interval value</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• <i>max-advertisement-interval (Protocols IPv6 Neighbor Discovery)</i>• <i>Example: Configuring IPv6 Interfaces and Enabling Neighbor Discovery</i>

multi-address-embedded-option-response (DHCP Local Server)

Syntax	multi-address-embedded-option-response;
Hierarchy Level	[edit system services dhcp-local-server dhcpv6 overrides], [edit system services dhcp-local-server dhcpv6 group group-name overrides], [edit system services dhcp-local-server dhcpv6 group group-name interface interface-name overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 ...], [edit logical-systems <i>logical-system-name</i> system services system services dhcp-local-server dhcpv6 ...], [edit routing-instances <i>routing-instance-name</i> system services system services dhcp-local-server dhcpv6 ...]
Release Information	Statement introduced in Junos OS Release 12.3R3 and supported in later 12.3Rx releases. Statement supported in Junos OS Release 13.3 and later releases. (Not supported in Junos OS 13.1 and 13.2.)
Description	Configure DHCPv6 local server to return the DNS server address (DHCPv6 attribute 23) as a suboption in the respective IA_NA or IA_PD headers.
Default	DHCPv6 local server returns the DNS server address as a global DHCPv6 option.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Overriding How the DNS Server Address Is Returned in a DHCPv6 Multiple Address Environment on page 326 • Overriding Default DHCP Local Server Configuration Settings on page 255

name-server

Syntax	name-server [<i>server-names</i>];
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	Configure one or more Domain Name System (DNS) name servers available to the client to resolve hostname-to-client mappings. This is equivalent to DHCP option 6.
Options	<i>server-names</i> —IP addresses of the domain name servers, listed in order of preference.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Address-Assignment Pools on page 316

nas-identifier

Syntax	<code>nas-identifier <i>identifier-value</i>;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	Configure the value for the client RADIUS attribute 32 (NAS-Identifier). This attribute is used for authentication and accounting requests.
Options	<i>identifier-value</i> —String to use for authentication and accounting requests. Range: 1 through 64 characters
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Server Options for Subscriber Access on page 102• Configuring RADIUS Server Parameters for Subscriber Access on page 102

nas-port-extended-format (Access Profile)

Syntax

```
nas-port-extended-format {
    adapter-width width;
    ae-width width;
    port-width width;
    slot-width width;
    stacked-vlan-width width;
    vlan-width width;
    atm {
        adapter-width width;
        port-width width;
        slot-width width;
        vci-width width;
        vpi-width width;
    }
}
```

Hierarchy Level [edit access profile *profile-name* radius [options](#)]

Release Information Statement introduced in Junos OS Release 9.1.
 Statement introduced in Junos OS Release 9.1 for EX Series switches.
 Option **ae-width** introduced in Junos OS Release 12.1.
 Option **stacked** introduced in Junos OS Release 12.3.
 Option **atm** introduced in Junos OS Release 12.3R3 and supported in later 12.3Rx releases.
 Option **atm** supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)

Description In an access profile, configure the RADIUS client to use the extended format for RADIUS attribute 5 (NAS-Port) and specify the width of the fields in the NAS-Port attribute. You can use the same access profile to configure the NAS-Port extended format for Ethernet subscribers and ATM subscribers.

Options

- adapter-width *width***—Number of bits in the adapter field.
- ae-width *width***—Number of bits in the aggregated Ethernet identifier field.
- port-width *width***—Number of bits in the port field.
- slot-width *width***—Number of bits in the slot field.
- stacked**—Include stacked VLAN IDs, in addition to VLAN IDs, in the NAS-Port extended format.
- stacked-vlan-width *width***—Number of bits in the SVLAN ID field.
- vlan-width *width***—Number of bits in the VLAN ID field.
- atm**—Configure the NAS-Port extended format for ATM subscribers; options include:
 - **adapter-width *width***—Number of bits in the adapter field.
 - **port-width *width***—Number of bits in the port field.

- **slot-width *width***—Number of bits in the slot field.
- **vci-width *width***—Number of bits in the ATM virtual circuit identifier (VCI) field.
- **vpi-width *width***—Number of bits in the ATM virtual path identifier (VPI) field.



NOTE: Each field can be 0 through 32 bits wide; however, the total of the widths of all fields must not exceed 32 bits, or the configuration fails.

The router may truncate the values of individual fields depending on the bit width you specify.

Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
---------------------------------	---

Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Server Options for Subscriber Access on page 102• Configuring RADIUS Server Parameters for Subscriber Access on page 102
------------------------------	--

nas-port-extended-format (Interfaces)

Syntax

```
nas-port-extended-format {
    adapter-width width;
    ae-width width;
    port-width width;
    slot-width width;
    stacked;
    stacked-vlan-width width;
    vci-width width;
    vlan-width width;
    vpi-width width;
}
```

Hierarchy Level [edit interfaces *interface-name* radius-options **nas-port-options** *nas-port-options-name*]

Release Information Statement introduced in Junos OS Release 12.3.
Options **vci-width** and **vpi-width** introduced in Junos OS Release 12.3R3 and supported in later 12.3Rx releases.
Options **vci-width** and **vpi-width** supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)

Description Configure the RADIUS client to use the extended format for RADIUS attribute 5 (NAS-Port) and specify the width of the fields in the NAS-Port attribute.

Options

- adapter-width *width***—Number of bits in the adapter field.
- ae-width *width***—Number of bits in the aggregated Ethernet identifier field.
- port-width *width***—Number of bits in the port field.
- slot-width *width***—Number of bits in the slot field.
- stacked**—Include stacked VLAN IDs, in addition to VLAN IDs, in the NAS-Port extended format.
- stacked-vlan-width *width***—Number of bits in the SVLAN ID field.
- vci-width *width***—Number of bits in the ATM virtual circuit identifier (VCI) field.
- vlan-width *width***—Number of bits in the VLAN ID field.
- vpi-width *width***—Number of bits in the ATM virtual path identifier (VPI) field.



NOTE: Each field can be 0 through 32 bits wide; however, the total of the widths of all fields must not exceed 32 bits, or the configuration fails.

The router may truncate the values of individual fields depending on the bit width you specify.

Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 63• Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 62

nas-port-id-delimiter (Subscriber Management)

Syntax	nas-port-id-delimiter <i>delimiter-character</i> ;
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	Statement introduced in Junos OS Release 11.4. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Description	Specify the character that the router uses as a separator between the concatenated values in the NAS-Port-ID string. The router uses the delimiter when you configure more than one value in the nas-port-id-format statement.
Default	The hash (#) character.
Options	<i>delimiter-character</i> —Character used for the delimiter.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Server Options for Subscriber Access on page 102• Configuring RADIUS Server Parameters for Subscriber Access on page 102• Configuring a NAS-Port-ID with Additional Options on page 56

nas-port-id-format (Subscriber Management)

Syntax	<pre>nas-port-id-format { agent-circuit-id; agent-remote-id; interface-description; nas-identifier; }</pre>
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	<p>Statement introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p>
Description	Specify the information that the router includes in the NAS-Port-ID (RADIUS attribute 87) that it is passed to the RADIUS server during authentication and accounting. You can include any combination of the optional values.
Default	The router includes the interface description.
Options	<p>agent-circuit-id—Include the agent circuit ID from either DHCP option 82 or the DSL forum VSAs.</p> <p>agent-remote-id—Include the agent remote ID from either DHCP option 82 or the DSL forum VSAs.</p> <p>interface-description—Include the interface description.</p> <p>nas-identifier—Include the NAS identifier value (RADIUS attribute 32).</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring RADIUS Server Options for Subscriber Access on page 102 • Configuring RADIUS Server Parameters for Subscriber Access on page 102 • Configuring a NAS-Port-ID with Additional Options on page 56

nas-port-options (RADIUS Options)

Syntax `nas-port-options nas-port-options-name {
 nas-port-extended-format {
 adapter-width width;
 ae-width width;
 port-width width;
 slot-width width;
 stacked;
 stacked-vlan-width width;
 vci-width width;
 vlan-width width;
 vpi-width width;
 }
 nas-port-type port-type;
 stacked-vlan-ranges (any | low-outer-tag–high-outer-tag),any;
 vlan-ranges (any | low-tag–high-tag);
 }`

Hierarchy Level [edit interfaces *interface-name* *radius-options*]

Release Information Statement introduced in Junos OS Release 12.3.

Description Create a NAS-Port options definition to configure the NAS-Port-Type (61) RADIUS IETF attribute, and an extended format for the NAS-Port (5) RADIUS IETF attribute, on a per-physical interface, per-VLAN, or per-stacked VLAN (S-VLAN) basis. Each NAS-Port options definition includes the NAS-Port extended format, the NAS-Port-Type, and either the VLAN range of subscribers or the S-VLAN range of subscribers to which the definition applies.



NOTE: You can configure a maximum of 16 NAS-Port options definitions per physical interface. Each definition can include a maximum of 32 VLAN ranges or 32 S-VLAN ranges, but cannot include a combination of VLAN ranges and S-VLAN ranges.

Options *nas-port-options-name*—Name of the NAS-Port options definition.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 63](#)
- [Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 62](#)

nas-port-type (Subscriber Management)

Syntax `nas-port-type {
 ethernet {
 port-type;
 }
 }`

Hierarchy Level [edit access profile *profile-name* radius [options](#)]

Release Information Statement introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.

Description Specify the port type used to authenticate subscribers. The router includes the port type in RADIUS attribute 61 (NAS-Port-Type attribute).



NOTE: This statement is ignored if the [ethernet-port-type-virtual](#) statement is included in the same access profile.

Default The router uses a port type of **ethernet**.

Options *port-type*—One of the following port types:

- *value*—A value from 0-65535
- **adsl-cap**—Asymmetric DSL, carrierless amplitude phase (CAP) modulation
- **adsl-dmt**—Asymmetric DSL, discrete multitone (DMT)
- **async**—Asynchronous
- **cable**—Cable
- **ethernet**—Ethernet
- **fddi**—Fiber Distributed Data Interface
- **g3-fax**—G.3 Fax
- **hdlc-clear-channel**—HDLC Clear Channel
- **iapp**—Inter-Access Point Protocol (IAPP)
- **isdsl**—ISDN DSL
- **isdn-sync**—ISDN Synchronous
- **isdn-v110**—ISDN Async V.110
- **isdn-v120**—ISDN Async V.120
- **piafs**—Personal Handyphone System (PHS) Internet Access Forum Standard
- **sdsl**—Symmetric DSL

- **sync**—Synchronous
- **token-ring**—Token Ring
- **virtual**—Virtual
- **wireless**—Other wireless
- **wireless-1x-ev**—Wireless 1xEV
- **wireless-cdma2000**—Wireless code division multiple access (CDMA) 2000
- **wireless-ieee80211**—Wireless 802.11
- **wireless-umts**—Wireless universal mobile telecommunications system (UMTS)
- **x25**—X.25
- **x75**—X.75
- **xdsl**—DSL of unknown type

Required Privilege	admin—To view this statement in the configuration.
Level	admin-control—To add this statement to the configuration.

Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Server Options for Subscriber Access on page 102• Configuring RADIUS Server Parameters for Subscriber Access on page 102
------------------------------	--

nas-port-type (RADIUS Options)

Syntax	<code>nas-port-type <i>port-type</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> radius-options nas-port-options <i>nas-port-options-name</i>]
Release Information	Statement introduced in Junos OS Release 12.3.
Description	Specify the port type used to authenticate subscribers. The router includes the port type in the NAS-Port-Type (61) RADIUS IETF attribute.
Default	If you do not include the nas-port-type statement at the [edit interfaces <i>interface-name</i> radius-options nas-port-options <i>nas-port-options-name</i>] hierarchy level, the global value configured for nas-port-type at the [edit access profile <i>profile-name</i> radius options] hierarchy level takes effect.
Options	<p><i>port-type</i>—One of the following port types:</p> <ul style="list-style-type: none"> <i>value</i>—A value from 0 through 65535 adsl-cap—Asymmetric DSL, carrierless amplitude phase (CAP) modulation adsl-dmt—Asymmetric DSL, discrete mutilating (DOT) async—Asynchronous cable—Cable ethernet—Ethernet fdi—Fiber Distributed Data Interface g3-fax—G.3 Fax hdlc-clear-channel—HDLC Clear Channel iapp—Inter-Access Point Protocol (IAPP) idsl—ISDN DSL isdn-sync—ISDN Synchronous isdn-v110—ISDN Async V.110 isdn-v120—ISDN Async V.120 piafs—Personal Handyphone System (PHS) Internet Access Forum Standard sdsl—Symmetric DSL sync—Synchronous token-ring—Token Ring virtual—Virtual wireless—Other wireless wireless-1x-ev—Wireless 1xEV

- **wireless-cdma2000**—Wireless code division multiple access (CDMA) 2000
- **wireless-ieee80211**—Wireless 802.11
- **wireless-umts**—Wireless universal mobile telecommunications system (UMTS)
- **x25**—X.25
- **x75**—X.75
- **xdsl**—DSL of unknown type

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- [Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 63](#)
- [Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 62](#)

neighbor (Define ANCP)

Syntax `neighbor ip-address {
 adjacency-timer seconds;
 ietf-mode;
 maximum-discovery-table-entries;
 pre-ietf-mode;
}`

Hierarchy Level [edit protocols **ancp**]

Release Information Statement introduced in Junos OS Release 9.4.

Description Configure an ANCP neighbor with which the ANCP agent on the router forms an adjacency for reporting and shaping traffic.

Options *ip-address*—IP address of the ANCP neighbor.

The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- [Configuring the ANCP Agent on page 368](#)
- [Configuring ANCP Neighbors on page 369](#)

neighbor-discovery-router-advertisement (Address-Assignment Pools)

Syntax	<code>neighbor-discovery-router-advertisement <i>ndra-pool-name</i>;</code>
Hierarchy Level	[edit access address-assignment]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	Configure the name of the address-assignment pool used to assign the router advertisement prefix.
Options	<i>ndra-pool-name</i> —Name of the address-assignment pool.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Address-Assignment Pools Overview on page 315 • Configuring an Address-Assignment Pool for Router Advertisement

netbios-node-type

Syntax	<code>netbios-node-type <i>node-type</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	Specify the NetBIOS node type. This is equivalent to DHCP option 46.
Options	<i>node-type</i> —One of the following node types: <ul style="list-style-type: none"> • b-node—Broadcast node • h-node—Hybrid node • m-node—Mixed node • p-node—Peer-to-peer node
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Address-Assignment Pools on page 316

network

Syntax	<code>network <i>ip-prefix</i></<i>prefix-length</i>>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	Configure subnet information for an IPv4 address-assignment pool.
Options	<i>ip-prefix</i> —IP version 4 address or prefix value. <i>prefix-length</i> —(Optional) Subnet mask.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Address-Assignment Pools on page 316

network-element (Diameter Base Protocol)

```
Syntax  network-element element-name {
        forwarding {
            route dne-route-name {
                destination realm realm-name <host hostname> ;
                function function-name <partition partition-name>;
                metric route-metric;
            }
        }
        function function-name;
        peer peer-name {
            priority priority-number;
        }
    }
```

Hierarchy Level [edit [diameter](#)]

Release Information Statement introduced in Junos OS Release 9.6.

Description Specify the transport layer Diameter configuration. The Diameter network element includes a list of routes reachable through the Diameter instance, associated functions, and prioritized Diameter peers.


Options *element-name*—Name of the network element.
The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- [Configuring Diameter on page 434](#)
- [Configuring Diameter Network Elements on page 437](#)

no-bind-on-request (DHCP Relay Agent)

Syntax	no-bind-on-request;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay dhcpv6 overrides], [edit forwarding-options dhcp-relay overrides], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides], [edit forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.4. Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4. Statement introduced in Junos OS Release 12.3 for EX Series switches.</p>
Description	<p>Explicitly disable automatic binding of received DHCP request messages that have no entry in the database (<i>stray</i> requests). Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.</p> <p>M120 and M320 routers do not support DHCPv6.</p>
	<div>  <p>NOTE: Beginning with Junos OS Release 10.4, automatic binding of stray requests is enabled by default. In Junos OS Release 10.3 and earlier releases, automatic binding of stray requests is disabled by default.</p> </div>
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</p>

- Related Documentation**
- [Extended DHCP Relay Agent Overview on page 194](#)
 - [Overriding the Default DHCP Relay Configuration Settings on page 256](#)
 - [Disabling Automatic Binding of Stray DHCP Requests on page 265](#)

on-link (Dynamic Router Advertisement)

Syntax	(on-link no-on-link);
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols router-advertisement interface <i>interface-name</i> prefix <i>prefix</i>]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	Specify whether to enable prefixes to be used for onlink determination: <ul style="list-style-type: none"> • no-on-link—Disable prefixes from being used for onlink determination. • on-link—Enable prefixes to be used for onlink determination.
Default	The configured object is enabled unless explicitly disabled.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Example: Configuring IPv6 Interfaces and Enabling Neighbor Discovery</i>

no-vlan-interface-name

Syntax no-vlan-interface-name;

Hierarchy Level [edit forwarding-options dhcp-relay **dhcpv6** (**relay-agent-interface-id** | **relay-agent-remote-id**)],
 [edit forwarding-options dhcp-relay **dhcpv6** group *group-name* (**relay-agent-interface-id** | **relay-agent-remote-id**)],
 [edit forwarding-options dhcp-relay relay-option-82 (circuit-id | **remote-id**)],
 [edit forwarding-options dhcp-relay group *group-name* relay-option-82 (circuit-id | **remote-id**)],
 [edit logical-systems *logical-system-name* ... forwarding-options dhcp-relay **dhcpv6** (**relay-agent-interface-id** | **relay-agent-remote-id**)],
 [edit logical-systems *logical-system-name* ... forwarding-options dhcp-relay ... relay-option-82 (circuit-id | **remote-id**)],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay **dhcpv6** (**relay-agent-interface-id** | **relay-agent-remote-id**)],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay ... relay-option-82 (circuit-id | **remote-id**)],
 [edit vlans *vlan-name* forwarding-options dhcp-security dhcpv6-options option-18],
 [edit vlans *vlan-name* forwarding-options dhcp-security dhcpv6-options option-37]

Release Information Statement introduced in Junos OS Release 14.1.



NOTE: The EX Series switches that support the **no-vlan-interface-name** statement are the EX4300, EX4600, and EX9200 switches.

Description When you do not want bridge domain or VLAN tag information, do not include the VLAN ID nor the VLAN interface name (the default) in the circuit or remote ID value in the DHCP option 82 information.



NOTE: The **no-vlan-interface-name** statement is mutually exclusive with the **use-interface-description** and **use-vlan-id** statements.

When you configure the **no-vlan-interface-name** statement only, the format displays only the Layer 3 interface:

```
irb.subunit
```



NOTE: The *subunit* is required and used to differentiate the interface for remote systems.

When you configure the **no-vlan-interface-name** and **use-interface-description** statements, the format displays the IRB interface description:

irb_descr

If you configure the **no-vlan-interface-name** and **use-interface-description** statements, and no description for the IRB interface is found, the format displays the IRB interface name:

irb.subunit

When you configure the **no-vlan-interface-name** and **include-irb-and-l2** statements, the format displays the Layer 2 logical interface name and the IRB interface name:

(fe | ge)-fpc/pic/port.subunit+irb.subunit

When you configure the **no-vlan-interface-name**, **include-irb-and-l2** and **use-interface-name** statements, the format displays the Layer 2 interface description and the IRB interface name:

l2_descr+irb.subunit

If you configure the **no-vlan-interface-name**, **include-irb-and-l2** and **use-interface-name** statements, and no description for the Layer 2 interface is found, the format displays the Layer 2 logical interface name and the IRB interface name:

(fe | ge)-fpc/pic/port.subunit+irb.subunit

Required Privilege	routing—To view this statement in the configuration.
Level	routing-control—To add this statement to the configuration.

Related Documentation	<ul style="list-style-type: none"> • Including a Textual Description in DHCP Options on page 271 • Using DHCP Relay Agent Option 82 Information on page 266 • Configuring DHCPv6 Relay Agent Options on page 296
------------------------------	---

option

Syntax	<pre>option { [(id-number option-type option-value) (id-number array option-type option-value)]; }</pre>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family (inet inet6) dhcp-attributes]
Release Information	Statement introduced in Junos OS Release 9.0. hex-string option type introduced in Junos OS Release 13.3.
Description	Specify user-defined options that are added to client packets.
Options	<p>array—An option can include an array of option types.</p> <p>id-number—Any whole number. The ID number is used to index the option and must be unique across a DHCP server.</p> <p>option-type—Any of the following types: byte, byte-stream, flag, hex-string, integer, ip-address, short, string, unsigned-integer, or unsigned-short.</p> <p>option-value—Value associated with an option. The option value must be compatible with the option type (for example, an On or Off value for a flag type).</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Address-Assignment Pools on page 316


option-60 (DHCP Local Server)

Syntax	option-60;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify that the payload of Option 60 (Vendor Class Identifier) from the client PDU be concatenated with the username during the subscriber authentication or DHCP client authentication process.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using External AAA Authentication Services with DHCP on page 217

option-60 (DHCP Relay Agent)

Syntax	option-60;
Hierarchy Level	[edit forwarding-options dhcp-relay authentication username-include], [edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Specify that the payload of the Option 60 (Vendor Class Identifier) from the client PDU is concatenated with the username during the subscriber authentication or client authentication process.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Using External AAA Authentication Services with DHCP on page 217

option-82 (DHCP Relay Agent)

Syntax	<code>option-82 <circuit-id> <remote-id>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay authentication username-include],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify the option 82 that is concatenated with the username during the subscriber authentication or client authentication process. You can specify either, both, or neither the Agent Circuit ID and the Agent Remote ID suboptions. If you specify both, the Agent Circuit ID is supplied first, followed by a delimiter, and then the Agent Remote ID. If neither suboption is supplied, the raw payload of option 82 is concatenated to the username.
<div>  <p>NOTE: The option 82 value used in creating the username is based on the option 82 value that is encoded in the outgoing (relayed) PDU.</p> </div>	
Options	<p>circuit-id—(Optional) The string for the Agent Circuit ID suboption (suboption 1).</p> <p>remote-id—(Optional) The string for the Agent Remote ID suboption (suboption 2).</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using External AAA Authentication Services with DHCP on page 217

option-82 (DHCP Local Server Authentication)

Syntax	<code>option-82 <circuit-id> <remote-id>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	<p>Specify the type of Option 82 information from the client PDU that is concatenated with the username during the subscriber authentication or DHCP client authentication process. You can specify either, both, or neither of the Agent Circuit ID and Agent Remote ID suboptions. If you specify both, the Agent Circuit ID is supplied first, followed by a delimiter, and then the Agent Remote ID. If you specify that neither suboption is supplied, the raw payload of Option 82 from the PDU is concatenated to the username.</p>
Options	<p>circuit-id—(Optional) Agent Circuit ID suboption (suboption 1).</p> <p>remote-id—(Optional) Agent Remote ID suboption (suboption 2).</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using External AAA Authentication Services with DHCP on page 217

option-82 (DHCP Local Server Pool Matching)

Syntax	option-82;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server pool-match-order],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server pool-match-order],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server pool-match-order],</p> <p>[edit system services dhcp-local-server pool-match-order]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.0.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	<p>Configure the extended DHCP local server to use the option 82 value in the DHCP client DHCP PDU together with the ip-address-first method to determine which address-assignment pool to use. You must configure the ip-address-first statement before configuring the option-82 statement. The DHCP local server first determines which address-assignment pool to use based on the ip-address-first method. Then, the local server matches the option 82 value in the client PDU with the option 82 configuration in the address-assignment pool. This statement is supported for IPv4 address-assignment pools only.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 203 • Extended DHCP Local Server Overview on page 188 • Address-Assignment Pools Overview on page 315


option-82 (Address-Assignment Pools)

Syntax	<pre>option-82 { circuit-id value range named-range; remote-id value range named-range; }</pre>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes option-match]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	<p>Specify the list of option 82 suboption match criteria used to select the named address range used for the client. The server matches the option 82 value in the user PDU to the specified option 82 match criteria and uses the named address range associated with the string.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Address-Assignment Pools on page 316

option-match

Syntax	<pre>option-match { option-82 { circuit-id value range named-range; remote-id value range named-range; } }</pre>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	<p>Specify a list of match criteria used to determine which named address range in the address-assignment pool to use. The extended DHCP local server matches this information to the match criteria specified in the client PDUs. For example, for option 82 match criteria, the server matches the option 82 value in the user PDU to the specified option 82 string and uses the named range associated with the string.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Address-Assignment Pools on page 316

option-number (DHCP Relay Agent Option)

Syntax	<code>option-number <i>option-number</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay relay-option], [edit forwarding-options dhcp-relay dhcpv6 relay-option], [edit forwarding-options dhcp-relay group group-name relay-option], [edit forwarding-options dhcp-relay dhcpv6 group group-name relay-option], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...]</p>
Release Information	<p>Statement introduced in Junos OS Release 12.3.</p> <p>Statement introduced in Junos OS Release 12.3 for EX Series switches.</p>
Description	<p>Specify the DHCP option DHCP relay agent uses for selective processing of client traffic. You can configure support globally or for a named group of interfaces. You can also configure support for the extended DHCP relay agent on a per logical system and per routing instance basis.</p> <p>Use the [edit forwarding-options dhcp-relay dhcpv6] hierarchy level to configure the DHCPv6 relay agent support.</p>
Options	<i>option-number</i> —The DHCP or DHCPv6 option in the incoming traffic.
<div>  NOTE: EX Series switches do not support the User Class Options. </div>	
<ul style="list-style-type: none"> 15 (DHCPv6 only)—Use DHCPv6 option 15 (User Class Option) in packets 16 (DHCPv6 only)—(MX Series routers and EX Series switches only) Use DHCPv6 option 16 (Vendor Class Option) in packets 60 (DHCPv4 only)—(MX Series routers and EX Series switches only) Use DHCP option 60 (Vendor Class Identifier) in DHCP packets 77 (DHCPv4 only)—Use DHCP option 77 (User Class Identifier) in packets 	
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Using DHCP Option Information to Selectively Process DHCP Client Traffic on page 273 Configuring an Extended DHCP Relay Server on EX Series Switches (CLI Procedure)

options (Access Profile)

```
Syntax  options {
        accounting-session-id-format (decimal | description);
        calling-station-id-delimiter delimiter-character;
        calling-station-id-format {
            agent-circuit-id;
            agent-remote-id;
            interface-description;
            nas-identifier;
        }
        client-accounting-algorithm (direct | round-robin);
        client-authentication-algorithm (direct | round-robin);
        coa-dynamic-variable-validation;
        ethernet-port-type-virtual;
        access-loop-id-local;
        interface-description-format {
            exclude-adapter;
            exclude-sub-interface;
        }
        ip-address-change-notify message;
        juniper-dsl-attributes;
        nas-identifier identifier-value;
        nas-port-extended-format {
            adapter-width width;
            ae-width width;
            port-width width;
            slot-width width;
            stacked-vlan-width width;
            vlan-width width;
            atm {
                adapter-width width;
                port-width width;
                slot-width width;
                vci-width width;
                vpi-width width;
            }
        }
        nas-port-id-delimiter delimiter-character;
        nas-port-id-format {
            agent-circuit-id;
            agent-remote-id;
            interface-description;
            nas-identifier;
        }
        nas-port-type {
            ethernet {
                port-type;
            }
        }
        revert-interval interval;
        vlan-nas-port-stacked-format;
    }
```

Hierarchy Level	[edit access profile <i>profile-name</i> radius]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	Configure the options used by RADIUS authentication and accounting servers. The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring RADIUS Server Options for Subscriber Access on page 102 • RADIUS Server Options for Subscriber Access on page 4

order

Syntax	order [<i>accounting-method</i>];
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	Set the order in which the Junos OS tries different accounting methods for client activity. When a client logs in, the software tries the accounting methods in the specified order.
Options	<i>accounting-method</i> —One or more accounting methods. When a client logs in, the software tries the accounting methods in the following order, from first to last. The only valid value is radius for RADIUS accounting.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Authentication and Accounting Parameters for Subscriber Access on page 80


origin (Diameter Base Protocol)

Syntax	origin { host <i>hostname</i> ; realm <i>realm-name</i> ; }
Hierarchy Level	[edit diameter]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	<p>Specify values of Origin-Realm-AVP and Origin-Host-AVP used in all messages sent by the Diameter instance.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Diameter on page 434• Configuring the Origin Attributes of the Diameter Instance on page 435

other-stateful-configuration (Dynamic Router Advertisement)

Syntax	(other-stateful-configuration no-other-stateful-configuration);
Hierarchy Level	[edit dynamic-profiles protocols router-advertisement interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	<p>Specify whether to enable autoconfiguration of other nonaddress-related information:</p> <ul style="list-style-type: none">• no-other-stateful-configuration—Disable autoconfiguration of other nonaddress-related information.• other-stateful-configuration—Enable autoconfiguration of other nonaddress-related information.
Default	The configured object is disabled unless explicitly enabled.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Example: Configuring IPv6 Interfaces and Enabling Neighbor Discovery</i>

overhead-accounting (ANCP)

Syntax	overhead-accounting;
Hierarchy Level	[edit protocols ancp interfaces <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	<p>Prevent ANCP from performing an adjustment on the actual downstream data rate that ANCP receives from the DSLAM for the difference between the customer premise equipment (CPE) protocol overhead and the B-RAS protocol overhead. You include this statement when you want CoS to perform the adjustment on the data rate from the DSLAM according to the overhead accounting configuration in a CoS traffic control profile.</p> <p>When this statement is not configured (the default condition), ANCP makes the traffic rate adjustment according to the configuration of the qos-adjust-line-type statements and reports that rate to CoS. CoS then applies (if configured) the adjustment set by the overhead-accounting statement in the CoS traffic profile.</p>
	<div>  <p>NOTE: ANCP reports a traffic rate to CoS only if the qos-adjust statement at the [edit protocols ancp] hierarchy level has been configured.</p> </div>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring the ANCP Agent on page 368

overrides (DHCP Local Server)

Syntax	<pre> overrides { allow-no-end-option; client-discover-match (option60-and-option82 incoming-interface); delegated-pool; interface-client-limit <i>number</i>; multi-address-embedded-option-response; process-inform { pool <i>pool-name</i>; } rapid-commit; } </pre>
Hierarchy Level	<pre> [edit system services dhcp-local-server], [edit system services dhcp-local-server dhcpv6], [edit system services dhcp-local-server dhcpv6 group group-name], [edit system services dhcp-local-server dhcpv6 group group-name interface interface-name], [edit system services dhcp-local-server group group-name], [edit system services dhcp-local-server group group-name interface interface-name], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server ...], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...] </pre>
Release Information	<p>Statement introduced in Junos OS Release 9.2.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p> <p>Support for the allow-no-end-option option introduced in Junos OS Release 14.1X53-D15 for EX Series switches.</p>
Description	<p>Override the default configuration settings for the extended DHCP local server. Specifying the overrides statement with no subordinate statements removes all DHCP local server overrides at that hierarchy level.</p> <ul style="list-style-type: none"> To override global DHCP local server configuration options, include the overrides statement and its subordinate statements at the [edit system services dhcp-local-server] hierarchy level. To override configuration options for a named group of interfaces, include the statements at the [edit system services dhcp-local-server group group-name] hierarchy level. To override configuration options for a specific interface within a named group of interfaces, include the statements at the [edit system services dhcp-local-server group group-name interface interface-name] hierarchy level. Use the [edit system services dhcp-local-server dhcpv6] hierarchy level to override DHCPv6 configuration options. <p>The remaining statements are explained separately.</p> <p>The interface-client-limit statement is not supported in the [edit system services dhcp-local-server dhcpv6] hierarchy level.</p>

The [delegated-pool](#), [multi-address-embedded-option-response](#), and the [rapid-commit](#) statements are supported in the `[edit system services dhcp-local-server dhcpv6 ...]` hierarchy level only.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

Related Documentation

- [Extended DHCP Local Server Overview on page 188](#)
- [Overriding Default DHCP Local Server Configuration Settings on page 255](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 258](#)
- [Configuring a DHCP Server on Switches \(CLI Procedure\)](#)

overrides (DHCP Relay Agent)

Syntax	<pre> overrides { allow-snooped-clients; allow-no-end-options; always-write-giaddr; always-write-option-82; client-discover-match (option60-and-option82 incoming-interface); delay-authentication; delete-binding-on-renegotiation; disable-relay; interface-client-limit <i>number</i>; layer2-unicast-replies; no-allow-snooped-clients; no-bind-on-request; proxy-mode; replace-ip-source-with; send-release-on-delete; trust-option-82; } </pre>
Hierarchy Level	<pre> [edit forwarding-options dhcp-relay], [edit forwarding-options dhcp-relay dhcpv6], [edit forwarding-options dhcp-relay group <i>group-name</i>], [edit forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i>], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i>], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...] </pre>
Release Information	<p>Statement introduced in Junos OS Release 8.3.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p> <p>Support for the delete-binding-on-renegotiation statement introduced in Junos OS Release 13.2 for EX Series switches.</p> <p>Support for the allow-no-end-options statement introduced in Junos OS Release 14.1X53 for EX Series switches.</p>
Description	<p>Override the default configuration settings for the extended DHCP relay agent. Specifying the overrides statement with no subordinate statements removes all DHCP relay agent overrides at that hierarchy level. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.</p> <p>M120 and M320 routers do not support DHCPv6.</p> <p>The following statements are supported at both the [edit ... dhcp-relay] and [edit ... dhcpv6] hierarchy levels. All other statements are supported at the dhcp-relay hierarchy levels only.</p> <ul style="list-style-type: none"> • allow-snooped-clients

- `interface-client-limit`
- `no-allow-snooped-clients`
- `no-bind-on-request`
- `send-release-on-delete`

The remaining statements are explained separately.

Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Extended DHCP Relay Agent Overview on page 194 • Overriding the Default DHCP Relay Configuration Settings on page 256 • Deleting DHCP Local Server and DHCP Relay Override Settings on page 258 • dhcp-relay on page 689

packet-triggered-subscribers

Syntax

```
packet-triggered-subscribers {
  partition partition-name {
    destination-host hostname;
    destination-realm realm;
    diameter-instance instance-name;
  }
  traceoptions {
    file filename <files number> <match regular-expression > <size maximum-file-size>
      <world-readable | no-world-readable>;
    flag flag <disable>;
    no-remote-trace;
  }
}
```

Hierarchy Level [edit system services]

Release Information Statement introduced in Junos OS Release 10.2.

Description Configure PTSP to interact with an SAE in an SRC environment to provision packet-triggered subscribers.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- [Configuring the PTSP Partition on page 491](#)

packet-triggered-subscribers-partition

Syntax	packet-triggered-subscribers-partition <i>partition-name</i> ;
Hierarchy Level	[edit system]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Specify the PTSP partition to associate with the logical system and routing instance.
Options	<i>partition-name</i> —Name of the PTSP partition that you want PTSP to use. The name is defined with the partition statement at the [edit system services packet-triggered-subscribers] hierarchy level.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Assigning the PTSP Partition on page 492

padn (Domain Map)

Syntax	padn <i>destination-address</i> { <i>mask</i> <i>destination-mask</i> ; <i>metric</i> <i>route-metric</i> ; }
Hierarchy Level	[edit access domain map <i>domain-map-name</i>]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Configure PADN parameters for a domain map.
Options	<i>destination-address</i> —IP address of the destination. The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring PADN Parameters for a Domain Map on page 140

parse-direction (Domain Map)

Syntax	parse-direction (left-to-right right-to-left);
Hierarchy Level	[edit access domain]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Specify the direction in which the router searches for the domain name in a username.
Default	left-to-right
Options	<p>left-to-right—The router searches starting at the left-most character. When the router reaches a domain delimiter, it uses anything to the right of the delimiter as the domain name.</p> <p>right-to-left—The router searches starting at the right-most character. When the router reaches a domain delimiter, it uses anything to the right of the delimiter as the domain name.</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Specifying the Parsing Direction for Domain and Realm Names on page 138• Configuring Domain and Realm Name Usage for Domain Maps on page 136

parse-order (Domain Map)

Syntax	parse-order (domain-first realm-first);
Hierarchy Level	[edit access domain]
Release Information	Statement introduced in Junos OS Release 14.1.
Description	Specify the order in which the router searches for a domain name, either the domain first, or the realm first.
Default	domain-first
Options	<p>domain-first—The router searches for a domain name first. When the router reaches a domain delimiter, it uses anything to the right of the delimiter as the domain name.. If no domain is found, then the router searches for a realm. If the router does not find either a domain or realm, then there is no domain.</p> <p>realm-first—The router searches for a realm name first. When the router reaches a realm delimiter, it uses anything to the left of the delimiter as the domain name. If no realm is found, then the router searches for a domain. If the router does not find either a domain or realm, then there is no domain.</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Specifying the Parsing Direction for Domain and Realm Names on page 138• Configuring Domain and Realm Name Usage for Domain Maps on page 136

partition

Syntax	<pre>partition <i>partition-name</i> { <i>diameter-instance</i> <i>instance-name</i>; <i>destination-host</i> <i>hostname</i>; <i>destination-realm</i> <i>realm</i>; }</pre>
Hierarchy Level	[edit jsrc]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Configure a JSRC partition.
Options	<p><i>partition-name</i>—Name of the JSRC partition.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring JSRC on page 455 • Configuring the JSRC Partition on page 456

partition (Gx-Plus)

Syntax	<pre>partition <i>partition-name</i> { <i>diameter-instance</i> <i>instance-name</i>; <i>destination-host</i> <i>hostname</i>; <i>destination-realm</i> <i>realm</i>; }</pre>
Hierarchy Level	[edit access gx-plus]
Release Information	<p>Statement introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.</p>
Description	Configure a Gx-Plus partition.
Options	<p><i>partition-name</i>—Name of the Gx-Plus partition.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Gx-Plus on page 446 • Configuring the Gx-Plus Partition on page 447

partition (PTSP)

Syntax	<pre>partition <i>partition-name</i> { destination-host <i>hostname</i>; destination-realm <i>realm</i>; diameter-instance <i>instance-name</i>; }</pre>
Hierarchy Level	[edit system services packet-triggered-subscribers]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Configure a PTSP partition.
Options	<p><i>partition-name</i>—Name of the PTSP partition.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring the PTSP Partition on page 491

password (Static Subscribers)

Syntax	<pre>password password-string; username-include { domain-name domain-name; username-include; logical-system-name; routing-instance-name; user-prefix user-prefix-string; }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers group <i>group-name</i> authentication],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers authentication],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication username-include], authentication],</p> <p>[edit system services static-subscribers authentication],</p> <p>[edit system services static-subscribers group <i>group-name</i> authentication]</p>
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Specify the password that is sent to AAA for user login for all static subscribers on interfaces configured at the [edit system services static-subscribers interface] hierarchy level, or for the subscribers in a specified group. The group version of the statement takes precedence over the global version.
Options	<p>password-string—String that defines the password.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system-level—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Subscribers over Static Interfaces on page 466 • Configuring the Static Subscriber Global Authentication Password on page 473 • Configuring the Static Subscriber Group Authentication Password on page 477

password (DHCP Local Server)

Syntax	<code>password password-string;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group group-name authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group group-name authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication],</p> <p>[edit system services dhcp-local-server authentication],</p> <p>[edit system services dhcp-local-server dhcpv6],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name authentication],</p> <p>[edit system services dhcp-local-server group group-name authentication]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Configure the password that is sent to the external AAA authentication server for subscriber authentication or DHCP client authentication.
Options	<i>password-string</i> —Authentication password.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using External AAA Authentication Services with DHCP on page 217

password (DHCP Relay Agent)

Syntax	<code>password password-string;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay authentication], [edit forwarding-options dhcp-relay dhcpv6 authentication], [edit forwarding-options dhcp-relay group <i>group-name</i> authentication], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 authentication], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p>
Description	Configure the password that is sent to the external AAA authentication server for subscriber authentication or client authentication. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.
Options	<i>password-string</i> —Authentication password.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using External AAA Authentication Services with DHCP on page 217 • Configuring Passwords for Usernames on page 221

peer (Diameter Base Protocol)

Syntax	<pre>peer <i>peer-name</i> { address <i>ip-address</i>; connect-actively { port <i>port-number</i>; transport <i>transport-name</i>; } logical-system <i>logical-system-name</i> <routing-instance <i>routing-instance-name</i>>; routing-instance <i>routing-instance-name</i>; }</pre>
Hierarchy Level	[edit diameter]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Configure a remote peer for the Diameter instance.
Options	<p><i>peer-name</i>—Name of the peer.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Diameter on page 434• Configuring Diameter Peers on page 435

peer (Diameter Network Element)

Syntax	<pre>peer <i>peer-name</i> { priority <i>priority-value</i>; }</pre>
Hierarchy Level	[edit diameter network-element <i>element-name</i>]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Define and prioritize a peer associated with a Diameter network element.
Options	<p><i>peer-name</i>—Name of the peer.</p> <p>The remaining statement is explained separately.</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Diameter on page 434• Configuring Diameter Network Elements on page 437

pool (Address-Assignment Pools)

```
Syntax  pool pool-name {
        family family {
            dhcp-attributes {
                [ protocol-specific attributes ]
            }
            host hostname {
                hardware-address mac-address;
                ip-address ip-address;
            }
            network ip-prefix / <prefix-length>;
            prefix ipv6-prefix;
            range range-name {
                high upper-limit;
                low lower-limit;
                prefix-length prefix-length;
            }
        }
        link pool-name;
    }
```

Hierarchy Level [edit access [address-assignment](#)]

Release Information Statement introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description Configure the name of an address-assignment pool.



NOTE: Subordinate statement support depends on the platform. See individual statement topics for more detailed support information.

Options *pool-name*—Name assigned to the address-assignment pool.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- [Address-Assignment Pools Overview on page 315](#)
- [Configuring Address-Assignment Pools on page 316](#)
- [Configuring a DHCP Server on Switches \(CLI Procedure\)](#)

pool (DHCP Local Server Overrides)

Syntax `pool pool-name;`

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server overrides [process-inform](#)],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 overrides [process-inform](#)],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* overrides [process-inform](#)],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* interface *interface-name* overrides [process-inform](#)],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* overrides [process-inform](#)],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* interface *interface-name* overrides [process-inform](#)],
 [edit logical-systems *logical-system-name* system services dhcp-local-server overrides [process-inform](#)],
 [edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 overrides [process-inform](#)],
 [edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name* overrides [process-inform](#)],
 [edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name* interface *interface-name* overrides [process-inform](#)],
 [edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* overrides [process-inform](#)],
 [edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* interface *interface-name* overrides [process-inform](#)],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server overrides [process-inform](#)],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 overrides [process-inform](#)],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* overrides [process-inform](#)],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* interface *interface-name* overrides [process-inform](#)],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* overrides [process-inform](#)],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* interface *interface-name* overrides [process-inform](#)],
 [edit system services dhcp-local-server overrides [process-inform](#)],
 [edit system services dhcp-local-server dhcpv6 overrides [process-inform](#)],
 [edit system services dhcp-local-server dhcpv6 group *group-name* overrides [process-inform](#)],
 [edit system services dhcp-local-server dhcpv6 group *group-name* interface *interface-name* overrides [process-inform](#)],
 [edit system services dhcp-local-server group *group-name* overrides [process-inform](#)],
 [edit system services dhcp-local-server group *group-name* interface *interface-name* overrides [process-inform](#)]

Release Information Statement introduced in Junos OS Release 11.4.
 Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description	Configure DHCP or DHCPv6 local server to reply to DHCP information request messages (DHCPINFORM for DHCPv4 and INFORMATION-REQUEST for DHCPv6) with information taken from the specified pool without interacting with AAA.
Options	pool-name —Name of the address pool, which must be configured within family inet for DHCP local server and within family inet6 for DHCPv6 local server.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Enabling Processing of Client Information Requests on page 214 • Overriding Default DHCP Local Server Configuration Settings on page 255

pool-match-order

Syntax	<pre>pool-match-order { external-authority; ip-address-first; option-82; }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server], [edit system services dhcp-local-server]
Release Information	Statement introduced in Junos OS Release 9.0. Statement introduced in Junos OS Release 12.1.
Description	Configure the order in which the DHCP local server uses information in the DHCP client PDU to determine how to obtain an address for the client. The remaining statements are explained separately.
Default	DHCP local server uses the ip-address-first method to determine which address pool to use.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 203 • Extended DHCP Local Server Overview on page 188 • Configuring a DHCP Server on Switches (CLI Procedure)

port

Syntax	<code>port port-number;</code>
Hierarchy Level	[edit access radius-server server-address], [edit access profile profile-name radius-server server-address]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the port number on which to contact the RADIUS server.
Options	port-number —Port number on which to contact the RADIUS server. Default: 1812 (as specified in RFC 2865)
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Router or Switch Interaction with RADIUS Servers on page 99• Configuring Authentication and Accounting Parameters for Subscriber Access on page 80


port (Diameter Peer)

Syntax	<code>port port-number;</code>
Hierarchy Level	[edit diameter peer peer-name connect-actively]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Specify the destination TCP port used by the active connection to peer.
Options	port-number —Number of the TCP port. Default: 3868
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Diameter on page 434• Configuring Diameter Peers on page 435

pre-ietf-mode

Syntax	<code>pre-ietf-mode</code>
Hierarchy Level	[edit protocols ancp], [edit protocols ancp neighbor <i>ip-address</i>]
Release Information	Statement introduced in Junos OS Release 9.4.
Description	Configure the ANCP agent to run in a mode that is backward compatible with Internet draft draft-wadhwa-gsmp-l2control-configuration-00.txt, <i>GSMP extensions for layer2 control (L2C)</i> for all neighbors or for a specific neighbor.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring the ANCP Agent on page 368 • Configuring the ANCP Agent for Backward Compatibility on page 372 • Configuring ANCP Neighbors on page 369

preauthentication-order (Access Profile)

Syntax	<code>preauthentication-order [<i>preauthentication-method</i>];</code>
Hierarchy Level	[edit access profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 13.3.
Description	Set the order in which the Junos OS uses preauthentication methods for the LLID service when multiple methods are configured. Junos OS supports only the radius method.
<div style="display: flex; align-items: center;">  <div> <p>NOTE: You cannot configure this statement if the Calling-Station-ID attribute is excluded from RADIUS Access-Request messages by the exclude statement.</p> </div> </div>	
Options	<p><i>preauthentication-method</i></p> <ul style="list-style-type: none"> • radius—Verify the client using RADIUS.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • RADIUS Logical Line Identifier (LLID) Overview on page 121 • Configuring Logical Line Identification (LLID) Preauthentication on page 124

preauthentication-server (Access Profile)

Syntax	<code>preauthentication-server <i>ip-address</i>;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> radius]
Release Information	Statement introduced in Junos OS Release 13.3.
Description	Specify the RADIUS preauthentication server, which is used for the LLID service.



NOTE: You cannot configure this statement if the Calling-Station-ID attribute is excluded from RADIUS Access-Request messages by the [exclude](#) statement.

Options	<i>ip-address</i> —IPv4 address.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• RADIUS Logical Line Identifier (LLID) Overview on page 121• Configuring Logical Line Identification (LLID) Preauthentication on page 124

preferred-lifetime (Address-Assignment Pools)

Syntax	<code>preferred-lifetime <i>seconds</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet6 dhcp-attributes]
Release Information	Statement introduced in Junos OS Release 13.3.
Description	<p>Specify the length of time, in seconds, that the DHCPv6 server keeps the IPv6 prefix active. When the lifetime expires, the address is deprecated.</p> <p>If the valid-lifetime is also configured, the preferred-lifetime must be less than the valid-lifetime. The preferred-lifetime and the maximum-lease-time are mutually exclusive and cannot both be configured.</p>
Options	<p>seconds—Number of seconds that the IPv6 prefix is active.</p> <p>Range: 30 through 4,294,967,295 seconds</p> <p>Default: 86,400 (24 hours)</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Address-Assignment Pools on page 316 • DHCP Attributes for Address-Assignment Pools on page 201 • maximum-lease-time on page 800 • valid-lifetime (Address-Assignment Pools) on page 991

preferred-lifetime (Dynamic Router Advertisement)

Syntax	<code>preferred-lifetime <i>seconds</i>;</code>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols router-advertisement interface <i>interface-name</i> <code>prefix <i>prefix</i></code>]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	Specify how long the prefix generated by stateless autoconfiguration remains preferred.
Options	<i>seconds</i> —Preferred lifetime, in seconds. If you set the preferred lifetime to 0xffffffff , the lifetime is infinite. The preferred lifetime is never greater than the valid lifetime. Default: 604,800 seconds
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>valid-lifetime</i>• <i>Example: Configuring IPv6 Interfaces and Enabling Neighbor Discovery</i>

prefix (DHCP Relay Agent)

Syntax	<code>prefix <i>prefix</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id relay-agent-remote-id)],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> (relay-agent-interface-id relay-agent-remote-id)],</p> <p>[edit forwarding-options dhcp-relay relay-option-82 (circuit-id remote-id)],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> relay-option-82 (circuit-id remote-id)],</p> <p>[edit logical-systems <i>logical-system-name</i> ... forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id relay-agent-remote-id)],</p> <p>[edit logical-systems <i>logical-system-name</i> ... forwarding-options dhcp-relay ... relay-option-82 (circuit-id remote-id)],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id relay-agent-remote-id)],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ... relay-option-82 (circuit-id remote-id)]</p>
Release Information	<p>Statement introduced in Junos OS Release 8.3.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.3 for EX Series switches.</p> <p>Support at the [edit ... relay-agent-remote-id] and [edit ... remote-id] hierarchy levels introduced in Junos OS Release 14.1.</p>
Description	<p>Add a prefix to the DHCP base option 82 Agent Circuit ID (suboption 1) or Agent Remote ID (suboption 2) information, or to the DHCPv6 option 18 (Relay Agent Interface-ID) or option 37 (Relay Agent Remote-ID) information in DHCP packets that DHCP relay agent sends to a DHCP server. The prefix can consist of any combination of the hostname, logical system name, and routing instance name.</p>
Options	<p><i>prefix</i>—Any of the following:</p> <ul style="list-style-type: none"> • host-name—Prepend the hostname of the router configured with the host-name statement at the [edit system] hierarchy level to the DHCP option information. • logical-system-name—Prepend the name of the logical system to the option information. • routing-instance-name—Prepend the name of the routing instance to the option information.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Including a Prefix in DHCP Options on page 269 • Using DHCP Relay Agent Option 82 Information on page 266 • Configuring DHCPv6 Relay Agent Options on page 296

prefix (Address-Assignment Pools)

Syntax	<code>prefix <i>ipv6-prefix</i>;</code>
Hierarchy Level	[edit access address-assignment <code>pool <i>pool-name</i> family inet6</code>]
Release Information	Statement introduced in Junos OS Release 10.0. Statement introduced in Junos OS Release 12.3 for EX Series switches.
Description	Specify the IPv6 prefix for the IPv6 address-assignment pool. This statement is mandatory for IPv6 address-assignment pools.
Options	<i>ipv6-prefix</i> —The IPv6 prefix.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Address-Assignment Pools Overview on page 315• Configuring Address-Assignment Pools on page 316• <i>Configuring a DHCP Server on Switches (CLI Procedure)</i>• <i>Configuring an Extended DHCP Relay Server on EX Series Switches (CLI Procedure)</i>

prefix (Dynamic Router Advertisement)

Syntax	<pre>prefix <i>prefix</i> { (<code>autonomous</code> <code>no-autonomous</code>); (<code>on-link</code> <code>no-on-link</code>); <code>preferred-lifetime</code> <i>seconds</i>; <code>valid-lifetime</code> <i>seconds</i>; }</pre>
Hierarchy Level	[edit dynamic-profiles protocols router-advertisement <code>interface <i>interface-name</i></code>]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	Configure the prefix name in router advertisement messages.
Options	<i>prefix</i> —Prefix name. For dynamic configuration, specify the <code>\$junos-ipv6-ndra-prefix</code> dynamic variable. The remaining statements are explained separately.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Example: Configuring IPv6 Interfaces and Enabling Neighbor Discovery</i>

priority (Diameter Peer)

Syntax	<code>priority <i>priority-value</i>;</code>
Hierarchy Level	[edit diameter network-element <i>element-name</i> peer <i>peer-name</i>]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Set the priority for a peer within a Diameter network element. A peer with a lower number has a higher priority.
Options	<i>priority-value</i> —Priority for the peer within the network element. Range: 1 through 65535
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Diameter on page 434• Configuring Diameter Network Elements on page 437

profile (Access)

```
Syntax  profile profile-name {
        accounting {
            address-change-immediate-update
            accounting-stop-on-access-deny;
            accounting-stop-on-failure;
            ancp-speed-change-immediate-update;
            coa-immediate-update;
            coa-no-override service-class-attribute;
            duplication;
            duplication-vrf {
                access-profile-name profile-name;
                vrf-name vrf-name;
            }
            immediate-update;
            order [ accounting-method ];
            send-acct-status-on-config-change;
            statistics (time | volume-time);
            update-interval minutes;
            wait-for-acct-on-ack;
        }
        authentication-order [ authentication-methods ];
        client client-name {
            chap-secret chap-secret;
            group-profile profile-name;
            ike {
                allowed-proxy-pair {
                    remote remote-proxy-address local local-proxy-address;
                }
                pre-shared-key (ascii-text character-string | hexadecimal hexadecimal-digits);
                ike-policy policy-name;
                interface-id string-value;
            }
            l2tp {
                aaa-access-profile profile-name;
                interface-id interface-id;
                lcp-renegotiation;
                local-chap;
                maximum-sessions-per-tunnel number;
                multilink {
                    drop-timeout milliseconds;
                    fragment-threshold bytes;
                }
                ppp-authentication (chap | pap);
                ppp-profile profile-name;
                shared-secret shared-secret;
            }
            pap-password pap-password;
            ppp {
                cell-overhead;
                encapsulation-overhead bytes;
                framed-ip-address ip-address;
                framed-pool framed-pool;
            }
        }
    }
```

```

    idle-timeout seconds;
    interface-id interface-id;
    keepalive seconds;
    primary-dns primary-dns;
    primary-wins primary-wins;
    secondary-dns secondary-dns;
    secondary-wins secondary-wins;
  }
  user-group-profile profile-name;
}
domain-name-server;
domain-name-server-inet;
domain-name-server-inet6;
preauthentication-order preauthentication-method;
provisioning-order (gx-plus | jsrc);
radius {
  accounting-server [ ip-address ];
  attributes {
    exclude {
      ...
    }
    ignore {
      framed-ip-netmask;
      input-filter;
      logical-system::routing-instance;
      output-filter;
    }
  }
}
authentication-server [ ip-address ];
options {
  accounting-session-id-format (decimal | description);
  calling-station-id-delimiter delimiter-character;
  calling-station-id-format {
    agent-circuit-id;
    agent-remote-id;
    interface-description;
    nas-identifier;
  }
  client-accounting-algorithm (direct | round-robin);
  client-authentication-algorithm (direct | round-robin);
  coa-dynamic-variable-validation;
  ethernet-port-type-virtual;
  interface-description-format {
    exclude-adapter;
    exclude-sub-interface;
  }
  juniper-dsl-attributes;
  nas-identifier identifier-value;
  nas-port-extended-format {
    adapter-width width;
    ae-width width;
    port-width width;
    slot-width width;
    stacked-vlan-width width;
    vlan-width width;
    atm {

```

```
        adapter-width width;  
        port-width width;  
        slot-width width;  
        vci-width width;  
        vpi-width width;  
    }  
}  
nas-port-id-delimiter delimiter-character;  
nas-port-id-format {  
    agent-circuit-id;  
    agent-remote-id;  
    interface-description;  
    nas-identifier;  
}  
nas-port-type {  
    ethernet {  
        port-type;  
    }  
}  
revert-interval interval;  
vlan-nas-port-stacked-format;  
}  
preauthentication-server ip-address;  
}  
radius-server server-address {  
    accounting-port port-number;  
    accounting-retry number;  
    accounting-timeout seconds;  
    port port-number;  
    retry attempts;  
    routing-instance routing-instance-name;  
    secret password;  
    max-outstanding-requests value;  
    source-address source-address;  
    timeout seconds;  
}  
service {  
    accounting-order (activation-protocol | radius);  
}  
session-options {  
    client-idle-timeout minutes;  
    client-session-timeout minutes;  
}  
}
```

Hierarchy Level [edit access]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure PPP CHAP, or a profile and its subscriber access, L2TP, or PPP properties.

Options *profile-name*—Name of the profile.

For CHAP, the name serves as the mapping between peer identifiers and CHAP secret keys. This entity is queried for the secret key whenever a CHAP challenge or response is received.

The remaining statements are explained separately.

Required Privilege admin—To view this statement in the configuration.
Level admin-control—To add this statement to the configuration.

Related Documentation

- *Configuring the PPP Authentication Protocol*
- *Configuring Access Profiles for L2TP or PPP Parameters*
- *Configuring L2TP Properties for a Client-Specific Profile*
- *Configuring an L2TP LNS with Inline Service Interfaces*
- *Configuring PPP Properties for a Client-Specific Profile*
- [Configuring Service Accounting with JSRC on page 460](#)
- [AAA Service Framework Overview on page 3](#)
- [show network-access aaa statistics on page 1164](#)
- [clear network-access aaa statistics on page 1027](#)

process-inform

Syntax	<pre>process-inform { pool pool-name; }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i> overrides],</p> <p>[edit system services dhcp-local-server overrides],</p> <p>[edit system services dhcp-local-server dhcpv6 overrides],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> overrides],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i> overrides],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i> overrides]</p>
Release Information	<p>Statement introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	<p>Enable the processing of DHCP information request messages (DHCPINFORM for DHCPv4 and INFORMATION-REQUEST for DHCPv6) sent from the client to request DHCP options. For DHCP local servers, the messages are also passed to the configured server list.</p>

The remaining statement is explained separately.

Default	Information request messages are not processed.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Enabling Processing of Client Information Requests on page 214• Overriding Default DHCP Local Server Configuration Settings on page 255• Configuring a DHCP Server on Switches (CLI Procedure)

protocol

Syntax	<code>protocol protocol-number;</code>
Hierarchy Level	[edit services ptsp rule <i>rule-name</i> term <i>precedence</i> from]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Identify the protocol for inclusion as a match condition.
Options	<i>protocol-number</i> —Protocol number.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>

protocols (Dynamic Profiles)

```

Syntax protocols {
    igmp {
        interface interface-name {
            accounting;
            disable;
            group-policy;
            immediate-leave;
            no-accounting;
            promiscuous-mode;
            ssm-map ssm-map-name;
            static {
                group group {
                    source source;
                }
            }
            version version;
        }
    }
    mld {
        interface interface-name {
            disable;
            (accounting | no-accounting);
            group-policy;
            immediate-leave;
            oif-map;
            passive;
            ssm-map ssm-map-name;
            static {
                group multicast-group-address {
                    exclude;
                    group-count number;
                    group-increment increment;
                    source ip-address {
                        source-count number;
                        source-increment increment;
                    }
                }
            }
            version version;
        }
    }
    router-advertisement {
        interface interface-name {
            current-hop-limit number;
            default-lifetime seconds;
            (managed-configuration | no-managed-configuration);
            max-advertisement-interval seconds;
            min-advertisement-interval seconds;
            (other-stateful-configuration | no-other-stateful-configuration);
            prefix prefix;
            reachable-time milliseconds;
            retransmit-timer milliseconds;
        }
    }
}

```

```
    }  
  }  
}
```

Hierarchy Level [edit dynamic-profiles *profile-name*]

Release Information Statement introduced in Junos OS Release 9.2.
Support at the [edit dynamic-profiles *profile-name* protocols mld] and [edit dynamic-profiles *profile-name* protocols router-advertisement] hierarchy levels introduced in Junos OS Release 10.1.

Description Enable IGMP on the router. IGMP must be enabled for the router to receive multicast packets.

Default IGMP is disabled on the router. IGMP is automatically enabled on all broadcast interfaces when you configure Protocol Independent Multicast (PIM) or Distance Vector Multicast Routing Protocol (DVMRP).

The statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Configuring IGMP*
- *Examples: Configuring MLD*

provisioning-order

Syntax	provisioning-order (gx-plus jsrc);
Hierarchy Level	[edit access profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 9.6. Support for Gx-Plus introduced in Junos OS Release 11.2. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Description	Configure AAA to use the specified application for subscriber service provisioning.
Options	<p>gx-plus—Specify Gx-Plus as the application used to communicate with a PCRF for subscriber service provisioning.</p> <p>jsrc—Specify JSRC as the application used to communicate with the SAE for subscriber service provisioning. JSRC is used in an SRC environment to request services from the SAE for an authenticated subscriber. JSRC attempts to activate these services. If successful, JSRC returns an ACK message. If unsuccessful, the subscriber is denied access.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring JSRC on page 455• Provisioning Subscribers with JSRC on page 458• Configuring Gx-Plus on page 446• Provisioning Subscribers with Gx-Plus on page 449

proxy-mode

Syntax	proxy-mode;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay overrides],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.5.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	<p>Enable DHCP relay proxy mode on the extended DHCP relay. Proxy mode supports all extended DHCP relay functionality.</p> <p>You cannot configure both the DHCP relay proxy and the extended DHCP local server on the same interface.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • DHCP Relay Proxy Overview on page 197 • Extended DHCP Relay Agent Overview on page 194 • Enabling DHCP Relay Proxy Mode on page 281

qos-adjust

Syntax	qos-adjust;
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 9.4.
Description	Specify that the ANCP agent reports net data rates for downstream traffic to CoS. When this statement is not configured, ANCP does not report traffic rates to CoS.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the ANCP Agent to Report Traffic Rates to CoS on page 399• Traffic Rate Reporting and Adjustment by the ANCP Agent on page 395• Configuring the ANCP Agent on page 368

qos-adjust-adsl

Syntax	qos-adjust-adsl <i>adjustment-factor</i> ;
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Configure an adjustment factor that is applied globally to the downstream and upstream data rates reported by the ANCP agent for all subscribers on an ADSL line. The ANCP agent reports the adjusted rate only to AAA.
Options	<p><i>adjustment-factor</i>—Adjustment factor applied to upstream and downstream data rates for the DSL type.</p> <p>Range: 0 through 100 percent</p> <p>Default: 100 percent</p>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Setting a Global Adjustment Factor per DSL Subscriber Line for ANCP Agent-Reported Traffic Rates on page 402• Configuring the ANCP Agent on page 368

qos-adjust-adsl2

Syntax	<code>qos-adjust-adsl2 <i>adjustment-factor</i>;</code>
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Configure an adjustment factor that is applied globally to the downstream and upstream data rates reported by the ANCP agent for all subscribers on an ADSL2 line. The ANCP agent reports the adjusted rate only to AAA.
Options	<p><i>adjustment-factor</i>—Adjustment factor applied to upstream and downstream data rates for the DSL type.</p> <p>Range: 0 through 100 percent</p> <p>Default: 100 percent</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Setting a Global Adjustment Factor per DSL Subscriber Line for ANCP Agent-Reported Traffic Rates on page 402 • Configuring the ANCP Agent on page 368

qos-adjust-adsl2-plus

Syntax	<code>qos-adjust-adsl2-plus <i>adjustment-factor</i>;</code>
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Configure an adjustment factor that is applied globally to the downstream and upstream data rates reported by the ANCP agent for all subscribers on an ADSL2+ line. The ANCP agent reports the adjusted rate only to AAA.
Options	<p><i>adjustment-factor</i>—Adjustment factor applied to upstream and downstream data rates for the DSL type.</p> <p>Range: 0 through 100 percent</p> <p>Default: 100 percent</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Setting a Global Adjustment Factor per DSL Subscriber Line for ANCP Agent-Reported Traffic Rates on page 402 • Configuring the ANCP Agent on page 368

qos-adjust-sds1

Syntax	<code>qos-adjust-sds1 <i>adjustment-factor</i>;</code>
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Configure an adjustment factor that is applied globally to the downstream and upstream data rates reported by the ANCP agent for all subscribers on an SDS1 line. The ANCP agent reports the adjusted rate only to AAA.
Options	<i>adjustment-factor</i> —Adjustment factor applied to upstream and downstream data rates for the DSL type. Range: 0 through 100 percent Default: 100 percent
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Setting a Global Adjustment Factor per DSL Subscriber Line for ANCP Agent-Reported Traffic Rates on page 402• Configuring the ANCP Agent on page 368

qos-adjust-vds1

Syntax	<code>qos-adjust-vds1 <i>adjustment-factor</i>;</code>
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Configure an adjustment factor that is applied globally to the downstream and upstream data rates reported by the ANCP agent for all subscribers on an VDS1 line. The ANCP agent reports the adjusted rate only to AAA.
Options	<i>adjustment-factor</i> —Adjustment factor applied to upstream and downstream data rates for the DSL type. Range: 0 through 100 percent Default: 100 percent
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Setting a Global Adjustment Factor per DSL Subscriber Line for ANCP Agent-Reported Traffic Rates on page 402• Configuring the ANCP Agent on page 368

qos-adjust-vds2

Syntax	<code>qos-adjust-vds2 <i>adjustment-factor</i>;</code>
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Configure an adjustment factor that is applied globally to the downstream and upstream data rates reported by the ANCP agent for all subscribers on an VDS2 line. The ANCP agent reports the adjusted rate only to AAA.
Options	<p><i>adjustment-factor</i>—Adjustment factor applied to upstream and downstream data rates for the DSL type.</p> <p>Range: 0 through 100 percent</p> <p>Default: 100 percent</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Setting a Global Adjustment Factor per DSL Subscriber Line for ANCP Agent-Reported Traffic Rates on page 402• Configuring the ANCP Agent on page 368

radius (Access Profile)

```
Syntax  radius {
        accounting-server [ ip-address ];
        attributes {
            exclude
            ...
        }
        ignore {
            framed-ip-netmask;
            input-filter;
            logical-system-routing-instance;
            output-filter;
        }
    }
    authentication-server [ ip-address ];
    options {
        accounting-session-id-format (decimal | description);
        calling-station-id-delimiter delimiter-character;
        calling-station-id-format {
            agent-circuit-id;
            agent-remote-id;
            interface-description;
            nas-identifier;
        }
        client-accounting-algorithm (direct | round-robin);
        client-authentication-algorithm (direct | round-robin);
        coa-dynamic-variable-validation;
        ethernet-port-type-virtual;
        interface-description-format {
            exclude-adapter;
            exclude-sub-interface;
        }
        ip-address-change-notify message;
        juniper-dsl-attributes;
        nas-identifier identifier-value;
        nas-port-extended-format {
            adapter-width width;
            ae-width width;
            port-width width;
            slot-width width;
            stacked-vlan-width width;
            vlan-width width;
            atm {
                adapter-width width;
                port-width width;
                slot-width width;
                vci-width width;
                vpi-width width;
            }
        }
        nas-port-id-delimiter delimiter-character;
        nas-port-id-format {
            agent-circuit-id;
```

```

    agent-remote-id;
    interface-description;
    nas-identifier;
  }
  nas-port-type {
    ethernet {
      port-type;
    }
  }
  revert-interval interval;
  vlan-nas-port-stacked-format;
}
preauthentication-server ip-address;
}

```

Hierarchy Level [edit access [profile](#) *profile-name*]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the RADIUS parameters that the router uses for AAA authentication and accounting for subscribers.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- [Configuring RADIUS Server Parameters for Subscriber Access on page 102](#)
- [RADIUS Server Options for Subscriber Access on page 4](#)

radius-disconnect (DHCP Local Server)

Syntax	radius-disconnect;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure trigger],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure trigger],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure trigger],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure trigger],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server reconfigure trigger],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 reconfigure trigger],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure trigger],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure trigger],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure trigger],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure trigger],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure trigger],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure trigger],</p> <p>[edit system services dhcp-local-server reconfigure trigger],</p> <p>[edit system services dhcp-local-server dhcpv6 reconfigure trigger],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> reconfigure trigger],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure trigger]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.0.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.</p>
Description	Configure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces to be reconfigured when a RADIUS-initiated disconnect is received by the DHCP client or group of clients. A group configuration takes precedence over a DHCP local server configuration.
Default	The client is deleted when a RADIUS-initiated disconnect is received.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Dynamic Client Reconfiguration of Extended Local Server Clients on page 244 • Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect on page 247

radius-options (Edit Access)

Syntax	<pre>radius-options { revert-interval <i>seconds</i>; request-rate <i>rate</i>; }</pre>
Hierarchy Level	[edit access]
Release Information	Statement introduced in Junos OS Release 8.3.
Description	<p>Configure RADIUS options.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>access—To view this statement in the configuration.</p> <p>access-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Server Options for Subscriber Access on page 102• Configuring Authentication and Accounting Parameters for Subscriber Access on page 80

radius-options (Interfaces)

Syntax radius-options {
 [nas-port-options](#) *nas-port-options-name* {
 [nas-port-extended-format](#) {
 adapter-width *width*;
 ae-width *width*;
 port-width *width*;
 slot-width *width*;
 stacked;
 stacked-vlan-width *width*;
 vci-width *width*;
 vlan-width *width*;
 vpi-width *width*;
 }
 [nas-port-type](#) *port-type*;
 [stacked-vlan-ranges](#) (*any* | *low-outer-tag-high-outer-tag*),*any*;
 [vlan-ranges](#) (*any* | *low-tag-high-tag*);
 }
 }

Hierarchy Level [edit interfaces *interface-name*]

Release Information Statement introduced in Junos OS Release 12.3.

Description Configure RADIUS options to set the NAS-Port-Type (61) RADIUS IETF attribute, and an extended format for the NAS-Port (5) RADIUS IETF attribute, on a per-physical interface, per-VLAN, or per-stacked VLAN (S-VLAN) basis.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 63](#)
- [Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 62](#)

radius-server

Syntax	<pre>radius-server server-address { accounting-port port-number; accounting-retry number; accounting-timeout seconds; port port-number; retry attempts; routing-instance routing-instance-name; secret password; max-outstanding-requests value; source-address source-address; timeout seconds; }</pre>
Hierarchy Level	<p>[edit access],</p> <p>[edit access profile profile-name]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	<p>Configure RADIUS for subscriber access management, L2TP, or PPP.</p> <p>To configure multiple RADIUS servers, include multiple radius-server statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.</p>
Options	<p>server-address—Address of the RADIUS authentication server.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring RADIUS Authentication for L2TP</i> • <i>Configuring the PPP Authentication Protocol</i> • <i>Configuring RADIUS Authentication</i> • Configuring Authentication and Accounting Parameters for Subscriber Access on page 80 • show network-access aaa statistics on page 1164 • clear network-access aaa statistics on page 1027

range (Address-Assignment Pools)

Syntax	<pre>range <i>range-name</i> { high <i>upper-limit</i>; low <i>lower-limit</i>; prefix-length <i>prefix-length</i>; }</pre>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family (inet inet6)]
Release Information	Statement introduced in Junos OS Release 9.0. IPv6 support introduced in Junos OS Release 10.0. Statement introduced in Junos OS Release 12.3 for EX Series switches.
Description	Configure a named range of IPv4 addresses or IPv6 prefixes, used within an address-assignment pool.
Options	<p>high <i>upper-limit</i>—Upper limit of an address range or IPv6 prefix range.</p> <p>low <i>lower-limit</i>—Lower limit of an address range or IPv6 prefix range.</p> <p>prefix-length <i>prefix-length</i>—Assigned length of the IPv6 prefix.</p> <p><i>range-name</i>—Name assigned to the range of IPv4 addresses or IPv6 prefixes.</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Address-Assignment Pools Overview on page 315• Configuring Address-Assignment Pools on page 316• Configuring a DHCP Server on Switches (CLI Procedure)

rapid-commit (DHCPv6 Local Server)

Syntax	rapid-commit;
Hierarchy Level	<p>[edit system services dhcp-local-server dhcpv6 overrides],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name overrides],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name interface interface-name overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 ...],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 ...],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 ...]</p>
Release Information	<p>Statement introduced in Junos OS Release 12.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	<p>Configure DHCPv6 local server to recognize the Rapid Commit option (DHCPv6 option 14) in DHCPv6 solicit messages sent from the DHCPv6 client. When rapid commit is enabled for both DHCPv6 local server and the DHCPv6 client, a two-message handshake is used instead of the standard four-message handshake. You can enable rapid commit support on DHCPv6 local server globally, for a named group, or for a specific interface.</p>
Default	Rapid commit support is not enabled.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Enabling DHCPv6 Rapid Commit Support on page 291 • Overriding Default DHCP Local Server Configuration Settings on page 255

reachable-time (Dynamic Router Advertisement)

Syntax	<code>reachable-time <i>milliseconds</i>;</code>
Hierarchy Level	[edit protocols router-advertisement interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	Set the length of time that a node considers a neighbor reachable until another reachability confirmation is received from that neighbor.
Options	<i>milliseconds</i> —Reachability time limit. Range: 0 through 3,600,000 milliseconds Default: 0 milliseconds
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Example: Configuring IPv6 Interfaces and Enabling Neighbor Discovery</i>

realm (Diameter Origin)

Syntax	<code>realm <i>realm-name</i>;</code>
Hierarchy Level	[edit diameter <i>origin</i>]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Specify the realm of the host that originates the Diameter message.
Options	<i>realm-name</i> —Name of the message origin realm. Supplied as the value of Origin-Realm AVP for all messages sent by the Diameter master instance.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Diameter on page 434• Configuring the Origin Attributes of the Diameter Instance on page 435

realm-delimiter (Domain Map)

Syntax	<code>realm-delimiter [<i>delimiter-character</i>];</code>
Hierarchy Level	[edit access domain]
Release Information	Statement introduced in Junos OS Release 14.1.
Description	Specify the characters that the router uses to separate usernames from realm names.
Default	none
Options	<i>delimiter-character</i> —One or more characters used as delimiters. You can specify a maximum of eight delimiters. You cannot use the semicolon (;) as a delimiter. Do not include spaces between characters.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Specifying Domain and Realm Name Delimiters on page 136 • Configuring Domain and Realm Name Usage for Domain Maps on page 136

realm-parse-direction (Domain Map)

Syntax	<code>realm-parse-direction (left-to-right right-to-left);</code>
Hierarchy Level	[edit access domain]
Release Information	Statement introduced in Junos OS Release 14.1.
Description	Specify the direction in which the router searches for the realm name in a username.
Default	left-to-right
Options	<p>left-to-right—The router searches starting at the left-most character. When the router reaches a realm delimiter, it uses anything to the left of the delimiter as the realm name.</p> <p>right-to-left—The router searches starting at the right-most character. When the router reaches a realm delimiter, it uses anything to the left of the realm as the domain name.</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Specifying the Parsing Direction for Domain and Realm Names on page 138 • Configuring Domain and Realm Name Usage for Domain Maps on page 136

reconfigure (DHCP Local Server)

Syntax

```
reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    timeout timeout-value;
    token token-value;
    trigger {
        radius-disconnect;
    }
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services **dhcp-local-server**],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server **dhcpv6**],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server **group** *group-name*],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name*],
 [edit logical-systems *logical-system-name* system services **dhcp-local-server**],
 [edit logical-systems *logical-system-name* system services dhcp-local-server **dhcpv6**],
 [edit logical-systems *logical-system-name* system services dhcp-local-server **group** *group-name*],
 [edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 **group** *group-name*],
 [edit routing-instances *routing-instance-name* system services **dhcp-local-server**],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server **dhcpv6**],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server **group** *group-name*],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name*],
 [edit system services **dhcp-local-server**],
 [edit system services dhcp-local-server **dhcpv6**],
 [edit system services dhcp-local-server **group** *group-name*],
 [edit system services dhcp-local-server dhcpv6 **group** *group-name*]

Release Information

Statement introduced in Junos OS Release 10.0.
 Support at the [edit ... **dhcpv6** ...] hierarchy levels introduced in Junos OS Release 10.4.
 Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Enable dynamic reconfiguration triggered by the DHCP local server of all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. A group configuration takes precedence over a DHCP local server configuration. The **strict** statement is available only for DHCPv6.

The remaining statements are explained separately.

Required Privilege Level

system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

- Related Documentation**
- [Configuring Dynamic Client Reconfiguration of Extended Local Server Clients on page 244](#)
 - [Configuring a DHCP Server on Switches \(CLI Procedure\)](#)

relay-agent-interface-id (DHCP Local Server)

Syntax	<code>relay-agent-interface-id;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify that the DHCPv6 Relay Agent Interface-ID option (option 18) in the client PDU name is concatenated with the username during the subscriber authentication or DHCP client authentication process.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Creating Unique Usernames for DHCP Clients on page 218

relay-agent-interface-id (DHCPv6 Relay Agent)

Syntax	<pre>relay-agent-interface-id { <i>prefix prefix</i>; use-interface-description (logical device); use-option-82; }</pre>
Hierarchy Level	<pre>[edit forwarding-options dhcp-relay dhcpv6], [edit forwarding-options dhcp-relay dhcpv6 group group-name], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 ...], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 ...]</pre>
Release Information	<p>Statement introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.3 for EX Series switches.</p>
Description	<p>Insert the DHCPv6 Relay Agent Interface-ID option (option 18) in DHCPv6 packets destined for the DHCPv6 server.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• dhcp-relay on page 689• Extended DHCP Relay Agent Overview on page 194• DHCPv6 Relay Agent Overview• Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets on page 297

relay-agent-interface-id (DHCPv6 Relay Agent Username)

Syntax	relay-agent-interface-id;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include]</p>
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Specify that the DHCPv6 Relay Agent Interface-ID option (option 18) in the client PDU name is concatenated with the username during the subscriber authentication process.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • DHCPv6 Relay Agent Overview • Creating Unique Usernames for DHCP Clients on page 218

relay-agent-remote-id (DHCP Local Server)

Syntax	relay-agent-remote-id;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>For MX Series routers only, enterprise-id and remote-id options introduced in Junos OS Release 12.3R3.</p> <p>For MX Series routers only, the enterprise-id and remote-id options are obsoleted starting in Junos OS Releases 12.3R7, 13.2R4, 13.3R2, and 14.1R1.</p>
Description	Specify that the DHCPv6 Relay Agent Remote-ID option (option 37) in the client PDU name is concatenated with the username during the subscriber authentication or DHCP client authentication process. In order to generate an ASCII version of the username, the router concatenates only the remote-id portion of option 37 to the username, and ignores the enterprise number.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Creating Unique Usernames for DHCP Clients on page 218

relay-agent-remote-id (DHCPv6 Relay Agent Username)

Syntax	<code>relay-agent-remote-id;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>For MX Series routers only, enterprise-id and remote-id options introduced in Junos OS Release 12.3R3.</p> <p>For MX Series routers only, the enterprise-id and remote-id options are obsoleted starting in Junos OS Releases 12.3R7, 13.2R4, 13.3R2, and 14.1R1.</p>
Description	Specify that the DHCPv6 Relay Agent Remote-ID option (option 37) in the client PDU name is concatenated with the username during the subscriber authentication or client authentication process. In order to generate an ASCII version of the username, the router concatenates only the remote-id portion of option 37 to the username, and ignores the enterprise number.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> DHCPv6 Relay Agent Overview Creating Unique Usernames for DHCP Clients on page 218

relay-agent-remote-id (DHCPv6 Relay Agent)

Syntax	<pre>relay-agent-remote-id { <i>prefix</i> <i>prefix</i>; <i>use-interface-description</i> (logical device); }</pre>
Hierarchy Level	[edit forwarding-options dhcp-relay <i>dhcpv6</i>], [edit forwarding-options dhcp-relay <i>dhcpv6</i> <i>group</i> <i>group-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay <i>dhcpv6</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay <i>dhcpv6</i> ...], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay <i>dhcpv6</i> ...]
Release Information	Statement introduced in Junos OS Release 14.1.
Description	<p>Specify that the DHCPv6 relay agent include the Relay Agent Remote-ID (option 37) in DHCPv6 packets destined for a DHCPv6 server. Optionally specify that the option includes a prefix or interface textual description, or both.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Extended DHCP Relay Agent Overview on page 194• DHCPv6 Relay Agent Overview• DHCPv6 Relay Agent Options on page 295• Configuring DHCPv6 Relay Agent Options on page 296

relay-agent-subscriber-id (DHCP Local Server)

Syntax	relay-agent-subscriber-id;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include]</p>
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Specify that the DHCPv6 Relay Agent Subscriber-ID option (option 38) in the client PDU name is concatenated with the username during the subscriber authentication process.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Creating Unique Usernames for DHCP Clients on page 218

relay-agent-subscriber-id (DHCPv6 Relay Agent)

Syntax	relay-agent-subscriber-id;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include]</p>
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Specify that the DHCPv6 Relay Agent Subscriber-ID option (option 38) in the client PDU name is concatenated with the username during the subscriber authentication process.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• DHCPv6 Relay Agent Overview• Creating Unique Usernames for DHCP Clients on page 218

relay-option (DHCP Relay Agent)

Syntax	<pre> relay-option { option-number option-number; default-action { drop; forward-only; local-server-group local-server-group; relay-server-group relay-server-group; } equals (ascii ascii-string hexadecimal hexadecimal-string) { drop; forward-only; local-server-group local-server-group; relay-server-group relay-server-group; } starts-with (ascii ascii-string hexadecimal hexadecimal-string) { drop; forward-only; local-server-group local-server-group; relay-server-group relay-server-group; } } </pre>
Hierarchy Level	<pre> [edit forwarding-options dhcp-relay], [edit forwarding-options dhcp-relay dhcpv6], [edit forwarding-options dhcp-relay group group-name], [edit forwarding-options dhcp-relay dhcpv6 group group-name], [edit logical-systems logical-system-name forwarding-options dhcp-relay ...], [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...], [edit routing-instances routing-instance-name forwarding-options dhcp-relay ...] </pre>
Release Information	<p>Statement introduced in Junos OS Release 12.3.</p> <p>Statement introduced in Junos OS Release 12.3 for EX Series switches.</p>
Description	<p>Configure the extended DHCP relay agent selective processing that is based on DHCP options in DHCP client packets and specify the action to perform on client traffic. You can configure support globally or for a named group of interfaces, and for either DHCP or DHCPv6 relay agent.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using DHCP Option Information to Selectively Process DHCP Client Traffic on page 273

relay-option-82

```
Syntax  relay-option-82 {
        circuit-id {
            include-irb-and-l2;
            no-vlan-interface-name;
            prefix prefix;
            use-interface-description (logical | device);
            use-vlan-id;
        }
        remote-id {
            include-irb-and-l2;
            no-vlan-interface-name;
            prefix prefix;
            use-interface-description (logical | device);
            use-vlan-id;
        }
    }
```

Hierarchy Level [edit forwarding-options dhcp-relay],
 [edit forwarding-options dhcp-relay **group** *group-name*],
 [edit logical-systems *logical-system-name* forwarding-options **dhcp-relay**],
 [edit logical-systems *logical-system-name* forwarding-options dhcp-relay **group** *group-name*],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*
 forwarding-options dhcp-relay],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*
 forwarding-options dhcp-relay **group** *group-name*],
 [edit routing-instances *routing-instance-name* forwarding-options **dhcp-relay**],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay **group**
group-name]

Release Information Statement introduced in Junos OS Release 8.3.
 Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description Enable or disable the insertion of the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server.

When you configure **relay-option-82** without configuring the **circuit-id** or **remote-id** option, the Agent Circuit ID is added by default.

You can use the **relay-option-82** statement and its subordinate statements at the [edit forwarding-options dhcp-relay] hierarchy level to control insertion of option 82 information globally, or at the [edit forwarding-options dhcp-relay **group** *group-name*] hierarchy level to control insertion of option 82 information for a named group of interfaces.

To restore the default behavior (option 82 information is not inserted into DHCP packets), use the **delete relay-option-82** statement.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

- Related Documentation**
- [Using DHCP Relay Agent Option 82 Information on page 266](#)
 - [dhcp-relay on page 689](#)

relay-server-group (DHCP Relay Agent Option)

Syntax	<code>relay-server-group <i>relay-server-group</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay relay-option (default-action equals starts-with), [edit forwarding-options dhcp-relay dhcpv6 relay-option (default-action equals starts-with), [edit forwarding-options dhcp-relay group <i>group-name</i> relay-option (default-action equals starts-with), [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> relay-option (default-action equals starts-with), [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...]</p>
Release Information	<p>Statement introduced in Junos OS Release 12.3.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Relay DHCP client packets to the specified group of DHCP servers when you use the DHCP relay selective processing feature. You can configure the relay operation globally or for a group of interfaces, and for either DHCP or DHCPv6 relay agent.
Options	<i>relay-server-group</i> —Name of DHCP server group.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using DHCP Option Information to Selectively Process DHCP Client Traffic on page 273

remote-address

Syntax	<code>remote-address (<i>address</i> any-unicast) <except>;</code>
Hierarchy Level	[edit services ptsp rule <i>rule-name</i> term <i>precedence</i> from]
Release Information	Statement introduced in Junos OS Release 10.2. IPv6 support introduced in Junos OS Release 12.2
Description	Specify the address for rule matching. Remote address values are matched against a destination or source IP address for the flow depending on the configured value for the demux statement. If you do not specify an address, then any remote address matches this term. If you do not specify a prefix value, then a host mask is the default.
Options	address —IPv4 or IPv6 address or prefix value. any-unicast —Match all unicast addresses. except —(Optional) Exclude the specified address, prefix, or unicast packets from rule matching.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>• demux on page 679

remote-address-range

Syntax	<code>remote-address-range low <i>low-value</i> high <i>high-value</i> <except>;</code>
Hierarchy Level	[edit services ptsp rule <i>rule-name</i> term <i>precedence</i> from]
Release Information	Statement introduced in Junos OS Release 10.2. IPv6 support introduced in Junos OS Release 12.2
Description	Specify the address range for rule matching. Remote address values are matched against a destination or source IP address for the flow depending on the configured value for the demux statement. If you do not specify an address, then any remote address matches this term.
Options	<p>low-value—Lower boundary for the IPv4 or IPv6 address range.</p> <p>high-value—Upper boundary for the IPv4 or IPv6 address range.</p> <p>except—(Optional) Exclude the specified address range from rule matching.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i> • demux on page 679

remote-id

Syntax	<code>remote-id value range <i>named-range</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes option-match option-82]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	Specify the address-assignment pool named range to use based on the particular option 82 Agent Remote ID value.
Options	<p>range <i>named-range</i>—Name of the address-assignment pool range to use.</p> <p>value—String for Agent Remote ID suboption (suboption 2) of the DHCP relay agent information option (option 82) in DHCP packets.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Address-Assignment Pools on page 316

remote-id (DHCP Relay Agent)

Syntax	<pre>remote-id { include-irb-and-l2; no-vlan-interface-name; prefix <i>prefix</i>; use-interface-description (logical device); use-vlan-id; }</pre>
Hierarchy Level	<pre>[edit forwarding-options dhcp-relay relay-option-82], [edit forwarding-options dhcp-relay group <i>group-name</i> relay-option-82], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay ... relay-option-82], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ... relay-option-82], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ... relay-option-82]</pre>
Release Information	Statement introduced in Junos OS Release 14.1.
Description	Specify the Agent Remote ID suboption (suboption 2) of the DHCP relay agent information option (option 82) to include in DHCP packets destined for a DHCP server. Optionally specify that the suboption includes a prefix, textual description, or VLAN tag.



NOTE: For Layer 3 interfaces, when you configure relay-option-82 only, the Agent Remote ID is the default. If no VLAN tags are configured, then the default is the logical interface device (IFL) name. For integrated routing and bridging (IRB) interfaces, the default is the Layer 2 IFL name and bridge domain name.

The interface to bridge domain relationship may be implicit (the interface is mapped to the bridge domain by the system based on VLAN tag) or explicit (the interface is mapped to the bridge domain by configuring it in the bridge domain definition). For the explicit case, tagging might not be relevant for the mapping.

The format of the Agent Remote ID information for Fast Ethernet or Gigabit Ethernet interfaces that do not use virtual LANs (VLANs), stacked VLANs (S-VLANs), or bridge domains is as follows:

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



NOTE: For remote systems, the *subunit* is required and is used to differentiate an interface.

The format of the Agent Remote ID information for Fast Ethernet or Gigabit Ethernet interfaces that use VLANs is as follows:

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

The format of the Agent Remote ID information for Fast Ethernet or Gigabit Ethernet interfaces that use S-VLANs is as follows:

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

In the case of an IRB interface, the format displays the Layer 2 interface instead of the IRB interface along with the bridge domain name. For IRB interfaces (or other pseudo devices) the default format is as follows:

- IRB interfaces that use bridge domains but do not use VLANs or S-VLANs:

(fe | ge)-fpc/pic/port.subunit:bridge-domain-name

- IRB interfaces that use VLANs:

(fe | ge)-fpc/pic/port.subunit:vlan-name

To include the IRB interface name with the Layer 2 interface name, configure the **include-irb-and-l2** statement. The format is as follows:

- IRB interfaces that use bridge domains but do not use VLANs or S-VLANs:

(fe | ge)-fpc/pic/port:bridge-domain-name+irb.subunit

- IRB interfaces that use VLANs:

(fe | ge)-fpc/pic/port:vlan-name+irb.subunit

To include only the IRB interface name without the Layer 2 interface and bridge domain or VLAN, configure the **no-vlan-interface-name** statement. The format is as follows:

irb.subunit

The remaining statements are explained separately.

Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Using DHCP Relay Agent Option 82 Information on page 266 • Configuring Option 82 Information on page 267

remote-port-range

Syntax	<code>remote-port-range low <i>low-value</i> high <i>high-value</i>;</code>
Hierarchy Level	[edit services ptsp rule <i>rule-name</i> term <i>precedence</i> from]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Specify the port range for rule matching.
Options	<i>low-value</i> —Lower boundary for the port range. <i>high-value</i> —Upper boundary for the port range.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>

remote-ports

Syntax	<code>remote-ports [<i>port-numbers</i>];</code>
Hierarchy Level	[edit services ptsp rule <i>rule-name</i> term <i>precedence</i> from]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Identify one or more ports for inclusion as a match condition.
Options	<i>port-numbers</i> —Port number.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>

remote-prefix-list

Syntax	<code>remote-prefix-list <i>prefix-list-name</i> <except>;</code>
Hierarchy Level	[edit services ptsp rule <i>rule-name</i> term <i>precedence</i> from]
Release Information	Statement introduced in Junos OS Release 10.2. IPv6 support introduced in Junos OS Release 12.2
Description	Specify the prefix list for rule matching. You configure the prefix list by including the prefix-list statement at the [edit policy-options] hierarchy level.
Options	<i>prefix-list-name</i> —Prefix list. except —(Optional) Exclude the specified prefix list from rule matching.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>

replace-ip-source-with

Syntax	replace-ip-source-with giaddr;
Hierarchy Level	[edit forwarding-options dhcp-relay overrides], [edit forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]
Release Information	Statement introduced in Junos OS Release 9.6. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr).
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Extended DHCP Relay Agent Overview on page 194• Replacing the DHCP Relay Request and Release Packet Source Address on page 261

report-interface-descriptions (Edit Access)

Syntax	report-interface-descriptions;
Hierarchy Level	[edit access]
Release Information	Statement introduced in Junos OS Release 13.1.
Description	Enable storing and reporting of interface descriptions through RADIUS. To disable storing and reporting of interface descriptions, configure the [edit access profile <i>profile-name</i> radius attributes exclude] statement to exclude the interface description attribute. The description can contain letters, numbers, and hyphens (-), and can be up to 64 characters long.
Required Privilege Level	access—To view this statement in the configuration. access-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• exclude on page 724• Configuring RADIUS Server Options for Subscriber Access on page 102• Configuring Authentication and Accounting Parameters for Subscriber Access on page 80• Subscriber Access Interface Description Storage and Reporting Through RADIUS Overview on page 7

[request network-access aaa replay pending-accounting-stops](#)

Syntax	request network-access aaa replay pending-accounting-stops
Release Information	Command introduced in Junos OS Release 13.1.
Description	Force the router to attempt contact with the accounting sever immediately, rather than allowing it to wait until the periodic interval has expired.
Options	This command has no options.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• Forcing the Router to Contact the Accounting Server Immediately on page 101• show accounting pending-accounting-stops on page 1051
List of Sample Output	request network-access aaa replay pending-accounting-stops on page 902
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

[request network-access aaa replay pending-accounting-stops](#)

```
user@host> request network-access aaa replay pending-accounting-stops
replay started
```

request network-access aaa subscriber add session-id

Syntax	<code>request network-access aaa subscriber add session-id <i>subscriber-session-id</i> service-profile <i>profile-name</i></code>
Release Information	Command introduced in Junos OS Release 11.2.
Description	Locally activate a dynamic subscriber service for a subscriber who is currently logged in to the network.
Options	<p><i>profile-name</i>—Name of service-profile to activate.</p> <p><i>subscriber-session-id</i>—ID of the subscriber session for which the service will be added.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • CLI-Activated Subscriber Services on page 331 • Activating and Deactivating Subscriber Services Locally with the CLI on page 332 • request network-access aaa subscriber delete session-id on page 905
List of Sample Output	request network-access aaa subscriber add session-id service-profile on page 904
Output Fields	When you enter this command, you are provided feedback on the status of your request. Table 55 on page 903 lists possible error messages that might be returned if the service activation fails.

Table 55: Service Activation/Deactivation Error Messages

Message	Description	Corrective Action
Command failed: <i>reason</i>	—	—
Error: AUTHD ISSU in progress	A unified ISSU operation is active.	Wait until the unified ISSU operation completes and then retry the service activation/deactivation.
Provisioning is already active	Remote provisioning by a JSRC server or Gx-plus server is active.	—
Service activation/deactivation already in progress	Another service activation/deactivation operation is currently in progress.	Wait until the active operation completes and then retry the activation/deactivation operation.
Session identifier is not for a subscriber session	The session ID is incorrect.	Verify the correct session ID for the subscriber and then retry the activation/deactivation operation.

Sample Output

request network-access aaa subscriber add session-id service-profile

```
user@host> request network-access aaa subscriber add session-id 49 service-profile  
service-bronze  
Successful completion
```

request network-access aaa subscriber delete session-id

Syntax	<code>request network-access aaa subscriber delete session-id <i>subscriber-session-id</i> service-profile <i>profile-name</i></code>
Release Information	Command introduced in Junos OS Release 11.2.
Description	Deactivate a dynamic subscriber service for a subscriber who is currently logged in to the network.
Options	<p><i>profile-name</i>—Name of the service-profile to deactivate. To deactivate a single instance of a subscriber service that has multiple instances, you can specify the service-profile name and its service parameters.</p> <p><i>subscriber-session-id</i>—ID of the subscriber session for which the service will be deleted.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • CLI-Activated Subscriber Services on page 331 • Activating and Deactivating Subscriber Services Locally with the CLI on page 332 • Deactivating a Single Instance of a Subscriber Service with Multiple Instances on page 341 • Deactivating All Instances of a Subscriber Service with Multiple Instances on page 343 • request network-access aaa subscriber add session-id on page 903
List of Sample Output	<p>request network-access aaa subscriber delete session-id service-profile on page 906</p> <p>request network-access aaa subscriber delete session-id service-profile (Deactivating a Single Server Instance) on page 906</p> <p>request network-access aaa subscriber delete session-id service-profile (Deactivating All Server Instances) on page 906</p>
Output Fields	When you enter this command, you are provided feedback on the status of your request. Table 56 on page 905 lists possible error messages that might be returned if the service deactivation fails.

Table 56: Service Activation/Deactivation Error Messages

Message	Description	Corrective Action
Command failed: <i>reason</i>	Error condition that caused the command to fail.	Correct the error condition.
Error: AUTHD ISSU in progress	A unified ISSU operation is active.	Wait until the unified ISSU operation completes and then retry the service activation/deactivation.

Table 56: Service Activation/Deactivation Error Messages (*continued*)

Message	Description	Corrective Action
Provisioning is already active	Remote provisioning by a JSRC server or Gx-plus server is active.	Disable provisioning.
Service activation/deactivation already in progress	Another service activation/deactivation operation is currently in progress.	Wait until the active operation completes and then retry the activation/deactivation operation.
Session identifier is not for a subscriber session	The session ID is incorrect.	Verify the correct session ID for the subscriber and then retry the activation/deactivation operation.

Sample Output

request network-access aaa subscriber delete session-id service-profile

```
user@host> request network-access aaa subscriber delete session-id 49 service-profile
service-silver
Successful completion
```

request network-access aaa subscriber delete session-id service-profile (Deactivating a Single Server Instance)

```
user@host> request network-access aaa subscriber delete session-id 6 service-profile
economy-service(up-filter,down-filter)
Successful completion
```

request network-access aaa subscriber delete session-id service-profile (Deactivating All Server Instances)

```
user@host> request network-access aaa subscriber delete session-id 6 service-profile
economy-service
Successful completion
```

request network-access aaa subscriber modify session-id

Syntax	<code>request network-access aaa subscriber modify session-id <i>subscriber-session-id</i> <i>predefined-variable</i> <i>variable-option</i></code>
Release Information	Command introduced in Junos OS Release 11.2.
Description	Modify a predefined variable that is applied to a subscriber who is currently logged in to the network.
Options	<p><i>predefined-variable</i>—Name of the predefined variable that you want to modify.</p> <p><i>subscriber-session-id</i>—ID of the subscriber session.</p> <p><i>variable-option</i>—Name of the variable option that you want to apply to the predefined variable.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Using the CLI to Modify Traffic-Control Profiles That Are Currently Applied to Subscribers on page 335 • CLI-Activated Subscriber Services on page 331
List of Sample Output	request network-access aaa subscriber modify session-id on page 907
Output Fields	When you enter this command, you are provided feedback on the status of your request. Table 57 on page 907 lists possible messages that might be returned.

Table 57: Service Activation/Deactivation Error Messages

Message	Description	Corrective Action
Successful completion	Variable was successfully modified	—
Error: AUTHD ISSU in progress	A unified ISSU operation is active.	Wait until the unified ISSU operation completes and then retry the service activation/deactivation.

Sample Output

request network-access aaa subscriber modify session-id

```
user@host> request network-access aaa subscriber modify session-id 49
junos-cos-traffic-control-profile TCP-gold
Successful completion
```

request-rate

Syntax	<code>request-rate <i>rate</i>;</code>
Hierarchy Level	[edit access radius-options]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	(M120, M320, and MX Series routers) Configure the number of requests the router can send per second to all configured RADIUS servers collectively. By limiting the flow of requests from the router to the RADIUS servers, you can prevent the RADIUS servers from being flooded with requests.
Options	<p>rate—Number of requests per second.</p> <p>Range: 500 through 4000 requests per second</p> <p>Default: 500 requests per second</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Server Options for Subscriber Access on page 102• Configuring Router or Switch Interaction with RADIUS Servers on page 99

requested-ip-network-match (DHCP Local Server)

Syntax	<code>requested-ip-network-match <i>subnet-mask</i>;</code>
Hierarchy Level	<p>[edit system services dhcp-local-server] [edit system services dhcp-local-server dhcpv6], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server ...], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...]</p>
Release Information	Statement introduced in Junos OS Release 12.2.
Description	<p>Configure the subnet to which the DHCP local server matches the requested IP address (IPv6 address for DHCPv6 local server). The server accepts and uses the active client's requested address for address assignment only when the requested address and the IP address of the DHCP server interface (or IPv6 address of the DHCPv6 local server) are in the same subnet. The server accepts and uses the passive client's requested address for address assignment only when the requested address and the address of the relay interface are in the same subnet.</p>
Options	<p><i>subnet-mask</i>—Length of the subnet mask.</p> <p>Range:</p> <ul style="list-style-type: none"> DHCP: 0 through 15 DHCPv6: 0 through 127 <p>Default:</p> <ul style="list-style-type: none"> DHCP: 8 DHCPv6: 16
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Specifying the Subnet for DHCP Client Address Assignment on page 206

retransmit-timer (Dynamic Router Advertisement)

Syntax	<code>retransmit-timer <i>milliseconds</i>;</code>
Hierarchy Level	[edit protocols router-advertisement interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	Set the retransmission frequency of neighbor solicitation messages.
Options	<i>milliseconds</i> —Retransmission frequency. Default: 0 milliseconds
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Example: Configuring IPv6 Interfaces and Enabling Neighbor Discovery</i>

retry

Syntax	<code>retry <i>attempts</i>;</code>
Hierarchy Level	[edit access radius-server <i>server-address</i>], [edit access profile <i>profile-name</i> radius-server <i>server-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify the number of times that the router or switch is allowed to attempt to contact a RADIUS authentication or accounting server.
Options	<i>attempts</i> —Number of times that the router is allowed to attempt to contact a RADIUS server. Range: 1 through 30 Default: 3
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Authentication and Accounting Parameters for Subscriber Access on page 80• Configuring Router or Switch Interaction with RADIUS Servers on page 99• <i>Example: Configuring CHAP Authentication with RADIUS</i>• <i>Configuring RADIUS Authentication for L2TP</i>• timeout on page 950

revert-interval

Syntax	<code>revert-interval <i>interval</i>;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> radius options], [edit access radius-options]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	Configure the amount of time the router or switch waits after a server has become unreachable. The router or switch rechecks the connection to the server when the specified interval expires. If the server is then reachable, it is used in accordance with the order of the server list.
Options	<i>interval</i> —Amount of time to wait. Range: 0 through 604800 seconds Default: 60 seconds
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring RADIUS Server Options for Subscriber Access on page 102 • Configuring Authentication and Accounting Parameters for Subscriber Access on page 80

route (Diameter Network Element)

Syntax	<pre>route <i>dne-route-name</i> { destination realm <i>realm-name</i> <host <i>hostname</i>>; function <i>function-name</i> <partition <i>partition-name</i>>; metric <i>route-metric</i>; }</pre>
Hierarchy Level	[edit diameter network-element <i>element-name</i> forwarding]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Define a route reachable through the Diameter network element by associating a metric with a combination of destination and function partition.
Options	<i>dne-route-name</i> —Route name defined for the Diameter network element. The remaining statements are explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Diameter on page 434• Configuring Diameter Network Elements on page 437

router (Address-Assignment Pools)

Syntax	<pre>router [<i>router-address</i>];</pre>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	Specify one or more routers located on the client's subnet. This statement is the equivalent of DHCP option 3.
Options	<i>router-address</i> —IP address of one or more routers.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Address-Assignment Pools on page 316

router-advertisement (Dynamic Profiles)

Syntax	router-advertisement {...}
Hierarchy Level	[edit dynamic-profiles protocols]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	Enable router advertisement. The remaining statements are explained separately.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Example: Configuring IPv6 Interfaces and Enabling Neighbor Discovery</i>

routing-instance

Syntax	routing-instance <i>routing-instance-name</i> ;
Hierarchy Level	[edit access radius-server <i>server-address</i>], [edit access profile <i>profile-name</i> radius-server <i>server-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the routing instance used to send RADIUS packets to the RADIUS server.
Options	<i>routing-instance-name</i> —Routing instance name.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring the PPP Authentication Protocol</i> • Configuring Authentication and Accounting Parameters for Subscriber Access on page 80

routing-instance (Diameter Peer)

Syntax	<code>routing-instance <i>routing-instance-name</i> ;</code>
Hierarchy Level	<code>[edit diameter peer <i>peer-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Specify a routing instance for a Diameter peer. Alternatively, you can include the logical-system statement at the <code>[edit diameter peer <i>peer-name</i>]</code> hierarchy level to configure a logical and routing instance.
Options	<i>routing-instance-name</i> —Name of the routing instance. Default: Master routing instance
Required Privilege Level	admin —To view this statement in the configuration. admin-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Diameter on page 434• Configuring Diameter Peers on page 435

routing-instance (Diameter Transport)

Syntax	<code>routing-instance <i>routing-instance-name</i> ;</code>
Hierarchy Level	<code>[edit diameter transport <i>transport-name</i>]</code>
Release Information	Statement introduced in Junos OS Release 11.2.
Description	Specify a routing instance for the Diameter transport layer connection.
Options	<i>routing-instance-name</i> —Name of the routing instance. Default: Master routing instance
Required Privilege Level	admin —To view this statement in the configuration. admin-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Diameter Transport on page 436

routing-instance-name (Static Subscribers)

Syntax	routing-instance-name;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers authentication username-include],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication username-include],</p> <p>[edit system services static-subscribers authentication username-include],</p> <p>[edit system services static-subscribers group <i>group-name</i> authentication username-include]</p>
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Specify that the name of the routing instance is included as part of the username created for all static subscribers or for the static subscribers in the specified group. The group version of the statement takes precedence over the global version. The username is also sent to RADIUS in the Access-Request message.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Subscribers over Static Interfaces on page 466 • Configuring the Static Subscriber Global Username on page 473 • Configuring the Static Subscriber Group Username on page 478

routing-instance-name (DHCP Relay Agent)

Syntax	routing-instance-name;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay authentication username-include],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p>
Description	Specify that the routing instance name is concatenated with the username during the subscriber authentication or client authentication process. No routing instance name is concatenated if the configuration is in the default routing instance. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using External AAA Authentication Services with DHCP on page 217 • Creating Unique Usernames for DHCP Clients on page 218

routing-instance-name (DHCP Local Server)

Syntax	routing-instance-name;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server group group-name authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify that the routing instance name be concatenated with the username during the subscriber authentication or DHCP client authentication process. No routing instance name is concatenated if the configuration is in the default routing instance.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

- Related Documentation**
- [Using External AAA Authentication Services with DHCP on page 217](#)

rule (Configuring)

Syntax

```
rule rule-name {
  count-type (application | rule);
  demux (destination-address | source-address);
  forward-rule forward-rule-name;
  match-direction (input | input-output | output);
  term precedence {
    from {
      application-group-any;
      application-groups [ application-group-name ];
      applications [ application-name ];
      local-port-range low low-value high high-value;
      local-ports [ value-list ];
      protocol protocol-number;
      remote-address address <except>;
      remote-address-range low low-value high high-value <except>;
      remote-ports [ value-list ];
      remote-port-range low low-value high high-value;
      remote-prefix-list prefix-list-name <except>;
    }
    then {
      (accept | discard);
      count (application | application-group | application-group-any | rule | none);
      forwarding-class forwarding-class;
      police policer-name;
    }
  }
}
```

Hierarchy Level [edit services ptsp]

Release Information Statement introduced in Junos OS Release 10.2.

Description Specify the rule the router uses when applying this service.

Options *rule-name*—Identifier for the collection of terms that constitute this rule.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

- Related Documentation**
- [Configuring Static PTSP Rules on page 495 in Junos OS Subscriber Management and Services Library](#)

rule (Including in Rule Set)

Syntax	<code>rule rule-name;</code>
Hierarchy Level	[edit services ptsp rule-set rule-set-name]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Specify the rule the router uses when applying this service.
Options	rule-name —Identifier for the collection of terms that constitute this rule.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>

rule-set (Services PTSP)

Syntax	<pre>rule-set rule-set-name { [rule rule-names]; }</pre>
Hierarchy Level	[edit services ptsp]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Specify the rule set the router uses when applying this service.
Options	rule-set-name —Identifier for the collection of rules that constitute this rule set.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>

secret

Syntax	<code>secret password;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> radius-server <i>server-address</i>], [edit access radius-disconnect <i>client-address</i>], [edit access radius-server <i>server-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the password to use with the RADIUS server. The secret password used by the local router or switch must match that used by the server.
Options	password —Password to use; it can include spaces if the character string is enclosed in quotation marks.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Authentication and Accounting Parameters for Subscriber Access on page 80• Configuring Router or Switch Interaction with RADIUS Servers on page 99• Example: Configuring CHAP Authentication with RADIUS• Configuring RADIUS Authentication for L2TP• Configuring the RADIUS Disconnect Server for L2TP• Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure)

send-acct-status-on-config-change (Access Profile)

Syntax	send-acct-status-on-config-change;
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in Junos OS Release 13.1. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Description	Configure the router's authd process to send an Acct-On message when the first RADIUS server is added to an access profile, and to send an Acct-Off message when the last RADIUS server is removed from an access profile.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Server Parameters for Subscriber Access on page 102• Configuring Per-Subscriber Session Accounting on page 92

send-release-on-delete (DHCP Relay Agent)

Syntax	send-release-on-delete;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay dhcpv6 overrides], [edit forwarding-options dhcp-relay overrides], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides], [edit forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.2.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.3 for EX Series switches.</p>
Description	<p>Send a release message to the DHCP (or DHCPv6) server whenever DHCP relay or relay proxy deletes a client. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.</p> <p>M120 and M320 routers do not support DHCPv6.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Extended DHCP Relay Agent Overview on page 194 • Overriding the Default DHCP Relay Configuration Settings on page 256 • Sending Release Messages When Clients Are Deleted on page 264

server-group

Syntax	<pre>server-group { server-group-name { server-ip-address; } }</pre>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay], [edit forwarding-options dhcp-relay dhcpv6], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6]</p>
Release Information	<p>Statement introduced in Junos OS Release 8.3. Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4. Statement introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	<p>Specify the name of a group of DHCP server addresses for use by the extended DHCP relay agent. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.</p>
Options	<p><i>server-group-name</i>—Name of the group of DHCP or DHCPv6 server addresses.</p> <p><i>server-ip-address</i>—IP address of the DHCP server belonging to this named server group. Use IPv6 addresses when configuring DHCPv6 support. You can configure a maximum of five IP addresses in each named server group.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • dhcp-relay on page 689 • Extended DHCP Relay Agent Overview on page 194 • Configuring Server Groups on page 259

server-identifier (Address-Assignment Pools)

Syntax	<code>server-identifier <i>ipv4-address</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Specify the IP address that is used as the source address the DHCP server includes in IP packets when communicating with clients. The address is included in the DHCP packet in option 54.
Options	<i>ipv4-address</i> —IP address.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Address-Assignment Pools on page 316

server-response-time (DHCP Relay Agent)

Syntax	<code>server-response-time <i>seconds</i>;</code>
Hierarchy Level	[edit forwarding-options dhcp-relay], [edit forwarding-options dhcp-relay dhcpv6], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...]
Release Information	Statement introduced in Junos OS Release 13.3.
Description	Configure the timeframe during which the router monitors DHCP server responsiveness within the routing instance. The router generates a system log message when the DHCP server does not respond to relayed packets during the specified timeframe.
Options	<i>seconds</i> —Number of seconds the DHCP server is monitored. Range: 30 through 4,294,967,295 seconds Default: 0 (no limit)
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Monitoring DHCP Relay Server Responsiveness on page 310

service (Service Accounting)

Syntax	<pre>service { accounting-order (activation-protocol radius); }</pre>
Hierarchy Level	[edit access profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 11.4. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Description	Define the subscriber service accounting configuration. The remaining statement is explained separately.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Service Accounting with JSRC on page 460• Service Accounting with JSRC on page 459

service-profile (DHCP Local Server)

Syntax	<code>service-profile <i>dynamic-profile-name</i>;</code>
Hierarchy Level	<p>[edit system services dhcp-local-server], [edit system services dhcp-local-server dhcpv6], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i>], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>], [edit system services dhcp-local-server group <i>group-name</i>], [edit system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...]</p>
Release Information	<p>Statement introduced in Junos OS Release 11.2. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	<p>Specify the default subscriber service or DHCP client management service, which is activated when the subscriber or client logs in and no other service is activated by a RADIUS server or a provisioning server.</p> <ul style="list-style-type: none"> To specify the default service for all DHCP local server clients, include the service-profile statement at the [edit system services dhcp-local-server] hierarchy level. To specify the default service for a named group of interfaces, include the service-profile statement at the [edit system services dhcp-local-server group <i>group-name</i>] hierarchy level. To specify the default service for a particular interface within a named group of interfaces, include the service-profile statement at the [edit system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i>] hierarchy level. For DHCPv6 clients, use the service-profile statement at the [edit system services dhcp-local-server dhcpv6] hierarchy level.
Options	<i>dynamic-profile-name</i> —Name of the dynamic profile that defines the service.
Required Privilege Level	<p>system—To view this statement in the configuration. system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Extended DHCP Local Server Overview on page 188 Default Subscriber Service Overview on page 199 Configuring a Default Subscriber Service on page 200

service-profile (DHCP Relay Agent)

Syntax	<code>service-profile <i>dynamic-profile-name</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay], [edit forwarding-options dhcp-relay dhcpv6], [edit forwarding-options dhcp-relay group <i>group-name</i>], [edit forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i>], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i>], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...]</p>
Release Information	<p>Statement introduced in Junos OS Release 11.2. Statement introduced in Junos OS Release 12.3R2 for EX Series switches. Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 11.4.</p>
Description	<p>Specify the default subscriber service (or the default DHCP client management service), which is activated when the subscriber (or client) logs in and no other service is activated by a RADIUS server or a provisioning server.</p> <ul style="list-style-type: none"> • To specify the default service for all DHCP relay agent clients, include the service-profile statement at the [edit forwarding-options dhcp relay] hierarchy level. • To specify the default service for a named group of interfaces, include the service-profile statement at the [edit forwarding-options dhcp relay group <i>group-name</i>] hierarchy level. • To specify the default service for a particular interface within a named group of interfaces, include the service-profile statement at the [edit forwarding-options dhcp relay group <i>group-name</i> interface <i>interface-name</i>] hierarchy level.
Options	<i>dynamic-profile-name</i> —Name of the dynamic profile.
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • dhcp-relay on page 689 • Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces • Grouping Interfaces with Common DHCP Configurations on page 223 • Default Subscriber Service Overview on page 199 • Configuring a Default Subscriber Service on page 200

services (PTSP)

Syntax	<code>services ptsp { ... }</code>
Hierarchy Level	[edit]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Define the services to be applied to traffic.
Options	ptsp —Identify the values configured for PTSP matching rules. The statements are explained separately.
Required Privilege Level	interface —To view this statement in the configuration. interface-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>

session-options

Syntax	<pre>session-options { client-idle-timeout minutes; client-session-timeout minutes; }</pre>
Hierarchy Level	[edit access profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 8.5.
Description	(MX Series and SRX Series devices) Define options that control a user's session after successful authentication. The remaining statements are explained separately.
Required Privilege Level	access —To view this statement in the configuration. access-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding Session Options for Subscriber Access on page 109• Configuring Subscriber Session Options on page 111

sip-server-address

Syntax	<code>sip-server-address <i>ipv6-address</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family <i>family</i> dhcp-attributes]
Release Information	Statement introduced in Junos OS Release 10.0.
Description	Specify a SIP outbound proxy server that DHCPv6 local server clients can use. This is equivalent to DHCPv6 option 22. To specify multiple serv <i>ipv6-addressers</i> , add multiple sip-server-address statements in order of preference.
Options	<i>ipv6-address</i> —IPv6 address of a SIP outbound proxy server.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Address-Assignment Pools Overview on page 315 • Configuring Address-Assignment Pools on page 316

sip-server-domain-name

Syntax	<code>sip-server-domain-name <i>domain-name</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family <i>family</i> dhcp-attributes]
Release Information	Statement introduced in Junos OS Release 10.0.
Description	Configure the domain name of the SIP outbound proxy server that DHCPv6 local server clients can use. This is equivalent to DHCPv6 option 21.
Options	<i>domain-name</i> —Name of the domain.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Address-Assignment Pools Overview on page 315 • Configuring Address-Assignment Pools on page 316

source-address

Syntax	<code>source-address <i>source-address</i>;</code>
Hierarchy Level	<code>[edit access radius-server <i>server-address</i>],</code> <code>[edit access profile <i>profile-name</i> radius-server <i>server-address</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure a source address for each configured RADIUS server. Each RADIUS request sent to a RADIUS server uses the specified source address.
Options	<i>source-address</i> —Valid IPv4 address configured on one of the router or switch interfaces. On M Series routers only, the source address can be an IPv6 address and the UDP source port is 514.
Required Privilege Level	<code>admin</code> —To view this statement in the configuration. <code>admin-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Router or Switch Interaction with RADIUS Servers on page 99• Configuring Authentication and Accounting Parameters for Subscriber Access on page 80• <i>Example: Configuring CHAP Authentication with RADIUS</i>• <i>Configuring RADIUS Authentication for L2TP</i>

stacked-vlan-ranges (RADIUS Options)

Syntax	stacked-vlan-ranges (any <i>low-outer-tag–high-outer-tag</i>),any;
Hierarchy Level	[edit interfaces <i>interface-name</i> radius-options nas-port-options <i>nas-port-options-name</i>]
Release Information	Statement introduced in Junos OS Release 12.3.
Description	Configure the stacked VLAN (S-VLAN) range of subscribers to which the named NAS-Port options definition applies.



NOTE: You can configure a maximum of 16 NAS-Port options definitions per physical interface. Each definition can include a maximum of 32 VLAN ranges or 32 S-VLAN ranges, but cannot include a combination of VLAN ranges and S-VLAN ranges.

Options **any**—Entire S-VLAN range representing all S-VLAN IDs. The inner tag (S-VLAN ID) of the S-VLAN range must be configured as **any** to represent all inner VLAN ID tags.

low-outer-tag—Outer VLAN ID tag representing the lower limit of the S-VLAN range.

Range: 1 through 4094

high-outer-tag—Outer VLAN ID tag representing the upper limit of the S-VLAN range.

Range: 1 through 4094



NOTE: To specify a single outer VLAN ID tag, set **low-outer-tag** and **high-outer-tag** to the same value.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 63](#)
- [Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 62](#)

starts-with (DHCP Relay Agent Option)

Syntax	<pre>starts-with (ascii <i>ascii-string</i> hexadecimal <i>hexadecimal-string</i>) { drop; forward-only; local-server-group <i>local-server-group</i>; relay-server-group <i>relay-server-group</i>; }</pre>
Hierarchy Level	<pre>[edit forwarding-options dhcp-relay relay-option], [edit forwarding-options dhcp-relay dhcpv6 relay-option], [edit forwarding-options dhcp-relay group <i>group-name</i> relay-option], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> relay-option], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...]</pre>
Release Information	Statement introduced in Junos OS Release 12.3.
Description	<p>Configure a partial match criteria used with the DHCP relay agent selective processing feature. DHCP relay agent compares the configured partial match string with the option-specific string received in DHCP client packets. If there is an partial left-to-right match, DHCP performs the action you define for the match criteria.</p> <p>The option-specific string in the DHCP client packets can contain a superset of the specified ASCII or hexadecimal match string, provided that the leftmost characters of the option-specific string entirely match the characters in the configured match string.</p> <p>You can configure an unlimited number of match strings. If you have multiple partial match configurations, the longest match rule applies. For example, DHCP relay agent matches the string "test123" before it matches the string "test". Match strings do not support wildcard attributes.</p> <p>The local-server-group option is not supported for DHCPv6 relay agent.</p>
Options	<p><i>ascii-string</i>—ASCII string of 1 through 255 alphanumeric characters.</p> <p><i>hexadecimal-string</i>—Hexadecimal string of 1 through 255 hexadecimal characters (0 through 9, a through f, A through F).</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using DHCP Option Information to Selectively Process DHCP Client Traffic on page 273

static-subscribers

Syntax	<pre> static-subscribers { access-profile <i>profile-name</i>; authentication { password <i>password-string</i>; username-include { domain-name <i>domain-name</i>; interface; logical-system-name; routing-instance-name; user-prefix <i>user-prefix-string</i>; } } dynamic-profile <i>profile-name</i> { aggregate-clients (merge replace); } group <i>group-name</i> { access-profile <i>profile-name</i>; authentication { password <i>password-string</i>; username-include { domain-name <i>domain-name</i>; interface; logical-system-name; routing-instance-name; user-prefix <i>user-prefix-string</i>; } } dynamic-profile <i>profile-name</i> { aggregate-clients (merge replace); } interface <i>interface-name</i> <exclude> <upto <i>upto-interface-name</i>>; } } </pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> system services], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services], [edit routing-instances <i>routing-instances-name</i> system services], [edit system services]</p>
Release Information	Statement introduced in Junos OS Release 9.6.
Description	<p>Configure and associate subscribers with statically configured interfaces for dynamic service provisioning.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration. system-control—To add this statement to the configuration.</p>

- Related Documentation**
- [Configuring Subscribers over Static Interfaces on page 466](#)

statistics (Access Profile)

Syntax	statistics (time volume-time);
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches. Option volume-time introduced in Junos OS Release 9.4.
Description	Configure the router or switch to collect time statistics, or both volume and time statistics, for the sessions being managed by AAA.
Options	time —Collect uptime statistics only. volume-time —Collect both volume and uptime statistics. This option is not available for Mobile IP.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Mobile IP Home Agent Elements and Behavior</i>• Configuring Authentication and Accounting Parameters for Subscriber Access on page 80


strict (DHCP Local Server)

Syntax	strict;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.4.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify whether the server denies a client to bind when the client does not indicate that it accepts reconfigure messages. This feature is available only for DHCPv6.
Default	Accept solicit messages from clients that do not support reconfiguration and permit them to bind.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Dynamic Client Reconfiguration of Extended Local Server Clients on page 244 • Preventing Binding of Clients That Do Not Support Reconfigure Messages on page 292

strip-domain (Domain Map)

Syntax	strip-domain;
Hierarchy Level	[edit access domain map <i>domain-map-name</i>]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Remove the domain name from the username before continuing with any AAA services specified in a domain map.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Enabling Domain Name Stripping on page 139• Configuring Domain and Realm Name Usage for Domain Maps on page 136

subscriber-identification (PTSP)

Syntax	<code>subscriber-identification <i>subscriber-identification</i></code>
Hierarchy Level	[edit system services packet-triggered-subscribers partition radius <i>radius-partition-name</i>]
Release Information	Statement introduced in Junos OS Release 11.3.
Description	Configure the subscriber identification to be used in a PTSP partition. You can configure the subscriber identification only in a RADIUS partition.
Options	<p><i>subscriber-identification</i>—String of user-defined characters or a RADIUS attribute type that is supported by the PTSP application. To enable subscriber identification for the specified RADIUS attribute, you may configure the following RADIUS attributes:</p> <ul style="list-style-type: none"> • <code>\$attribute-1\$</code>—User-Name • <code>\$attribute-4\$</code>—NAS-IP-Address • <code>\$attribute-5\$</code>—NAS-Port • <code>\$attribute-8\$</code>—Framed-IP-Address • <code>\$attribute-32\$</code>—NAS-Identifier • <code>\$attribute-87\$</code>—NAS-Port-ID <p>When configuring subscriber identification, you must precede the "\$" with a slash (\) to enable the CLI interface to process and store the variable correctly.</p>
<div style="display: flex; align-items: center;">  <div> <p>NOTE: The IP address is formatted in dotted decimal notation—for example, 192.168.1.1. All the other numeric values are converted to a string of characters.</p> </div> </div>	
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring the PTSP Partition on page 491

subscriber-packet-idle-timeout

Syntax	<code>subscriber-packet-idle-timeout <i>subscriber-packet-idle-timeout</i>;</code>
Hierarchy Level	[edit system services packet-triggered-subscribers]
Description	The subscriber packet idle timeout for packet triggered subscribers.
Options	<i>subscriber-packet-idle-timeout</i> —Maximum idle time. Range: 15 through 1440 minutes.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Packet-Triggered Subscribers Services Overview on page 482

subscriber-management (Subscriber Management)

Syntax	<pre> subscriber-management { enforce-strict-scale-limit-license; gres-route-flush-delay; maintain-subscriber { interface-delete; } traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i> > <size <i>maximum-file-size</i>> <world-readable no-world-readable>; flag <i>flag</i>; } } </pre>
Hierarchy Level	[edit system services]
Release Information	Statement introduced in Junos OS Release 11.1.
Description	<p>Configure global services for subscriber management, such as maintaining subscribers and tracing operations.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring the Router to Strictly Enforce the Subscriber Scaling License</i> • <i>Delaying Removal of Access Routes and Access-Internal Routes After Graceful Routing Engine Switchover</i> • Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events on page 238 • Tracing Subscriber Management Database Operations for Subscriber Access on page 531

subscriber-profile

Syntax subscriber-profile *profile-name* {
 enable *service-name* {
 concurrent-data-sessions *max-session-number*;
 }
 disable *service-name*;
 max-data-sessions-per-subscriber {
 limit *max-sub-sessions*;
 exceed-action {
 drop;
 syslog;
 }
 }
 }

Hierarchy Level [edit services service-set *services-set-name*]

Release Information Statement introduced in Junos OS Release 11.4.

Description Specify the subscriber profile name. A subscriber profile specifies which services should be enabled and which services should be disabled for traffic belonging to a subscriber bound to a particular subscriber profile. A subscriber is bound to a minimum of one subscriber profile at any given time.

Options *profile-name*—Name of the profile.

Required Privilege Level admin—To view this statement in the configuration.
 admin-control—To add this statement to the configuration.


t1-percentage (Address-Assignment Pools)

Syntax	<code>t1-percentage <i>percentage</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet6 dhcp-attributes]
Release Information	Statement introduced in Junos OS Release 13.3.
Description	<p>Specify a percentage of the preferred-lifetime value. After this percentage of the preferred-lifetime value elapses, the router requests an extension on its lease from the originating DHCPv6 server. The t1-percentage is also referred to as the renewal time.</p> <p>The t1-percentage value must be less than the t2-percentage value.</p>
Options	<p>percentage—Percentage of the preferred-lifetime value.</p> <p>Range: 0 through 100</p> <p>Default: If the t1-percentage value is not configured, the default is based on the preferred-lifetime value, as follows.</p> <ul style="list-style-type: none"> • If the preferred-lifetime value is finite, the default is 50 percent of the preferred-lifetime value. • If the preferred-lifetime value is infinite, the default is also infinite.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Address-Assignment Pools on page 316 • DHCP Attributes for Address-Assignment Pools on page 201 • dhcp-attributes (Address-Assignment Pools) on page 683 • preferred-lifetime (Address-Assignment Pools) on page 853 • t2-percentage (Address-Assignment Pools) on page 942


t2-percentage (Address-Assignment Pools)

Syntax	t2-percentage <i>percentage</i> ;
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet6 dhcp-attributes]
Release Information	Statement introduced in Junos OS Release 13.3.
Description	<p>Specify a percentage of the preferred-lifetime value. After this percentage of the preferred-lifetime value elapses, the router requests an extension on its lease from any available DHCPv6 server. The t1-percentage is also referred to as the rebinding time.</p> <p>The t2-percentage value must be greater than the t1-percentage value.</p>
Options	<p>percentage—Percentage of the preferred-lifetime value.</p> <p>Range: 0 through 100</p> <p>Default: If the t2-percentage value is not configured, the default is based on the preferred-lifetime value.</p> <ul style="list-style-type: none">• If the preferred-lifetime value is finite, the default is 80 percent. of the preferred-lifetime value.• When the preferred-lifetime value is infinite, the default is also infinite.
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring Address-Assignment Pools on page 316• DHCP Attributes for Address-Assignment Pools on page 201• dhcp-attributes (Address-Assignment Pools) on page 683• preferred-lifetime (Address-Assignment Pools) on page 853• t1-percentage (Address-Assignment Pools) on page 941

target-logical-system (Domain Map)

Syntax	target-logical-system <i>logical-system-name</i> { target-routing-instance <i>routing-instance-name</i> ; }
Hierarchy Level	[edit access domain map <i>domain-map-name</i>]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	<p>Configure a non-default logical system and optionally a non-default routing instance for the subscriber's interface in a domain map.</p> <p>You use the target-routing-instance statement at the [edit access domain map <i>domain-map-name</i>] hierarchy level to configure a non-default routing instance for the default logical system.</p>
	<div>  <p>NOTE: Subscriber management is supported in the default logical system only.</p> </div>
Default	Default logical system for the subscriber..
Options	<p><i>logical-system-name</i>—Name of the logical system.</p> <p>The remaining statement is explained separately.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Specifying a Target Logical System/Routing Instance in a Domain Map on page 135

target-routing-instance (Domain Map)

Syntax	target-routing-instance (<i>routing-instance-name</i> default);
Hierarchy Level	[edit access domain map <i>domain-map-name</i>], [edit access domain map <i>domain-map-name</i> target-logical-system <i>logical-system-name</i>]
Release Information	Statement introduced in Junos OS Release 10.4. Option default introduced in Junos OS Release 13.3.
Description	Configure the routing instance of the subscriber context.
<div> NOTE: Subscriber management is supported in the default logical system only. The target-logical-system statement, which appears in the CLI, is not supported in current Junos OS releases.</div>	
Default	For dynamic LNS sessions, the routing instance of the peer (LAC facing) interface. For all other sessions, the default logical system/routing instance context.
Options	routing-instance-name —Name of the routing instance. default —The default (master) routing instance.
Required Privilege Level	admin —To view this statement in the configuration. admin-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Understanding Domain Maps and Logical System/Routing Instance Contexts on page 130• Specifying a Target Logical System/Routing Instance in a Domain Map on page 135

term (Forward Rule)

Syntax	<pre> term <i>precedence</i> { from { application-groups [<i>application-group-name</i>]; applications [<i>application-name</i>]; local-address <i>address</i> <except>; local-address-range low <i>low-value</i> high <i>high-value</i> <except>; local-prefix-list <i>prefix-list-name</i> <except>; } then { forwarding-instance <i>forwarding-instance</i>; unit-number <i>unit-number</i>; } } </pre>
Hierarchy Level	[edit services ptsp forward-rule <i>forward-rule-name</i>]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Define the term properties for the forward rule.
Options	<p><i>precedence</i>—Precedence value for this term in relation to other terms. Term with lowest precedence is evaluated first.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>

term (Rule)

Syntax	<pre> term precedence { from { application-group-any; application-groups [application-group-name]; applications [application-name]; local-port-range low low-value high high-value; local-ports [value-list]; protocol protocol-number; remote-address address <except>; remote-address-range low low-value high high-value <except>; remote-port-range low low-value high high-value; remote-ports [value-list]; remote-prefix-list prefix-list-name <except>; } then { (accept discard); count (application application-group application-group-any rule); forwarding-class forwarding-class; police policer-name; } } </pre>
Hierarchy Level	[edit services ptsp rule rule-name]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Define the term properties for the PTSP rule.
Options	<p>precedence—Precedence value for this term in relation to other terms. Term with lowest precedence is evaluated first.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>

terminate-code

Syntax	<pre> terminate-code { (aaa (deny shutdown) dhcp l2tp ppp) <i>term-reason</i> radius <i>term-cause</i>; } </pre>
Hierarchy Level	[edit access]
Release Information	Statement introduced in Junos OS Release 11.4.
Description	Customize mappings between a terminate reason and a RADIUS Acct-Terminate-Cause attribute.
Options	<p>aaa—Defines AAA as the protocol type, and specifies either the deny or shutdown action to perform with the specified terminate reason.</p> <p>dhcp—Defines DHCP as the protocol type associated with the specified terminate reason.</p> <p>l2tp—Defines L2TP as the protocol type associated with the specified terminate reason.</p> <p>ppp—Defines PPP as the protocol type associated with the specified terminate reason.</p> <p><i>term-reason</i>—Terminate reason for the specified protocol type.</p> <p><i>term-cause</i>—Standards-based RADIUS Acct-Terminate-Cause code that identifies the terminate reason.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Custom Terminate Reason Mappings on page 153 • AAA Terminate Reasons on page 154 • DHCP Terminate Reasons on page 155 • L2TP Terminate Reasons on page 156 • PPP Terminate Reasons on page 172

tftp-server

Syntax	<code>tftp-server <i>ip-address</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	Specify the Trivial File Transfer Protocol (TFTP) server that the client uses to obtain the client configuration file. This is equivalent to DHCP option 150.
Options	<i>ip-address</i> —IP address of the TFTP server.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Address-Assignment Pools on page 316

then (Forward Rule)

Syntax	<pre>then { forwarding-instance <i>forwarding-instance</i>; unit-number <i>unit-number</i>; }</pre>
Hierarchy Level	[edit services ptsp forward-rule <i>forward-rule-name</i> term precedence]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Define the term actions for the forward rule.
Options	<i>forwarding-instance</i> —Identifier for the forwarding instance for packet flows accepted under this policy. <i>unit-number</i> —Unit number associated with the forwarding instance.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>

then (Rule)

Syntax	<pre> then { (accept discard); count (application application-group application-group-any rule); forwarding-class <i>forwarding-class</i>; police <i>policer-name</i>; } </pre>
Hierarchy Level	[edit services ptsp rule <i>rule-name</i> term <i>precedence</i>]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Define the term actions. You can configure the router to accept or discard the targeted traffic. The action modifiers (count and forwarding-class) are optional.
Options	<p>You can configure one of the following actions:</p> <ul style="list-style-type: none"> • accept—Accept the packets and all subsequent packets in flows that match the rules. • discard—Discard the packet and all subsequent packets in flows that match the rules. <p>When you select accept as the action, you can optionally configure one or both of the following action modifiers. No action modifiers are allowed with the discard action.</p> <ul style="list-style-type: none"> • count (application application-group application-group-any rule none)—For all accepted packets that match the rules, record a packet count using PTSP statistics practices. You can specify one of the following options; there is no default setting: <ul style="list-style-type: none"> • application—Count the application that matched in the from clause. • application-group—Count the application group that matched in the from clause. • application-group-any—Count all application groups that match from application-group-any under the any group name. • rule—Count the rule that matched in the from clause. • none—Same as not specifying count as an action. • forwarding-class <i>forwarding-class</i>—Specify the forwarding class name for outgoing packets. <p>When you include a policer, the only allowed action is discard. For more information on policers, see the <i>Routing Policies, Firewall Filters, and Traffic Policers Feature Guide for Routing Devices</i>.</p> <ul style="list-style-type: none"> • police <i>policer-name</i>—Apply rate-limiting properties to the traffic as configured at the [edit firewall policer <i>policer-name</i>] hierarchy level. This configuration allows bit-rate and burst-size attributes to be applied to the traffic that are not supported by PTSP rules.

Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Static PTSP Rules on page 495 in <i>Junos OS Subscriber Management and Services Library</i>

timeout (RADIUS)

Syntax	timeout <i>seconds</i> ;
Hierarchy Level	[edit access radius-server <i>server-address</i>], [edit access profile <i>profile-name</i> radius-server <i>server-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the amount of time that the local router or switch waits to receive a response from a RADIUS server.
Options	<i>seconds</i> —Amount of time to wait. Range: 1 through 90 seconds Default: 3 seconds
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Router or Switch Interaction with RADIUS Servers on page 99• Configuring Authentication and Accounting Parameters for Subscriber Access on page 80• <i>Example: Configuring CHAP Authentication with RADIUS</i>• <i>Configuring RADIUS Authentication for L2TP</i>

timeout (DHCP Local Server)

Syntax	<code>timeout <i>timeout-value</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit system services dhcp-local-server reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.0.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.</p>
Description	Configure the initial value in seconds between attempts to reconfigure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces.
Options	<p><i>timeout-value</i>—Initial retry timeout value.</p> <p>Range: 1 through 10 seconds</p> <p>Default: 2 seconds</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Dynamic Client Reconfiguration of Extended Local Server Clients on page 244 • Configuring Dynamic Reconfiguration Attempts for DHCP Clients on page 246

token (DHCP Local Server)

Syntax	<code>token <i>token-value</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit system services dhcp-local-server reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.0.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.</p>
Description	<p>Configure a plain-text token for all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. The token enables rudimentary entity authentication to protect against inadvertently instantiated DHCP servers. A null token (empty string) indicates that the configuration token functionality is not enabled. A group configuration takes precedence over a DHCP local server configuration. For more information about tokens, see RFC 3118, <i>Authentication for DHCP Messages</i>, section 4.</p>
Options	<p><i>token-value</i>—Plain-text alphanumeric string.</p> <p>Default: null (empty string)</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring Dynamic Client Reconfiguration of Extended Local Server Clients on page 244 Configuring a Token for DHCP Local Server Authentication on page 283

trace (DHCP Local Server)

Syntax	trace;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.4.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Enable trace operations for a group of interfaces or for a specific interface within a group.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Tracing Extended DHCP Operations on page 521 • Tracing Extended DHCP Operations for Specific Interfaces on page 526

traceoptions (ANCP)

Syntax	<pre>traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i> > <size <i>maximum-file-size</i>> <world-readable no-world-readable>; flag <i>flag</i> <disable>; level (all error info notice verbose warning); no-remote-trace; }</pre>
Hierarchy Level	[edit protocols ancp]
Release Information	Statement introduced in Junos OS Release 9.4.
Description	Define tracing operations for ANCP agent processes.
Options	<p>file <i>filename</i>— Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the size option.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. Include the disable option after a flag to disable tracing for that flag. You can include the following flags:</p> <ul style="list-style-type: none">• all—Trace all operations.• config—Trace configuration events.• cos—Trace class-of-service events.• general—Trace general flow.• packet—Trace ANCP packet transmit and receive operations.• process—Trace process internals.• protocol—Trace protocol events.• restart—Trace process restart flow• routing-socket—Trace routing socket events.• session—Trace connection events and flow.• startup—Trace ANCP startup events and flow.• subscriber—Trace subscriber events.• timer—Trace timer processing. <p>level—Level of tracing to perform. You can specify any of the following levels:</p>

- **all**—Match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

Default: error

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: *sizek* to specify KB, *sizem* to specify MB, or *sizeg* to specify GB

Range: 10240 through 1073741824

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level	trace—To view this statement in the configuration. trace-control—To add this statement to the configuration.
---------------------------------	---

Related Documentation	<ul style="list-style-type: none"> • Tracing ANCP Agent Operations for Subscriber Access on page 553
------------------------------	---

traceoptions (Diameter Base Protocol)

Syntax	<pre>traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i> > <size <i>maximum-file-size</i>> <world-readable no-world-readable>; flag <i>flag</i>; level (all error info notice verbose warning); no-remote-trace; }</pre>
Hierarchy Level	[edit system processes diameter-service]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Define tracing options for Diameter processes.
Options	<p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. Enclose the filename within quotation marks. All files are placed in the directory /var/log.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the size option.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:</p> <ul style="list-style-type: none">• all—Trace all operations• application—Trace Diameter application interface events• configuration—Trace configuration events• daemon—Trace Diameter daemon level events• diameter-instance—Trace Diameter instance events• dne—Trace Diameter network element events• framework—Trace Diameter framework events• memory-management—Trace memory management events• messages—Trace Diameter messages• node—Trace Diameter node events• peer—Trace Diameter peer events <p>level—Level of tracing to perform. You can specify any of the following levels:</p> <ul style="list-style-type: none">• all—Match all levels.• error—Match error conditions.

- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: *sizek* to specify KB, *sizem* to specify MB, or *sizeg* to specify GB

Range: 10240 through 1073741824

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege	trace—To view this statement in the configuration.
Level	trace-control—To add this statement to the configuration.

Related Documentation	<ul style="list-style-type: none">• Tracing Diameter Base Protocol Processes for Subscriber Access on page 543
------------------------------	--

traceoptions (DHCP)

Syntax	<pre>traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i> > <size <i>maximum-file-size</i>> <world-readable no-world-readable>; flag <i>flag</i>; level (all error info notice verbose warning); no-remote-trace; }</pre>
Hierarchy Level	[edit system processes dhcp-service]
Release Information	Statement introduced in Junos OS Release 11.4. Statement introduced in Junos OS Release 12.1 for EX Series switches.
Description	<p>Define global tracing operations for extended DHCP local server and extended DHCP relay agent processes.</p> <p>Replaces deprecated traceoptions statements at the [edit forwarding-options dhcp-relay] and [edit system services dhcp-local-server] hierarchy levels.</p>
Options	<p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the size option.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements:</p> <ul style="list-style-type: none">• all—Trace all events.• auth—Trace authentication events.• database—Trace database events.• fwd—Trace firewall process events.• general—Trace miscellaneous events.• ha—Trace high availability-related events.• interface—Trace interface operations.• io—Trace I/O operations.• liveness-detection—Trace liveness detection operations.• packet—Trace packet and option decoding operations.• performance—Trace performance measurement operations.• profile—Trace profile operations.

- **rpd**—Trace routing protocol process events.
- **rtsock**—Trace routing socket operations.
- **security-persistence**—Trace security persistence events.
- **session-db**—Trace session database events.
- **state**—Trace changes in state.
- **statistics**—Trace baseline statistics.
- **ui**—Trace user interface operations.

level—Level of tracing to perform; also known as severity level. The option you configure enables tracing of events at that level and all higher (more restrictive) levels. You can specify any of the following levels:

- **all**—Match messages of all levels.
- **error**—Match error messages.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages. This is the lowest (least restrictive) severity level; when you configure **verbose**, messages at all higher levels are traced. Therefore, the result is the same as when you configure **all**.
- **warning**—Match warning messages.

Default: error

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access, allowing only the user **root** and users who have the Junos OS **maintenance** permission to access the trace files.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (***maximum-file-sizek***), megabytes (***maximum-file-sizem***), or gigabytes (***maximum-file-sizeg***). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Range: 10,240 through 1,073,741,824

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege	trace—To view this statement in the configuration.
Level	trace-control—To add this statement to the configuration.

- Related Documentation**
- [Tracing Extended DHCP Operations on page 521](#)

traceoptions (General Authentication Service)

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i> > <size <i>maximum-file-size</i>> <world-readable no-world-readable>; filter { user <i>user@domain</i>; } flag <i>flag</i>; no-remote-trace; } </pre>
Hierarchy Level	[edit system processes general-authentication-service]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	Configure tracing options for the general authentication service.
Options	<p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. All files are placed in the directory <code>/var/log</code>.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the size option.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>filter—Additional filter to refine the output to display particular subscribers. Filtering based on the following subscriber identifier simplifies troubleshooting in a scaled environment.</p> <ul style="list-style-type: none"> user <i>user@domain</i>—Username of a subscriber. Optionally use an asterisk (*) as a wildcard to substitute for characters at the beginning or end of either term or both terms. <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:</p> <ul style="list-style-type: none"> address-assignment—Trace address-assignment pool events all—Trace all tracing operations configuration—Trace configuration events framework—Trace authentication framework events gx-plus—Trace Gx-Plus events jsrc—Trace JSRC events ldap—Trace LDAP authentication events local-authentication—Trace local authentication events

- **radius**—Trace RADIUS authentication events
- **user-access**—Trace user access events, such as login, logout, and authenticate.

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: *sizek* to specify KB, *sizem* to specify MB, or *sizeg* to specify GB

Range: 10240 through 1073741824

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level	trace—To view this statement in the configuration. trace-control—To add this statement to the configuration.
---------------------------------	---

Related Documentation	<ul style="list-style-type: none">• Tracing General Authentication Service Processes on page 559
------------------------------	--

traceoptions (PTSP)

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i> > <size <i>maximum-file-size</i>> <world-readable no-world-readable>; flag <i>flag</i> <disable>; no-remote-trace; } </pre>
Hierarchy Level	[edit system services packet-triggered-subscribers]
Release Information	Statement introduced in Junos OS Release 10.2.
Description	Define tracing operations for PTSP.
Options	<p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the size option.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:</p> <ul style="list-style-type: none"> • all—Trace all operations. • configuration—Trace configuration events. • general—Trace general flow. • peer—Trace SRC peer events. • pic—Trace PIC events. • rtsock—Trace routing socket events. • session—Trace session events. <p>disable—Disable this trace flag.</p> <p>match <i>regular-expression</i>—(Optional) Refine the output to include lines that contain the regular expression.</p> <p>no-remote-trace—Disable remote tracing.</p> <p>no-world-readable—(Optional) Disable unrestricted file access.</p> <p>size <i>maximum-file-size</i>—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the files option.</p>

Syntax: *sizek* to specify KB, *sizem* to specify MB, or *sizeg* to specify GB

Range: 10240 through 1073741824

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege	trace—To view this statement in the configuration.
Level	trace-control—To add this statement to the configuration.

Related Documentation	<ul style="list-style-type: none">• Tracing Packet-Triggered Subscriber Operations on page 575
------------------------------	--

traceoptions (Static Subscribers)

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i>> <size <i>maximum-file-size</i>> <world-readable no-world-readable>; flag <i>flag</i>; level (all error info notice verbose warning); no-remote-trace; } </pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> system processes static-subscribers], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system processes static-subscribers], [edit routing-instances <i>routing-instances-name</i> system processes static-subscribers], [edit system processes static-subscribers]</p>
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Define tracing operations for static subscriber processes.
Options	<p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory <code>/var/log</code>.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the size option.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:</p> <ul style="list-style-type: none"> • all—Trace all operations. • authentication—Trace authentication events. • configuration—Trace configuration events. • database—Trace database events. • general—Trace general events. • gres—Trace GRES events. • profile—Trace dynamic profile events. • rtsock—Trace routing socket events. • statistics—Trace statistics events. • subscriber—Trace subscriber events. <p>level—Level of tracing to perform. You can specify any of the following levels:</p> <ul style="list-style-type: none"> • all—Match all levels.

- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

Default: error

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—(Optional) Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: *sizek* to specify KB, *sizem* to specify MB, or *sizeg* to specify GB

Range: 10240 through 1073741824

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege	trace—To view this statement in the configuration.
Level	trace-control—To add this statement to the configuration.

Related Documentation	<ul style="list-style-type: none">• Tracing Static Subscriber Operations on page 571
------------------------------	--

traceoptions (Subscriber Management)

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i> > <size <i>maximum-file-size</i>> <world-readable no-world-readable>; flag <i>flag</i>; } </pre>
Hierarchy Level	[edit system services subscriber-management]
Release Information	Statement introduced in Junos OS Release 11.1.
Description	Define tracing operations for subscriber management interface processes.
Options	<p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. Enclose the filename within quotation marks. All files are placed in the directory <code>/var/log</code>.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the size option.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:</p> <ul style="list-style-type: none"> • all—Trace all operations. • database—Trace database events. • general—Trace general events. • issu—Trace unified ISSU events. • server—Trace server events. • session-db—Trace session database interactions. • ui—Trace user interface events. <p>match <i>regular-expression</i>—(Optional) Refine the output to include lines that contain the regular expression.</p> <p>no-world-readable—(Optional) Disable unrestricted file access.</p> <p>size <i>maximum-file-size</i>—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the files option.</p> <p>Syntax: sizek to specify KB, sizem to specify MB, or sizeg to specify GB</p> <p>Range: 10240 through 1073741824</p> <p>Default: 128 KB</p>

world-readable—(Optional) Enable unrestricted file access.

Required Privilege trace—To view this statement in the configuration.
Level trace-control—To add this statement to the configuration.

Related Documentation • [Tracing Subscriber Management Database Operations for Subscriber Access on page 531](#)

tracoptions (Subscriber Session Database Replication)

Syntax	<pre>tracoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i> > <size <i>maximum-file-size</i>> <world-readable no-world-readable>; flag <i>flag</i>; no-remote-trace; }</pre>
Hierarchy Level	[edit system services database-replication]
Release Information	Statement introduced in Junos OS Release 9.3.
Description	Define tracing operations for subscriber management session database replication processes.
Options	<p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory <code>/var/log</code>.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the size option.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements. You can include the following flags:</p> <ul style="list-style-type: none"> • all—Trace all operations. • database—Trace database events. • general—Trace general flow. • mirror—Trace mirroring events. • replication—Trace database replication events. • server—Trace server events. • session-db—Trace session database interactions. • ui—Trace user interface events. <p>match <i>regular-expression</i>—(Optional) Refine the output to include lines that contain the regular expression.</p> <p>no-remote-trace—Disable remote tracing.</p> <p>no-world-readable—(Optional) Disable unrestricted file access.</p> <p>size <i>maximum-file-size</i>—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to</p>

indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: *sizek* to specify KB, *sizem* to specify MB, or *sizeg* to specify GB

Range: 10240 through 1073741824

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level trace—To view this statement in the configuration.
trace-control—To add this statement to the configuration.

Related Documentation

- [Tracing Subscriber Management Session Database Replication Operations for Subscriber Access on page 535](#)

transport (Diameter Base Protocol)

Syntax

```
transport transport-name {  
    address;  
    logical-system logical-system-name <routing-instance routing-instance-name >;  
    routing-instance routing-instance-name  
}
```

Hierarchy Level [edit [diameter](#)]

Release Information Statement introduced in Junos OS Release 11.2.

Description Configure the Diameter instance and the local IP address for the Diameter local transport connection.

Options *transport-name*—Name of the transport.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- [Configuring Diameter on page 434](#)
- [Configuring the Diameter Transport on page 436](#)

transport (Diameter Peer)

Syntax	<code>transport <i>transport-name</i>;</code>
Hierarchy Level	[edit diameter peer <i>peer-name</i> connect-actively]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	Specify the transport layer connection to be used for establishing active connections to the peer.
Default	The transport is defined in the default logical system and master routing instance.
Options	<i>transport-name</i> —Name of the transport.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Diameter on page 434• Configuring Diameter Peers on page 435

trigger (DHCP Local Server)

Syntax	<pre>trigger { radius-disconnect; }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit system services dhcp-local-server reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.0.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.</p>
Description	<p>Configure behavior in response to a trigger for all DHCP clients or only the DHCP clients serviced by the specified group of interfaces.</p> <p>The remaining statement is explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Dynamic Client Reconfiguration of Extended Local Server Clients on page 244 • Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect on page 247 • radius-disconnect on page 874

trust-option-82

Syntax	trust-option-82;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay overrides],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]</p>
Release Information	<p>Statement introduced in Junos OS Release 8.3.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Enable processing of DHCP client packets that have a gateway IP address (giaddr) of 0 (zero) and contain option 82 information. By default, the DHCP relay agent treats such packets as if they originated at an untrusted source, and drops them without further processing.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Trusting Option 82 Information on page 264 • Overriding the Default DHCP Relay Configuration Settings on page 256

tunnel-profile (Domain Map)

Syntax	tunnel-profile <i>profile-name</i> ;
Hierarchy Level	[edit access domain map <i>domain-map-name</i>]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Tunnel profile that provides definitions for tunnels associated with the domain map.
Options	<i>profile-name</i> —Name of tunnel profile.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Specifying a Tunnel Profile in a Domain Map on page 139• Configuring a Tunnel Profile for Subscriber Access

underlying-interface (ANCP)

Syntax	underlying-interface <i>underlying-interface-name</i> ;
Hierarchy Level	[edit protocols ancp interfaces interface-set <i>interface-set-name</i>]
Release Information	Statement introduced in Junos OS Release 12.2.
Description	Configure the underlying interface on which the VLAN demux interface is running. The VLAN demux interface is the underlying interface for the PPPoE sessions controlled by ANCP.
Options	<i>underlying-interface-name</i> —Name of the underlying interface.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the ANCP Agent on page 368• Associating an Access Node with Subscribers for ANCP Agent Operations on page 370

update-interval

Syntax	update-interval <i>minutes</i> ;
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	Enable interim accounting updates and configure the amount of time that the router or switch waits before sending a new accounting update.
Default	No updates
Options	minutes —Amount of time between updates, in minutes. All values are rounded up to the next higher multiple of 10. For example, the values 811 through 819 are all accepted by the CLI, but are all rounded up to 820. Range: 10 through 1440 minutes
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Authentication and Accounting Parameters for Subscriber Access on page 80

upstream-rate (Traffic Shaping)

Syntax	<code>upstream-rate rate;</code>
Hierarchy Level	<code>[edit dynamic-profiles <i>profile-name</i> interfaces \$junos-interface-ifd-name unit \$junos-interface-unit advisory-options],</code> <code>[edit dynamic-profiles <i>profile-name</i> interfaces interface-set \$junos-interface-set-name interface \$junos-interface-ifd-name advisory-options],</code> <code>[edit interfaces demux0 unit <i>logical-unit-number</i> advisory-options],</code> <code>[edit interfaces <i>interface-name</i> <i>logical-unit-number</i> advisory-options]</code>
Release Information	Statement introduced in Junos OS Release 11.4. Support at the <code>[edit interfaces demux0 ...]</code> hierarchy level introduced in Junos OS Release 12.2. Support at the <code>[edit dynamic-profiles ...]</code> hierarchy level introduced in Junos OS Release 13.1.
Description	<p>Specify a recommended shaping rate to be applied to upstream traffic on an interface.</p> <p>For ANCP interfaces, this configured rate is used as the default value for the Juniper VSA Upstream-Calculated-Qos-Rate (26-142) when the router has not received and processed the attributes from the access node.</p> <p>For L2TP, the rate is configured on an underlying PPPoE logical interface for a subscriber on an MX Series router acting as a LAC. When the subscriber is tunneled, this rate, referred to as speed for L2TP, is sent to the LNS in the ICCN message as AVP 38.</p>
Options	<p>rate—Traffic rate in bits per second.</p> <p>Range: 1000 through 4,294,967,295 bits per second</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Setting a Recommended Shaping Rate for Traffic on ANCP Interfaces on page 400• Configuring the ANCP Agent on page 368• Configuring the Method to Set the LAC Connection Speeds to the LNS

use-interface-description

Syntax	<code>use-interface-description (logical device);</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id relay-agent-remote-id)],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> (relay-agent-interface-id relay-agent-remote-id)],</p> <p>[edit forwarding-options dhcp-relay relay-option-82 (circuit-id remote-id)],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> relay-option-82 (circuit-id remote-id)],</p> <p>[edit logical-systems <i>logical-system-name</i> ... forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id relay-agent-remote-id)],</p> <p>[edit logical-systems <i>logical-system-name</i> ... forwarding-options dhcp-relay ... relay-option-82 (circuit-id remote-id)],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id relay-agent-remote-id)],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ... relay-option-82 (circuit-id remote-id)],</p> <p>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security dhcpv6-options option-18],</p> <p>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security dhcpv6-options option-37]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.6.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.3 for EX Series switches.</p> <p>Support at the [edit ... relay-agent-remote-id] and [edit ... remote-id] hierarchy levels introduced in Junos OS Release 14.1.</p> <p>Support at the [edit vlans <i>vlan-name</i> dhcp-security dhcpv6-options option-18] and [edit vlans <i>vlan-name</i> dhcp-security dhcpv6-options option-37] hierarchy levels introduced in Junos OS Release 14.1X53-D10 for EX Series switches.</p>
Description	Use the textual interface description instead of the interface identifier in the DHCP base option 82 Agent Circuit ID (suboption 1) or Agent Remote ID (suboption 2) information, or in the DHCPv6 option 18 (Relay Agent Interface ID) or option 37 (Relay Agent Remote ID) information in DHCP packets that the DHCP relay agent sends to a DHCP server.



NOTE: For integrated routing and bridging (IRB) interfaces, the option 82 field must be able to uniquely identify the incoming interface based on either the Agent Circuit ID or Agent Remote ID. You can modify the information in the textual interface description to match the raw IFD (physical interface without a subunit) name and configure the option 82 field to use the interface description.

The textual description is configured using the **description** statement at the [edit **interfaces interface-name**] hierarchy level. If you specify that the textual description be used and no description is configured for the interface, DHCP relay defaults to using the Layer 2 interface name. When you use the interface description rather than the interface name,

the interface description has to be specified under interface unit ("set interfaces ge-0/0/0 unit 0 description "client"). If you do not do this, then the interface name is used.

In the case of integrated routing and bridging (IRB) interfaces, the textual description of the Layer 2 interface is used instead of the IRB interface. If there is no description configured, the Layer 2 logical interface name is used. To include the IRB interface description instead of the Layer 2 interface description, configure the **use-interface-description** and the **no-vlan-interface-name** statements. If no description is configured for the IRB interface, DHCP relay defaults to using the IRB interface name.



NOTE: The **use-interface-description** statement is mutually exclusive with the **use-vlan-id** statement.

If you specify the textual interface description, rather than accepting the default syntax, the identification is for packets returned from the server, and only for instances where that identification would be required by the DHCP relay, such as a stateless pass-through.



NOTE: By default, DHCP relay accepts a maximum of 253 ASCII characters. If the textual interface description exceeds 253 characters, DHCP relay drops the packet, which results in the DHCP client failing to bind.

Options **logical**—Use the textual description that is configured for the logical interface.
device—Use the textual description that is configured for the device interface.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Documentation

- [Including a Textual Description in DHCP Options on page 271](#)
- [Using DHCP Relay Agent Option 82 Information on page 266](#)
- [Configuring DHCPv6 Relay Agent Options on page 296](#)

use-option-82

Syntax	use-option-82;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> relay-agent-interface-id],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 ... relay-agent-interface-id],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 ... relay-agent-interface-id],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 ... relay-agent-interface-id]</p>
Release Information	Statement introduced in Junos OS Release 13.2.
Description	Specify that, in dual-stack environments, the DHCPv6 relay agent uses an Interface-ID option (option 18) that is based on the DHCPv4 relay agent information option (option 82). When you include this statement, the DHCPv6 relay agent checks for the option 82 Agent Circuit ID suboption (suboption 1) and inserts it into the outgoing RELAY-FORW message.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using DHCP Relay Agent Option 82 Information on page 266 • Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets on page 297

use-primary (DHCP Relay Agent)

Syntax	<code>use-primary <i>primary-profile-name</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay dhcpv6 dynamic-profile <i>profile-name</i>],</p> <p>[edit forwarding-options dhcp-relay dynamic-profile <i>profile-name</i>],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> dynamic-profile <i>profile-name</i>],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> dynamic-profile <i>profile-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 dynamic-profile <i>profile-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dynamic-profile <i>profile-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> dynamic-profile <i>profile-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> dynamic-profile <i>profile-name</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.3.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	<p>Specify the dynamic profile to configure as the primary dynamic profile. The primary dynamic profile is instantiated when the first subscriber logs in. Subsequent subscribers are not assigned the primary dynamic profile; instead, they are assigned the dynamic profile specified for the interface. When the first subscriber logs out, the next subscriber that logs in is assigned the primary dynamic profile.</p> <p>Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.</p> <p>EX Series switches do not support DHCPv6.</p>
Options	<i>primary-profile-name</i> —Name of the dynamic profile to configure as the primary dynamic profile
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

- Related Documentation**
- *Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*

use-vlan-id

Syntax	<code>use-vlan-id;</code>
For Platforms with Enhanced Layer 2 Software (ELS)	<code>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security option-82 circuit-id]</code>
For Platforms Without ELS	<code>[edit forwarding-options helpers bootp dhcp-option82-circuit-id],</code> <code>[edit forwarding-options helpers bootp interface <i>interface-name</i> dhcp-option82-circuit-id]</code>
For MX Series Platforms	<code>[edit bridge-domains <i>bridge-domain-name</i> forwarding-options dhcp-security option-82 circuit-id]</code>
Release Information	Statement introduced in Junos OS Release 9.3 for EX Series switches.



NOTE: The EX Series switches that support the `use-vlan-id` statement are the EX4300, EX4600, and EX9200 switches.

Statement introduced in Junos OS Release 11.3 for the QFX Series.

Hierarchy level `[edit vlans vlan-name forwarding-options dhcp-security]` introduced in Junos OS Release 13.2X50-D10. (See *Getting Started with Enhanced Layer 2 Software* for information about ELS.)

Hierarchy level `[edit bridge-domains bridge-domain-name forwarding-options dhcp-security]` introduced in Junos OS Release 14.1 for the MX Series.

Description Use the VLAN ID rather than the VLAN name (the default) in the circuit ID or remote ID value in the DHCP option 82 information.



NOTE: The `use-vlan-id` statement is mutually exclusive with the `use-interface-description` and `no-vlan-interface-name` statements.

The `use-vlan-id` statement only applies to interfaces in a bridge domain. The format of the Agent Circuit ID or Agent Remote ID information for Fast Ethernet or Gigabit Ethernet interfaces is as follows:

```
(fe | ge)-fpc/pic/port.subunit:svlan_id-vlan_id
```



NOTE: The *subunit* is required and used to differentiate the interface for remote systems, and *svlan_id-vlan_id* represents the VLANs associated with the bridge domain.

Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Example: Setting Up DHCP Option 82 with a Switch with No Relay Agent Between Clients and a DHCP Server</i>• <i>Example: Setting Up DHCP Option 82 with a Switch as a Relay Agent Between Clients and a DHCP Server</i>• RFC 3046, <i>DHCP Relay Agent Information Option</i>, at http://tools.ietf.org/html/rfc3046

user-prefix (DHCP Relay Agent)

Syntax	<code>user-prefix <i>user-prefix-string</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay authentication username-include],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p>
Description	Specify the user prefix that is concatenated with the username during the subscriber authentication or client authentication process. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.
Options	<i>user-prefix-string</i> —User prefix string.
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using External AAA Authentication Services with DHCP on page 217

user-prefix (Static Subscribers)

Syntax	<code>user-prefix <i>user-prefix-string</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers authentication username-include],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication username-include],</p> <p>[edit system services static-subscribers authentication username-include],</p> <p>[edit system services static-subscribers group <i>group-name</i> authentication username-include]</p>
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Specify that a string is included as the beginning of the username created for all static subscribers or for the static subscribers in a specified group. The group version of the statement takes precedence over the global version. The username is also sent to RADIUS in the Access-Request message.
Options	<i>user-prefix-string</i> —String that begins the username. The string can include the following characters: a through z, A through Z, 0 through 9, "-", or ".".
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Subscribers over Static Interfaces on page 466 • Configuring the Static Subscriber Global Username on page 473 • Configuring the Static Subscriber Group Username on page 478

user-prefix (DHCP Local Server)

Syntax	<code>user-prefix <i>user-prefix-string</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server group group-name authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify the user prefix that is concatenated with the username during the subscriber authentication or DHCP client authentication process.
Options	<i>user-prefix-string</i> —User prefix string.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

- Related Documentation**
- [Using External AAA Authentication Services with DHCP on page 217](#)

username-include (Static Subscribers)

Syntax	<pre>username-include { domain-name domain-name; interface; logical-system-name; routing-instance-name; user-prefix user-prefix-string; }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> system services static-subscribers group <i>group-name</i> authentication],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers authentication],</p> <p>[edit routing-instances <i>routing-instances-name</i> system services static-subscribers group <i>group-name</i> authentication],</p> <p>[edit system services static-subscribers authentication],</p> <p>[edit system services static-subscribers group <i>group-name</i> authentication]</p>
Release Information	Statement introduced in Junos OS Release 9.6.
Description	<p>Specify the information included in the username created for all static subscribers or for static subscribers in a specified group. The group version of the statement takes precedence over the global version. The username is also sent to RADIUS in the Access-Request message.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Subscribers over Static Interfaces on page 466 • Configuring the Static Subscriber Global Username on page 473 • Configuring the Static Subscriber Group Username on page 478

username-include (DHCP Local Server)

Syntax	<pre>username-include { circuit-type; client-id; delimiter <i>delimiter-character</i>; domain-name <i>domain-name-string</i>; interface-name; logical-system-name; mac-address; option-60; option-82 <circuit-id> <remote-id>; relay-agent-interface-id; relay-agent-remote-id; relay-agent-subscriber-id; routing-instance-name; user-prefix <i>user-prefix-string</i>; }</pre>
Hierarchy Level	<p>[edit system services dhcp-local-server authentication], [edit system services dhcp-local-server dhcpv6 authentication], [edit system services dhcp-local-server dhcpv6 group group-name authentication], [edit system services dhcp-local-server group group-name authentication], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server ...], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	<p>Configure the username that the router or switch passes to the external AAA server. You must include at least one of the optional statements for the username to be valid. If you do not configure a username, the router (or switch) accesses the local authentication service only and does not use external authentication services, such as RADIUS.</p> <p>The statements are explained separately. The option-60 and option-82 statements are not supported in the DHCPv6 hierarchy levels. The client-id, relay-agent-interface-id, relay-agent-remote-id and relay-agent-subscriber-id statements are supported in the DHCPv6 hierarchy levels only.</p>
Required Privilege Level	<p>system—To view this statement in the configuration. system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using External AAA Authentication Services with DHCP on page 217 • Creating Unique Usernames for DHCP Clients on page 218

username-include (DHCP Relay Agent)

Syntax `username-include {
 circuit-type;
 client-id;
 delimiter delimiter-character;
 domain-name domain-name-string;
 interface-name;
 logical-system-name;
 mac-address;
 option-60;
 option-82 <circuit-id> <remote-id>;
 relay-agent-interface-id;
 relay-agent-remote-id;
 relay-agent-subscriber-id;
 routing-instance-name;
 user-prefix user-prefix-string;
 }`

Hierarchy Level [edit forwarding-options dhcp-relay [authentication](#)],
 [edit forwarding-options dhcp-relay dhcpv6 [authentication](#)],
 [edit forwarding-options dhcp-relay dhcpv6 group *group-name* [authentication](#)],
 [edit forwarding-options dhcp-relay group *group-name* [authentication](#)],
 [edit logical-systems *logical-system-name* forwarding-options dhcp-relay ...],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*
 forwarding-options dhcp-relay ...],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay ...]

Release Information Statement introduced in Junos OS Release 9.1.
 Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
 Support at the [edit ... [dhcpv6](#)] hierarchy levels introduced in Junos OS Release 11.4.

Description Configure the username that the router (or switch) passes to the external AAA server. You must include at least one of the optional statements for the username to be valid. If you do not configure a username, the router (or switch) accesses the local authentication service only and does not use external authentication services, such as RADIUS. Use the statement at the [edit...[dhcpv6](#)] hierarchy levels to configure DHCPv6 support.

The following statements are not supported in the DHCPv6 hierarchy levels:

- `mac-address`
- `option-60`
- `option-82`

The following statements are supported in the DHCPv6 hierarchy levels only:

- `relay-agent-interface-id`
- `relay-agent-remote-id`
- `relay-agent-subscriber-id`

The remaining statements are explained separately.

Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Creating Unique Usernames for DHCP Clients on page 218• Using External AAA Authentication Services with DHCP on page 217

valid-lifetime (Dynamic Router Advertisement)

Syntax	<code>valid-lifetime <i>seconds</i>;</code>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> protocols router-advertisement interface <i>interface-name</i> prefix <i>prefix</i>]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	Specify how long the prefix remains valid for onlink determination.
Options	<i>seconds</i> —Valid lifetime, in seconds. If you set the valid lifetime to 0xffffffff , the lifetime is infinite. Default: 2,592,000 seconds
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>preferred-lifetime</i>• <i>Example: Configuring IPv6 Interfaces and Enabling Neighbor Discovery</i>

valid-lifetime (Address-Assignment Pools)

Syntax	<code>valid-lifetime <i>seconds</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet6 dhcp-attributes]
Release Information	Statement introduced in Junos OS Release 13.3.
Description	<p>Specify the length of time, in seconds, that the DHCPv6 server keeps the IPv6 prefix valid. When the lifetime expires, the address becomes invalid.</p> <p>If the preferred-lifetime is also configured, the valid-lifetime must be greater than the preferred-lifetime. The valid-lifetime and the maximum-lease-time are mutually exclusive and cannot both be configured.</p>
Options	<p>seconds—Number of seconds that the IPv6 prefix is valid.</p> <p>Range: 30 through 4,294,967,295 seconds</p> <p>Default: 86,400 (24 hours)</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Address-Assignment Pools on page 316 • DHCP Attributes for Address-Assignment Pools on page 201 • maximum-lease-time on page 800 • preferred-lifetime (Address-Assignment Pools) on page 853

violation-action (DHCP Local Server and DHCP Relay Agent)

Syntax	<code>violation-action <i>action</i>;</code>
Hierarchy Level	<code>[edit forwarding-options dhcp-relay lease-time-validation],</code> <code>[edit forwarding-options dhcp-relay dhcpv6 lease-time-validation],</code> <code>[edit forwarding-options dhcp-relay group <i>group-name</i> lease-time-validation],</code> <code>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> lease-time-validation],</code> <code>[edit logical-systems <i>logical-system-name</i> ...],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>...],</code> <code>[edit routing-instances <i>routing-instance-name</i> ...],</code> <code>[edit system services dhcp-local-server lease-time-validation],</code> <code>[edit system services dhcp-local-server dhcpv6 lease-time-validation],</code> <code>[edit system services dhcp-local-server group <i>group-name</i> lease-time-validation],</code> <code>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> lease-time-validation]</code>
Release Information	Statement introduced in Junos OS Release 14.1.
Description	Configure the action that the router performs when a DHCP lease-time violation occurs. The violation occurs when a third-party DHCP server or address-assignment pool offers a DHCP lease time that is less than the threshold specified by the lease-time-threshold statement.
Options	<i>action</i> —Action taken by the router when a lease-time violation occurs. <ul style="list-style-type: none">• drop—(Optional) For DHCPv4 and DHCPv6 relay agent, the third-party lease is dropped and the client binding fails.• override-lease—(Optional) For DHCPv4 and DHCPv6 local server, the third-party lease is overridden with the value specified by the lease-time-threshold statement and binds the client using the new value.• strict—(Optional) For DHCPv4 and DHCPv6 local server, DHCP ignores the third-party lease and the client binding fails.
Required Privilege Level	system —To view this statement in the configuration. system-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring a DHCP Lease-Time Threshold on page 209

vlan-nas-port-stacked-format

Syntax	vlan-nas-port-stacked-format;
Hierarchy Level	[edit access profile <i>profile-name</i> radius options]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 9.1 for EX Series switches.
Description	Configure RADIUS attribute 5 (NAS-Port) to include the S-VLAN ID, in addition to the VLAN ID, for subscribers on Ethernet interfaces.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring RADIUS Server Options for Subscriber Access on page 102• Configuring Authentication and Accounting Parameters for Subscriber Access on page 80

vlan-ranges (RADIUS Options)

Syntax	<code>vlan-ranges (any <i>low-tag-high-tag</i>);</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> radius-options nas-port-options <i>nas-port-options-name</i>]
Release Information	Statement introduced in Junos OS Release 12.3.
Description	Configure the VLAN range of subscribers to which the named NAS-Port options definition applies.



NOTE: You can configure a maximum of 16 NAS-Port options definitions per physical interface. Each definition can include a maximum of 32 VLAN ranges or 32 S-VLAN ranges, but cannot include a combination of VLAN ranges and S-VLAN ranges.

Options	<p>any—Entire VLAN range representing all VLAN IDs.</p> <p><i>low-tag</i>—VLAN ID tag representing the lower limit of the VLAN range. Range: 1 through 4094</p> <p><i>high-tag</i>—VLAN ID tag representing the upper limit of the VLAN range. Range: 1 through 4094</p>
----------------	---



NOTE: To specify a single VLAN ID, set *low-tag* and *high-tag* to the same value.

Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 63 • Guidelines for Configuring RADIUS NAS-Port Options for Subscriber Access per Physical Interface, VLAN, or Stacked VLAN on page 62

vrf-name (Duplicate Accounting)

Syntax	<code>vrf-name <i>vrf-name</i>;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> accounting duplication-vrf]
Release Information	Statement introduced in Junos OS Release 12.3R3 and supported in later 12.3Rx releases. Statement supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)
Description	Specify a nondefault VRF (LS:RI combination) to which duplicate accounting information is sent. Up to five access profiles can be defined in this VRF; the profiles point to the RADIUS accounting servers that receive the accounting information.
Options	<i>vrf-name</i> —Name of a nondefault VRF to receive duplicate accounting reports.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Understanding RADIUS Accounting Duplicate Reporting on page 87 • Configuring Authentication and Accounting Parameters for Subscriber Access on page 80

wait-for-acct-on-ack (Access Profile)

Syntax	<code>wait-for-acct-on-ack;</code>
Hierarchy Level	[edit access profile <i>profile-name</i> accounting]
Release Information	Statement introduced in Junos OS Release 12.3. Statement introduced in Junos OS Release 13.2X50-D10 for EX Series switches.
Description	Configure the router's authd process to wait for an Acct-On-Ack response message from RADIUS before sending new authentication and accounting updates to the RADIUS server. This configuration ensures that when a new subscriber session starts, the authentication and accounting information for the new session does not get deleted when RADIUS clears previously existing session state information.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring RADIUS Server Parameters for Subscriber Access on page 102 • Configuring Per-Subscriber Session Accounting on page 92

wins-server (Access)

Syntax	<code>wins-server { <code>ipv4-address</code>; }</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet dhcp-attributes]
Release Information	Statement introduced in Junos OS Release 9.0.
Description	Specify one or more NetBIOS name servers (NBNS) that the client uses to resolve NetBIOS names. This is equivalent to DHCP option 44.
Options	<i>ipv4-address</i> —IP address of each NetBIOS name server; add them to the configuration in order of preference.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring Address-Assignment Pools on page 316

CHAPTER 79

Operational Commands

- clear ancp neighbor
- clear ancp statistics
- clear ancp subscriber
- clear dhcp relay binding
- clear dhcp relay statistics
- clear dhcpv6 relay binding
- clear dhcpv6 relay statistics
- clear dhcp server binding
- clear dhcp server statistics
- clear dhcpv6 server binding
- clear dhcpv6 server statistics
- clear diameter function statistics
- clear diameter peer
- clear ipv6 router-advertisement
- clear network-access aaa statistics
- clear network-access aaa subscriber
- clear network-access gx-plus replay
- clear network-access gx-plus statistics
- clear request services subscribers
- clear services subscriber sessions
- request ancp oam interface
- request ancp oam neighbor
- request dhcp server reconfigure
- request dhcpv6 server reconfigure
- request network-access aaa subscriber set session-id
- request services static-subscribers login group
- request services static-subscribers logout group
- request services static-subscribers login interface

- request services static-subscribers logout interface
- request system reboot
- set request services subscribers
- show accounting pending-accounting-stops
- show ancp cos
- show ancp neighbor
- show ancp statistics
- show ancp subscriber
- show ancp summary
- show ancp summary neighbor
- show ancp summary subscriber
- show database-replication statistics
- show database-replication summary
- show network-access aaa accounting
- show dhcp relay binding
- show dhcp relay statistics
- show dhcp server binding
- show dhcp server statistics
- show dhcpv6 relay binding
- show dhcpv6 relay statistics
- show dhcpv6 server binding
- show dhcpv6 server statistics
- show diameter
- show diameter function
- show diameter function statistics
- show diameter instance
- show diameter network-element
- show diameter network-element map
- show diameter peer
- show diameter peer map
- show diameter peer statistics
- show diameter route
- show ipv6 router-advertisement
- show network-access aaa accounting
- show network-access aaa radius-servers
- show network-access aaa statistics
- show network-access aaa statistics authentication

- `show network-access aaa statistics pending-accounting-stops`
- `show network-access aaa statistics preauthentication`
- `show network-access aaa subscribers`
- `show network-access aaa subscribers session-id`
- `show network-access aaa terminate-code`
- `show network-access address-assignment pool`
- `show network-access domain-map`
- `show network-access gx-plus`
- `show route extensive`
- `show services subscriber bandwidth`
- `show services subscriber dynamic-policies`
- `show services subscriber flows`
- `show services subscriber sessions`
- `show services subscriber statistics`
- `show static-subscribers sessions`
- `show subscribers`
- `show subscribers summary`
- `show system subscriber-management summary`
- `test aaa authd-lite user`
- `test aaa dhcp user`
- `test aaa ppp user`

clear ancp neighbor

Syntax	clear ancp neighbor <ip-address <i>ip-address</i>> <system-name <i>mac-address</i>>
Release Information	Command introduced in Junos OS Release 9.4.
Description	Clear the ANCP agent connection with all ANCP neighbors or with the specified ANCP neighbor. This command deletes information for subscribers associated with the neighbor, causing the adjusted traffic rates to revert to the configured rate for the subscriber interfaces. The neighbor remains configured (its administrative state is <i>enabled</i>) and can reestablish adjacencies.
Options	none —Clear all ANCP neighbors. ip-address <i>ip-address</i> —(Optional) Clear the ANCP neighbor specified by the IP address. system-name <i>mac-address</i> —(Optional) Clear the ANCP neighbor specified by the MAC address.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show ancp neighbor on page 1058
List of Sample Output	clear ancp neighbor on page 1000 show ancp neighbor on page 1000
Output Fields	When you enter this command, you are provided no feedback on the status of your request. You can enter the show ancp neighbor command before and after clearing the ANCP neighbors to verify the clear operation.

Sample Output

clear ancp neighbor

```
user@host> clear ancp neighbor
```

show ancp neighbor

The following sample output displays the connections with ANCP neighbors before and after the **clear ancp neighbor** command was issued.

```
user@host> show ancp neighbor
```

IP Address	MAC Address	State	Subscriber Count	Capabilities
10.10.10.2	ba:ad:be:ef:10:10	Established	5	Topo
12.12.12.2	ba:ad:be:ef:10:12	Established	5	Topo
13.13.13.2	ba:ad:be:ef:10:13	Established	5	Topo

14.14.14.2	ba:ad:be:ef:10:14	Established	5	Topo
------------	-------------------	-------------	---	------

```
user@host> clear ancp neighbor ip-address 10.10.10.2
```

```
user@host> show ancp neighbor
```

IP Address	MAC Address	State	Subscriber Count	Capabilities
12.12.12.2	ba:ad:be:ef:10:12	Established	5	Topo
13.13.13.2	ba:ad:be:ef:10:13	Established	5	Topo
14.14.14.2	ba:ad:be:ef:10:14	Established	5	Topo

clear ancp statistics

Syntax	clear ancp statistics <ip-address <i>ip-address</i>> <system-name <i>mac-address</i>>
Release Information	Command introduced in Junos OS Release 13.3.
Description	Clear current statistics accumulated by the ANCP agent for all ANCP neighbors or the specified neighbor.
Options	none —Clear all ANCP statistics. ip-address <i>ip-address</i> —(Optional) Clear statistics for the ANCP neighbor specified by the IP address. system-name <i>mac-address</i> —(Optional) Clear statistics for the ANCP neighbor specified by the MAC address.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show ancp neighbor on page 1058
List of Sample Output	clear ancp statistics on page 1002 show ancp neighbor on page 1002
Output Fields	When you enter this command, you are provided no feedback on the status of your request. You can enter the show ancp neighbor command before and after clearing the ANCP neighbor statistics to verify the clear operation.

Sample Output

clear ancp statistics

```
user@host> clear ancp statistics
```

show ancp neighbor

The following sample output displays statistics for an ANCP neighbor before and after the **clear ancp statistics** command was issued.

```
user@host> show ancp neighbor ip-address 192.168.10.1 detail
Neighbor Information
  IP Address           : 192.168.10.1
  System Name          : 00:00:64:1b:01:02
  Up Time               : 38
  TCP Port              : 64959
  State                 : Established
  Subscriber Count      : 7
  Capabilities          : Topology Discovery
  System Instance       : 11
```

```

Peer Instance                : 1
Adjacency Timer (in 100ms)   : 50
Peer Adjacency Timer (in 100ms) : 100
Partition Type               : 0
Partition Flag               : 1
Partition Identifier         : 0
Dead Timer                   : 22
Received Syn Count           : 47
Received Synack Count        : 48
Received Rstack Count        : 2
Received Ack Count           : 12
Received Port Up Count       : 8
Received Port Down Count     : 2
Received Other Count         : 0
Sent Syn Count               : 48
Sent Synack Count            : 47
Sent Rstack Count            : 1
Sent Ack Count               : 12
Max Discovery Limit Exceed Count : 0

```

```
user@host> clear ancp statistics ip-address 192.168.10.1
```

```
user@host> show ancp neighbor ip-address 192.168.10.1 detail
```

Neighbor Information

```

IP Address                  : 192.168.10.1
System Name                 : 00:00:64:1b:01:02
Up Time                     : 38
TCP Port                    : 64959
State                       : Established
Subscriber Count            : 7
Capabilities                 : Topology Discovery
System Instance             : 11
Peer Instance               : 1
Adjacency Timer (in 100ms)  : 50
Peer Adjacency Timer (in 100ms) : 100
Partition Type              : 0
Partition Flag              : 1
Partition Identifier         : 0
Dead Timer                  : 22
Received Syn Count          : 0
Received Synack Count       : 0
Received Rstack Count       : 0
Received Ack Count          : 0
Received Port Up Count      : 0
Received Port Down Count    : 0
Received Other Count        : 0
Sent Syn Count              : 0
Sent Synack Count           : 0
Sent Rstack Count           : 0
Sent Ack Count              : 0
Max Discovery Limit Exceed Count : 0

```

clear ancp subscriber

Syntax	<pre>clear ancp subscriber <identifier <i>identifier-string</i>> <ip-address <i>ip-address</i>> system-name <i>mac-address</i>></pre>
Release Information	Command introduced in Junos OS Release 11.4.
Description	Clear the ANCP agent connection with all ANCP subscribers or with the specified ANCP subscriber. This command deletes information for the subscribers, causing the adjusted traffic rate to revert to the configured rate for the subscriber interface, but otherwise has no affect on ANCP neighbors.
Options	<p>none—Clear all ANCP subscribers.</p> <p>identifier <i>identifier-string</i>—(Optional) Clear the ANCP subscriber identified by the access loop ID.</p> <p>ip-address <i>ip-address</i>—(Optional) Clear all ANCP subscribers on the neighbor specified by the IP address.</p> <p>system-name <i>mac-address</i>—(Optional) Clear all ANCP subscribers on the neighbor specified by the MAC address.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> show ancp subscriber on page 1071
List of Sample Output	show ancp subscriber brief on page 1004 clear ancp subscriber on page 1005
Output Fields	When you enter this command, you are provided no feedback on the status of your request. You can enter the show ancp subscriber command before and after clearing the ANCP neighbors to verify the clear operation.

Sample Output

show ancp subscriber brief

```
user@host> show ancp subscriber brief
Loop Identifier      Type      Interface      Rate      Neighbor
                    Kbps
port-1-10            VDSL2     set-ge-10410   64         10.10.10.2
port-1-11            VDSL2     set-ge-10411   64         11.11.11.2
port-2-10            VDSL2     ge-1/0/4.12    64         10.12.12.2
port-2-10            VDSL2     ge-1/0/4.12    64         10.12.12.3
port-2-11            VDSL2     ge-1/0/4.13    64         10.13.13.2

user@host> clear ancp subscriber identifier port-2-10
```



```
user@host> show ancp subscriber brief
```

Loop Identifier	Type	Interface	Rate Kbps	Neighbor
port-1-10	VDSL2	set-ge-10410	64	10.10.10.2
port-1-11	VDSL2	set-ge-10411	64	11.11.11.2
port-2-11	VDSL2	ge-1/0/4.13	64	10.13.13.2

`clear ancp subscriber`

```
user@host> clear ancp subscriber
```

clear dhcp relay binding

Syntax	clear dhcp relay binding <address> <all> <interface <i>interface-name</i>> <interfaces-vlan> <interfaces-wildcard> <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>>
Release Information	Command introduced in Junos OS Release 8.3. Options all and interface added in Junos OS Release 8.4. Options interfaces-vlan and interfaces-wildcard added in Junos OS Release 12.1. Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Routers.
Description	Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the client table.
Options	<p>address—(Optional) Clear the binding state for the DHCP client, using one of the following entries:</p> <ul style="list-style-type: none">• ip-address—The specified IP address.• mac-address—The specified MAC address.• session-id—The specified session ID. <p>all—(Optional) Clear the binding state for all DHCP clients.</p> <p>interface <i>interface-name</i>—(Optional) Clear the binding state for DHCP clients on the specified interface.</p> <p>interfaces-vlan—(Optional) Clear the binding state on the interface VLAN ID and S-VLAN ID.</p> <p>interfaces-wildcard—(Optional) The set of interfaces on which to clear bindings. This option supports the use of the wildcard character (*).</p> <p>logical-system <i>logical-system-name</i>—(Optional) Clear the binding state for DHCP clients on the specified logical system.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Clear the binding state for DHCP clients on the specified routing instance.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• Clearing DHCP Bindings for Subscriber Access on page 308• show dhcp relay binding on page 1086

List of Sample Output [clear dhcp relay binding on page 1007](#)
[clear dhcp relay binding all on page 1007](#)
[clear dhcp relay binding interface on page 1007](#)
[clear dhcp relay binding <interfaces-vlan> on page 1007](#)
[clear dhcp relay binding <interfaces-wildcard> on page 1007](#)

Output Fields See [show dhcp relay binding](#) for an explanation of output fields.

Sample Output

clear dhcp relay binding

The following sample output displays the address bindings in the DHCP client table before and after the **clear dhcp relay binding** command is issued.

```
user@host> show dhcp relay binding
IP address      Hardware address  Type    Lease expires at
100.20.32.1     90:00:00:01:00:01 active    2007-02-08 16:41:17 EST
192.168.14.8    90:00:01:01:02:01 active    2007-02-10 10:01:06 EST
```

```
user@host> clear dhcp relay binding 100.20.32.1
```

```
user@host> show dhcp relay binding
IP address      Hardware address  Type    Lease expires at
192.168.14.8    90:00:01:01:02:01 active    2007-02-10 10:01:06 EST
```

clear dhcp relay binding all

The following command clears all DHCP relay agent bindings:

```
user@host> clear dhcp relay binding all
```

clear dhcp relay binding interface

The following command clears DHCP relay agent bindings on a specific interface:

```
user@host> clear dhcp relay binding interface fe-0/0/3
```

clear dhcp relay binding <interfaces-vlan>

The following command uses the *interfaces-vlan* option to clear all DHCP relay agent bindings on top of the underlying interface **ae0**, which clears DHCP bindings on all demux VLANs on top of **ae0**:

```
user@host> clear dhcp relay binding interface ae0
```

clear dhcp relay binding <interfaces-wildcard>

The following command uses the *interfaces-wildcard* option to clear all DHCP relay agent bindings over a specific interface:

```
user@host> clear dhcp relay binding ge-1/0/0.*
```

clear dhcp relay statistics

Syntax	<code>clear dhcp relay statistics</code> <code><logical-system <i>logical-system-name</i>></code> <code><routing-instance <i>routing-instance-name</i>></code>
Syntax	Syntax for EX Series switches: <code>show dhcp relay statistics</code> <code><routing-instance <i>routing-instance-name</i>></code>
Release Information	Command introduced in Junos OS Release 8.3. Statement introduced in Junos OS Release 12.1 for EX Series switches. Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Routers.
Description	Clear all Dynamic Host Configuration Protocol (DHCP) relay statistics.
Options	<code>logical-system <i>logical-system-name</i></code> —(On routers only) (Optional) Perform this operation on the specified logical system. If you do not specify a logical system name, statistics are cleared for the default logical system. <code>routing-instance <i>routing-instance-name</i></code> —(Optional) Perform this operation on the specified routing instance. If you do not specify a routing instance name, statistics are cleared for the default routing instance.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show dhcp relay statistics on page 1091
List of Sample Output	clear dhcp relay statistics on page 1009
Output Fields	Table 58 on page 1009 lists the output fields for the <code>clear dhcp relay statistics</code> command.

Table 58: clear dhcp relay statistics Output Fields

Field Name	Field Description
Packets dropped	<p>Number of packets discarded by the extended DHCP relay agent application due to errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.</p> <ul style="list-style-type: none"> • Total—Total number of packets discarded by the extended DHCP relay agent application. • Bad hardware address—Number of packets discarded because an invalid hardware address was specified. • Bad opcode—Number of packets discarded because an invalid operation code was specified. • Bad options—Number of packets discarded because invalid options were specified. • Invalid server address—Number of packets discarded because an invalid server address was specified. • Lease Time Violation—Number of packets discarded because of a lease time violation • No available addresses—Number of packets discarded because there were no addresses available for assignment. • No interface match—Number of packets discarded because they did not belong to a configured interface. • No routing instance match—Number of packets discarded because they did not belong to a configured routing instance. • No valid local address—Number of packets discarded because there was no valid local address. • Packet too short—Number of packets discarded because they were too short. • Read error—Number of packets discarded because of a system read error. • Send error—Number of packets that the extended DHCP relay application could not send. • Option 60—Number of packets discarded containing DHCP option 60 vendor-specific information. • Option 82—Number of packets discarded because DHCP option 82 information could not be added.
Messages received	<p>Number of DHCP messages received.</p> <ul style="list-style-type: none"> • BOOTREQUEST—Number of BOOTP protocol data units (PDUs) received • DHCPDECLINE—Number of DHCP PDUs of type DECLINE received • DHCPDISCOVER—Number of DHCP PDUs of type DISCOVER received • DHCPINFORM—Number of DHCP PDUs of type INFORM received • DHCPRELEASE—Number of DHCP PDUs of type RELEASE received • DHCPREQUEST—Number of DHCP PDUs of type REQUEST received
Messages sent	<p>Number of DHCP messages sent.</p> <ul style="list-style-type: none"> • BOOTREPLY—Number of BOOTP PDUs transmitted • DHCPOFFER—Number of DHCP OFFER PDUs transmitted • DHCPACK—Number of DHCP ACK PDUs transmitted • DHC PNACK—Number of DHCP NACK PDUs transmitted

Sample Output

clear dhcp relay statistics

The following sample output displays the DHCP relay statistics before and after the **clear dhcp relay statistics** command is issued.

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

```
Packets dropped:
  Total          1
  Lease Time Violated 1

Messages received:
  BOOTREQUEST    116
  DHCPDECLINE    0
  DHCPDISCOVER   11
  DHCPINFORM     0
  DHCPRELEASE    0
  DHCPREQUEST    105

Messages sent:
  BOOTREPLY      44
  DHCPOFFER      11
  DHCPACK        11
  DHCPNAK        11
```

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

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

```
Packets dropped:
  Total          0

Messages received:
  BOOTREQUEST    0
  DHCPDECLINE    0
  DHCPDISCOVER   0
  DHCPINFORM     0
  DHCPRELEASE    0
  DHCPREQUEST    0

Messages sent:
  BOOTREPLY      0
  DHCPOFFER      0
  DHCPACK        0
  DHCPNAK        0
```

clear dhcpv6 relay binding

Syntax	<pre>clear dhcpv6 relay binding <address> <all> <interface interface-name> <interfaces-vlan> <interfaces-wildcard> <logical-system logical-system-name> <routing-instance routing-instance-name></pre>
Release Information	<p>Command introduced in Junos OS Release 11.4.</p> <p>Command introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Options <i>interfaces-vlan</i> and <i>interfaces-wildcard</i> added in Junos OS Release 12.1.</p> <p>Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Routers.</p>
Description	Clear the binding state of Dynamic Host Configuration Protocol for IPv6 (DHCPv6) clients from the client table.
Options	<p>address—(Optional) Clear the binding state for the DHCPv6 client, using one of the following entries:</p> <ul style="list-style-type: none"> • <i>CID</i>—The specified Client ID (CID). • <i>ipv6-prefix</i>—The specified IPv6 prefix. • <i>session-id</i>—The specified session ID. <p>all—(Optional) Clear the binding state for all DHCPv6 clients.</p> <p>interfaces-vlan—(Optional) Clear the binding state on the interface VLAN ID and S-VLAN ID.</p> <p>interfaces-wildcard—(Optional) The set of interfaces on which to clear bindings. This option supports the use of the wildcard character (*).</p> <p>interface interface-name—(Optional) Clear the binding state for DHCPv6 clients on the specified interface.</p> <p>logical-system logical-system-name—(Optional) Clear the binding state for DHCPv6 clients on the specified logical system.</p> <p>routing-instance routing-instance-name—(Optional) Clear the binding state for DHCPv6 clients on the specified routing instance.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Clearing DHCP Bindings for Subscriber Access on page 308 • show dhcpv6 relay binding on page 1102

- List of Sample Output**
- [clear dhcpv6 relay binding on page 1012](#)
 - [clear dhcpv6 relay binding <prefix> on page 1012](#)
 - [clear dhcpv6 relay binding all on page 1012](#)
 - [clear dhc6p relay binding interface on page 1012](#)
 - [clear dhcpv6 relay binding <interfaces-vlan> on page 1013](#)
 - [clear dhcpv6 relay binding <interfaces-wildcard> on page 1013](#)
- Output Fields** See [show dhcpv6 relay binding](#) for an explanation of output fields.

Sample Output

clear dhcpv6 relay binding

The following sample output displays the DHCPv6 bindings before and after the **clear dhcpv6 relay binding** command is issued.

```
user@host> show dhcpv6 relay binding
```

Prefix	Session Id	Expires	State	Interface	Client DUID
2001:bd8:3c4d:15::/64	1	83720	BOUND	ge-1/0/0.0	
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01					
2001:bd8:3c4d:16::/64	2	83720	BOUND	ge-1/0/0.0	
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:02					
2001:bd8:3c4d:17::/64	3	83720	BOUND	ge-1/0/0.0	
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:03					
2001:bd8:3c4d:18::/64	4	83720	BOUND	ge-1/0/0.0	
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:04					
2001:bd8:3c4d:19::/64	5	83720	BOUND	ge-1/0/0.0	
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:05					
2001:bd8:3c4d:20::/64	6	83720	BOUND	ge-1/0/0.0	
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:06					

clear dhcpv6 relay binding <prefix>

```
user@host> clear dhcpv6 relay binding 2001:bd8:3c4d:15::/64
```

```
user@host> show dhcpv6 relay binding
```

Prefix	Session Id	Expires	State	Interface	Client DUID
2001:bd8:3c4d:16::/64	2	83720	BOUND	ge-1/0/0.0	
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:02					
2001:bd8:3c4d:17::/64	3	83720	BOUND	ge-1/0/0.0	
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:03					
2001:bd8:3c4d:18::/64	4	83720	BOUND	ge-1/0/0.0	
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:04					
2001:bd8:3c4d:19::/64	5	83720	BOUND	ge-1/0/0.0	
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:05					
2001:bd8:3c4d:20::/64	6	83720	BOUND	ge-1/0/0.0	
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:06					

clear dhcpv6 relay binding all

The following command clears all DHCP relay agent bindings:

```
user@host> clear dhcpv6 relay binding all
```

clear dhc6p relay binding interface

The following command clears DHCPv6 relay agent bindings on a specific interface:


```
user@host> clear dhcpv6 relay binding interface fe-0/0/2
```

clear dhcpv6 relay binding <interfaces-vlan>

The following command uses the *interfaces-vlan* option to clear all DHCPv6 relay agent bindings on top of the underlying interface **ae0**, which clears DHCPv6 bindings on all demux VLANs on top of **ae0**:

```
user@host> clear dhcpv6 relay binding interface ae0
```

clear dhcpv6 relay binding <interfaces-wildcard>

The following command uses the *interfaces-wildcard* option to clear all DHCPv6 relay agent bindings over a specific interface:

```
user@host> clear dhcpv6 relay binding ge-1/0/0.*
```

clear dhcpv6 relay statistics

Syntax	clear dhcpv6 relay statistics <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>>
Release Information	Command introduced in Junos OS Release 11.4. Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Routers.
Description	Clear all Dynamic Host Configuration Protocol for IPv6 (DHCPv6) relay statistics.
Options	logical-system <i>logical-system-name</i> —(Optional) Perform this operation on the specified logical system. If you do not specify a logical system name, statistics are cleared for the default logical system. routing-instance <i>routing-instance-name</i> —(Optional) Perform this operation on the specified routing instance. If you do not specify a routing instance name, statistics are cleared for the default routing instance.
Required Privilege Level	view
List of Sample Output	clear dhcpv6 relay statistics on page 1014
Output Fields	See show dhcpv6 relay statistics for an explanation of output fields.

Sample Output

clear dhcpv6 relay statistics

The following sample output displays the DHCPv6 relay statistics before and after the **clear dhcpv6 relay statistics** command is issued.

```
user@host> show dhcpv6 relay statistics
DHCPv6 Packets dropped:
    Total                0
    Lease Time Violated  1

Messages received:
    DHCPV6_DECLINE        0
    DHCPV6_SOLICIT        10
    DHCPV6_INFORMATION_REQUEST  0
    DHCPV6_RELEASE        0
    DHCPV6_REQUEST        10
    DHCPV6_CONFIRM        0
    DHCPV6_RENEW          0
    DHCPV6_REBIND         0
    DHCPV6_RELAY_REPL     0

Messages sent:
    DHCPV6_ADVERTISE      0
    DHCPV6_REPLY           0
    DHCPV6_RECONFIGURE    0
    DHCPV6_RELAY_FORW     0
```

```
user@host> clear dhcpv6 relay statistics
```

```
user@host> show dhcpv6 relay statistics
```

```
DHCPv6 Packets dropped:
```

```
    Total                                0
```

```
Messages received:
```

```
    DHCPV6_DECLINE                        0
```

```
    DHCPV6_SOLICIT                        0
```

```
    DHCPV6_INFORMATION_REQUEST           0
```

```
    DHCPV6_RELEASE                        0
```

```
    DHCPV6_REQUEST                        0
```

```
    DHCPV6_CONFIRM                        0
```

```
    DHCPV6_RENEW                          0
```

```
    DHCPV6_REBIND                         0
```

```
    DHCPV6_RELAY_REPL                    0
```

```
Messages sent:
```

```
    DHCPV6_ADVERTISE                      0
```

```
    DHCPV6_REPLY                          0
```

```
    DHCPV6_RECONFIGURE                    0
```

```
    DHCPV6_RELAY_FORW                     0
```

clear dhcp server binding

Syntax `clear dhcp server binding`
 `<address>`
 `<all>`
 `<interface interface-name>`
 `<interfaces-vlan>`
 `<interfaces-wildcard>`
 `<logical-system logical-system-name>`
 `<routing-instance routing-instance-name>`

Release Information Command introduced in Junos OS Release 9.0.
 Options *interfaces-vlan* and *interfaces-wildcard* added in Junos OS Release 12.1.

Description Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the client table on the extended DHCP local server.



NOTE: If you delete the DHCP server configuration, DHCP server bindings might still remain. To ensure that DHCP bindings are removed, issue the `clear dhcp server binding` command before you delete the DHCP server configuration.

Options ***address***—(Optional) Clear the binding state for the DHCP client, using one of the following entries:

- *ip-address*—The specified IP address.
- *mac-address*—The specified MAC address.
- *session-id*—The specified session ID.

all—(Optional) Clear the binding state for all DHCP clients.

interface interface-name—(Optional) Clear the binding state for DHCP clients on the specified interface.



NOTE: This option clears all bindings whose initial login requests were received over the specified interface. Dynamic demux login requests are not received over the dynamic demux interface, but rather the underlying interface of the dynamic demux interface. To clear a specific dynamic demux interface, use the *ip-address* or *mac-address* options.

interfaces-vlan—(Optional) Clear the binding state on the interface VLAN ID and S-VLAN ID.

interfaces-wildcard—(Optional) Clear bindings on a set of interfaces. This option supports the use of the wildcard character (*).

logical-system *logical-system-name*—(Optional) Clear the binding state for DHCP clients on the specified logical system.

routing-instance *routing-instance-name*—(Optional) Clear the binding state for DHCP clients on the specified routing instance.

Required Privilege Level view

Related Documentation

- [Clearing DHCP Bindings for Subscriber Access on page 308](#)
- [show dhcp server binding on page 1094](#)

List of Sample Output

- [clear dhcp server binding <ip-address> on page 1017](#)
- [clear dhcp server binding all on page 1017](#)
- [clear dhcp server binding interface on page 1018](#)
- [clear dhcp server binding <interfaces-vlan> on page 1018](#)
- [clear dhcp server binding <interfaces-wildcard> on page 1018](#)

Output Fields See [show dhcp server binding](#) for an explanation of output fields.

Sample Output

clear dhcp server binding <ip-address>

The following sample output displays the address bindings in the DHCP client table on the extended DHCP local server before and after the **clear dhcp server binding** command is issued.

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

```
2 clients, (0 bound, 0 selecting, 0 renewing, 0 rebinding)
```

IP address	Hardware address	Type	Lease expires at
100.20.32.1	90:00:00:01:00:01	active	2007-01-17 11:38:47 PST
100.20.32.3	90:00:00:02:00:01	active	2007-01-17 11:38:41 PST

```
user@host> clear dhcp server binding 10.20.32.1
```

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

```
1 clients, (0 bound, 0 selecting, 0 renewing, 0 rebinding)
```

IP address	Hardware address	Type	Lease expires at
100.20.32.3	90:00:00:02:00:01	active	2007-01-17 11:38:41 PST

clear dhcp server binding all

The following command clears all DHCP local server bindings:

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

clear dhcp server binding interface

The following command clears DHCP local server bindings on a specific interface:

```
user@host> clear dhcp server binding interface fe-0/0/2
```

clear dhcp server binding <interfaces-vlan>

The following command uses the *interfaces-vlan* option to clear all DHCP local server bindings on top of the underlying interface **ae0**, which clears DHCP bindings on all demux VLANs on top of **ae0**:

```
user@host> clear dhcp server binding ae0
```

clear dhcp server binding <interfaces-wildcard>

The following command uses the *interfaces-wildcard* option to clear all DHCP local server bindings over a specific interface:

```
user@host> clear dhcp server binding ge-1/0/0.*
```

clear dhcp server statistics

Syntax	<code>clear dhcp server statistics</code> <code><interface <i>interface-name</i>></code> <code><logical-system <i>logical-system-name</i>></code> <code><routing-instance <i>routing-instance-name</i>></code>
Release Information	Command introduced in Junos OS Release 9.0.
Description	Clear all extended Dynamic Host Configuration Protocol (DHCP) local server statistics.
Options	<p>logical-system <i>logical-system-name</i>—(Optional) Clear the statistics for DHCP clients on the specified logical system. If you do not specify a logical system, statistics are cleared for the default logical system.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Clear the statistics for DHCP clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.</p>
Required Privilege Level	view
List of Sample Output	clear dhcp server statistics on page 1019
Output Fields	See show dhcp server statistics for an explanation of output fields.

Sample Output

clear dhcp server statistics

The following sample output displays the extended DHCP local server statistics before and after the **clear dhcp server statistics** command is issued.

```

user@host> show dhcp server statistics
Packets dropped:
    Total                1
    Lease Time Violation 1

Messages received:
    BOOTREQUEST          89163
    DHCPDECLINE           0
    DHCPDISCOVER          8110
    DHCPINFORM            0
    DHCPRELEASE           0
    DHCPREQUEST          81053

Messages sent:
    BOOTREPLY             32420
    DHCPOFFER             8110
    DHCPACK               8110
    DHCPNAK               8100

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

```

Packets dropped:	
Total	0
Messages received:	
BOOTREQUEST	0
DHCPDECLINE	0
DHCPDISCOVER	0
DHCPINFORM	0
DHCPRELEASE	0
DHCPREQUEST	0
Messages sent:	
BOOTREPLY	0
DHCPOFFER	0
DHCPACK	0
DHCPNAK	0

clear dhcpv6 server binding

Syntax	<pre>clear dhcpv6 server binding <address> <all> <interface interface-name> <interfaces-vlan> <interfaces-wildcard> <logical-system logical-system-name> <routing-instance routing-instance-name></pre>
Release Information	<p>Command introduced in Junos OS Release 9.6.</p> <p>Options <i>interfaces-vlan</i> and <i>interfaces-wildcard</i> added in Junos OS Release 12.1.</p>
Description	Clear the binding state of a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) client from the client table on the extended DHCPv6 local server.
Options	<p>address—(Optional) Clear the binding state for the DHCPv6 client, using one of the following entries:</p> <ul style="list-style-type: none"> • <i>CID</i>—The specified Client ID (CID). • <i>ipv6-prefix</i>—The specified IPv6 prefix. • <i>session-id</i>—The specified session ID. <p>all—(Optional) Clear the binding state for all DHCPv6 clients.</p> <p>interface interface-name—(Optional) Clear the binding state for DHCPv6 clients on the specified interface.</p> <p>interfaces-vlan—(Optional) Clear the binding state on the interface VLAN ID and S-VLAN ID.</p> <p>interfaces-wildcard—(Optional) Clear bindings on a set of interfaces. This option supports the use of the wildcard character (*).</p> <p>logical-system logical-system-name—(Optional) Clear the binding state for DHCPv6 clients on the specified logical system.</p> <p>routing-instance routing-instance-name—(Optional) Clear the binding state for DHCPv6 clients on the specified routing instance.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • Clearing DHCP Bindings for Subscriber Access on page 308 • show dhcpv6 server binding on page 1111
List of Sample Output	<p>clear dhcpv6 server binding all on page 1022</p> <p>clear dhcpv6 server binding <ipv6-prefix> on page 1022</p>

[clear dhcpv6 server binding interface on page 1022](#)
[clear dhcpv6 server binding <interfaces-vlan> on page 1022](#)
[clear dhcpv6 server binding <interfaces-wildcard> on page 1022](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

`clear dhcpv6 server binding all`

The following command clears all DHCPv6 local server bindings:

```
user@host> clear dhcpv6 server binding all
```

`clear dhcpv6 server binding <ipv6-prefix>`

The following command clears DHCPv6 local server bindings for a specific IPv6 prefix:

```
user@host> clear dhcpv6 server binding 14/0x00010001/0x02b3be8f/0x00109400/0x0005
```

`clear dhcpv6 server binding interface`

The following command clears DHCPv6 local server bindings on a specific interface:

```
user@host> clear dhcpv6 server binding interface fe-0/0/2
```

`clear dhcpv6 server binding <interfaces-vlan>`

The following command uses the *interfaces-vlan* option to clear all DHCPv6 local server bindings on top of the underlying interface **ae0**, which clears DHCPv6 bindings on all demux VLANs on top of **ae0**:

```
user@host> clear dhcpv6 server binding interface ae0
```

`clear dhcpv6 server binding <interfaces-wildcard>`

The following command uses the *interfaces-wildcard* option to clear all DHCPv6 local server bindings over a specific interface:

```
user@host> clear dhcpv6 server binding ge-1/0/0.*
```

clear dhcpv6 server statistics

Syntax	clear dhcpv6 server statistics <interface <i>interface-name</i> > <logical-system <i>logical-system-name</i> > <routing-instance <i>routing-instance-name</i> >
Release Information	Command introduced in Junos OS Release 9.6.
Description	Clear all extended Dynamic Host Configuration Protocol for IPv6 (DHCPv6) local server statistics.
Options	<p>logical-system <i>logical-system-name</i>—(Optional) Clear the statistics for DHCPv6 clients on the specified logical system. If you do not specify a logical system, statistics are cleared for the default logical system.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Clear the statistics for DHCPv6 clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show dhcpv6 server statistics on page 1117
List of Sample Output	clear dhcpv6 server statistics on page 1023
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear dhcpv6 server statistics

```
user@host> clear dhcpv6 server statistics
```

clear diameter function statistics

Syntax	clear diameter function < <i>function-name</i> > statistics
Release Information	Command introduced in Junos OS Release 9.6. Support for PTSP introduced in Junos OS Release 10.2. Support for Gx-Plus introduced in Junos OS Release 11.2.
Description	Clear current statistics accumulated for a specified function (application) or for all functions associated with the Diameter instance.
Options	<i>function-name</i> —(Optional) Clear statistics for the specified function. Currently, Gx-Plus, JSRC, and packet-triggered-subscribers are supported functions.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• Gx-Plus for Provisioning Subscribers Overview on page 439• Juniper Networks Session and Resource Control (SRC) and JSRC Overview on page 451• PTSP Overview on page 479• show diameter on page 1120• show diameter function on page 1126• show diameter function statistics on page 1130
List of Sample Output	clear diameter function statistics on page 1024
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear diameter function statistics

```
user@host> clear diameter function jsrc statistics
```

clear diameter peer

Syntax	<code>clear diameter peer <i>peer-name</i></code> <code><connection statistics></code>
Release Information	Command introduced in Junos OS Release 9.6.
Description	Delete the specified Diameter peer and clear all statistics or only current statistics for the specified peer.
Options	<p><i>peer-name</i>—Delete the Diameter peer.</p> <p><i>connection</i>—(Optional) Clear all peer statistics and restart the peer state machine for the specified Diameter peer. This is the default action.</p> <p><i>statistics</i>—(Optional) Clear current statistics for the specified Diameter peer.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show diameter on page 1120 • show diameter peer on page 1141 • show diameter peer map on page 1146 • show diameter peer statistics on page 1149
List of Sample Output	clear diameter peer on page 1025
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear diameter peer

```
user@host> clear diameter peer peer5 connection
```

clear ipv6 router-advertisement

Syntax	<code>clear ipv6 router-advertisement</code> <code><interface <i>interface</i>></code> <code><logical-system (all <i>logical-system-name</i>)></code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Clear IPv6 router advertisement counters.
Options	none —Clear IPv6 router advertisement counters for all interfaces. interface <i>interface</i> —(Optional) Clear IPv6 router advertisement counters for the specified interface. logical-system (all <i>logical-system-name</i>) —(Optional) Perform this operation on all logical systems or on a particular logical system.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show ipv6 router-advertisement on page 1155
List of Sample Output	clear ipv6 router-advertisement on page 1026
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear ipv6 router-advertisement

```
user@host> clear ipv6 router-advertisement
```

clear network-access aaa statistics

Syntax	<pre>clear network-access aaa statistics <accounting> <address-assignment (client pool <i>pool-name</i>)> <authentication> <dynamic-requests> <radius> <re-authentication> <terminate-code></pre>
Release Information	<p>Command introduced in Junos OS Release 10.0.</p> <p>Option radius introduced in Junos OS Release 11.4.</p> <p>Option terminate-code introduced in Junos OS Release 11.4.</p>
Description	Clear AAA statistics.
Options	<p>accounting—(Optional) Clear AAA accounting statistics.</p> <p>address-assignment client—(Optional) Clear AAA address-assignment statistics for the client.</p> <p>address-assignment pool <i>pool-name</i>—(Optional) Clear AAA address-assignment pool statistics.</p> <p>authentication—(Optional) Clear AAA authentication statistics.</p> <p>dynamic-requests—(Optional) Clear AAA dynamic-request statistics.</p> <p>radius—(Optional) Clears the values in the Peak and Exceeded columns only.</p> <p>re-authentication—(Optional) Clear AAA reauthentication statistics.</p> <p>terminate-code—(Optional) Clear AAA termination code statistics.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • Verifying and Managing Subscriber AAA Information on page 181
List of Sample Output	<p>clear network-access aaa statistics accounting on page 1027</p> <p>clear network-access aaa statistics address-assignment pool on page 1028</p> <p>clear network-access aaa statistics radius on page 1028</p>
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear network-access aaa statistics accounting

```
user@host> clear network-access aaa statistics accounting
```

clear network-access aaa statistics address-assignment pool

```
user@host> clear network-access aaa statistics address-assignment pool isp_1
```

clear network-access aaa statistics radius

```
user@host> clear network-access aaa statistics radius
```


clear network-access aaa subscriber

Syntax	clear network-access aaa subscriber <statistics username <i>username</i> > <username <i>username</i> >
Release Information	Command introduced in Junos OS Release 9.1.
Description	Clear AAA subscriber statistics and log out subscribers.
Options	statistics username <i>username</i> —Clear AAA subscriber statistics and log out the subscriber. username <i>username</i> —Log out the AAA subscriber.
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • Verifying and Managing Subscriber AAA Information on page 181
List of Sample Output	clear network-access aaa subscriber statistics username on page 1029 clear network-access aaa subscriber username on page 1029
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear network-access aaa subscriber statistics username

```
user@host> clear network-access aaa subscriber statistics username dsmith@isp5555.com
```

clear network-access aaa subscriber username

```
user@host> clear network-access aaa subscriber username dsmith@isp5555.com
```

clear network-access gx-plus replay

Syntax	clear network-access gx-plus replay
Release Information	Command introduced in Junos OS Release 11.2.
Description	Clear pending Gx-Plus login and logout requests (replays). Sends JSER message to PCRF that includes the Juniper-Event-Type AVP (AVP code 2103) with a value of 3 indicating a discovery request. The PCRF returns a JDER message to initiate discovery of all subscribers. When this discovery completes, all pending subscriber requests are cleared.
Options	This command has no options.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• clear network-access gx-plus statistics on page 1031• show network-access gx-plus on page 1188
List of Sample Output	clear network-access gx-plus replay on page 1030
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear network-access gx-plus replay

```
user@host> clear network-access gx-plus replay
```

clear network-access gx-plus statistics

Syntax	clear network-access gx-plus statistics
Release Information	Command introduced in Junos OS Release 11.2.
Description	Clear Gx-Plus statistics.
Options	This command has no options.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show network-access gx-plus on page 1188
List of Sample Output	clear network-access gx-plus statistics on page 1031
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear network-access gx-plus statistics

```
user@host> clear network-access gx-plus statistics
```

clear request services subscribers

Syntax	<code>request services subscribers clear subscriber-profile <i>profile</i> client-id <i>client-id</i></code>
Release Information	Command introduced in Junos OS Release 11.4.
Description	Clear the subscriber profile associated with the given subscriber.
Options	<i>profile</i> —Name of the subscriber profile to clear the active subscriber profile for the given subscriber. <i>client-id</i> —Client session ID assigned to the subscriber.
Required Privilege Level	clear
List of Sample Output	request services subscriber clear subscriber-profile tc_act_prof client-id on page 1032

Sample Output

[request services subscriber clear subscriber-profile tc_act_prof client-id](#)

```
user@host>request services subscriber clear subscriber-profile tc_act_prof client-id
2533274790395909 | display xml
rpc-reply xmlns:junos="http://xml.juniper.net/junos/11.1I0/junos"
  packet-triggered-subscribers-information
    xmlns="http://xml.juniper.net/junos/11.1I0/junos-packet-triggered-subscribers"
      service-subscribers-request-result junos:style="success"
    /service-subscribers-request-result
  /packet-triggered-subscribers-information
cli
  banner/banner
/ccli
/rpc-reply
```

clear services subscriber sessions

Syntax	<code>clear services subscriber sessions client-id <i>client-id</i></code>
Release Information	Command introduced in Junos OS Release 10.2.
Description	Clear the packet-triggered subscriber sessions on the router to log out the subscribers.
Options	<code>client-id <i>client-id</i></code> —Logs out the packet-triggered subscriber with this client ID. The client ID is a generated identifier assigned to each packet-triggered subscriber known to the router.
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• show services subscriber sessions on page 1214
List of Sample Output	clear services subscriber sessions on page 1033
Output Fields	When you issue this command, you are provided feedback on the status of your request.

Sample Output

clear services
subscriber sessions

```
user@host> clear services subscriber sessions client-id 1
Initiated logout request for 1 subscriber session(s)
```

request ancp oam interface

Syntax	request ancp oam interface (<i>interface-name</i> interface-set <i>set-name</i>) <count <i>count</i> > <timeout <i>duration</i> >
Release Information	Command introduced in Junos OS Release 11.4.
Description	Trigger the access node to run a loopback test on the local loop between the access node and the customer premises equipment. You must specify either an ANCP interface or an ANCP interface set. The access node responds to the NAS with the results of the test.
Options	<p><i>interface-name</i>—Name of the ANCP interface on whose local loop the loopback test is run.</p> <p>interface-set <i>set-name</i>—Name of the ANCP interface set on whose local loop the loopback test is run.</p> <p>count <i>count</i>—(Optional) Number of times a loopback message is sent on the local loop. Range: 1 through 32. Default: 1.</p> <p>timeout <i>duration</i>—(Optional) Period of time in seconds that the NAS waits for a response to the OAM request. Range: 0 through 255. Default: 5.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• Triggering ANCP OAM to Test the Local Loop on page 411
List of Sample Output	request ancp oam interface on page 1034
Output Fields	When you enter this command, you are provided feedback on the status of your request, including the result of the test, the response code, and the response string returned with the OAM response in the event of failure, an error code is displayed.

Sample Output

request ancp oam interface

```
user@host> request ancp oam interface ge-1/0/4.12 count 5 timeout 40
request succeeded
0x503 : DSL line status showtime
DEFAULT RESPONSE
```

request ancp oam neighbor


Syntax	<code>request ancp oam neighbor</code> (<code>ip-address <i>ip-address</i> system-name <i>neighbor-name</i></code>) <code>subscriber <i>identifier-string</i></code> < <code>count <i>count</i></code> > < <code>timeout <i>duration</i></code> >
Release Information	Command introduced in Junos OS Release 11.4.
Description	Trigger the access node to run a loopback test on the local loop between the access node and the customer premises equipment. You must specify both the access node and the subscriber. The access node responds to the NAS with the results of the test.
Options	<p><code>ip-address <i>ip-address</i></code>—IP address that specifies the access node on whose local loop the loopback test is run.</p> <p><code>system-name <i>neighbor-name</i></code>—System name that specifies the access node on whose local loop the loopback test is run.</p> <p><code>subscriber <i>identifier-string</i></code>—Access identifier that specifies the subscriber on whose local loop the loopback test is run.</p> <p><code>count <i>count</i></code>—(Optional) Number of times a loopback message is sent on the local loop. Range: 1 through 32. Default: 1.</p> <p><code>timeout <i>duration</i></code>—(Optional) Period of time in seconds that the NAS waits for a response to the OAM request. Range: 0 through 255. Default: 5.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Triggering ANCP OAM to Test the Local Loop on page 411
List of Sample Output	request ancp oam subscriber on page 1035
Output Fields	When you enter this command, you are provided feedback on the status of your request, including the result of the test, the response code, and the response string returned with the OAM response in the event of failure, an error code is displayed.

Sample Output

request ancp oam subscriber

```
user@host> request ancp oam neighbor 10.10.10.1 subscriber "dslam port-1-11"
request succeeded
0x503 : DSL line status showtime
DEFAULT RESPONSE
```

request dhcp server reconfigure

Syntax	<code>request dhcp server reconfigure (all <i>address</i> interface <i>interface-name</i> logical-system <i>logical-system-name</i> routing-instance <i>routing-instance-name</i>)</code>
Release Information	Command introduced in Junos OS Release 10.0. Command introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	<p>Initiate reconfiguration processing for the specified DHCP clients if they are in the bound state. If the clients are in the reconfiguring state, this command has no effect. If the clients are in any state other than bound or reconfiguring, this command has the same effect as the clear dhcp server binding command.</p> <p>When the local server state machine starts the reconfiguration process on a bound client, the client transitions to the reconfiguring state and the local server sends a forcerenew message to the client. Because the client was in the bound state before entering the reconfiguring state, all subscriber (or DHCP client) services, such as forwarding and statistics, continue to work. An exponential back-off timer determines the interval at which the forcerenew message is sent. If the final attempt is unsuccessful, the client is returned to its original state by default. You can optionally include the clear-on-abort statement to configure the client to be cleared when reconfiguration fails.</p>
Options	<p>all—Initiate reconfiguration for all DHCP clients.</p> <p><i>address</i>—Initiate reconfiguration for DHCP client with the specified IP address or MAC address.</p> <p>interface <i>interface-name</i>—Initiate reconfiguration for all DHCP clients on this logical interface (clients whose initial login requests were received over the specified interface).</p>
	<p> NOTE: You cannot use the interface <i>interface-name</i> option with the request dhcp server reconfigure command for DHCP passive clients (clients that are added as a result of DHCP snooped packets). For passive clients, the interface is not guaranteed to be the next-hop interface to the client, as is the case for active clients.</p>
	<p>logical-system <i>logical-system-name</i>—Initiate reconfiguration for all DHCP clients on the specified logical system.</p> <p>routing-instance <i>routing-instance-name</i>—Initiate reconfiguration reconfigured for all DHCP clients in the specified routing instance.</p>
Required Privilege Level	view

Related Documentation • [Configuring Dynamic Client Reconfiguration of Extended Local Server Clients on page 244](#)

List of Sample Output [request dhcp server reconfigure on page 1037](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

[request dhcp server reconfigure](#)

```
user@host> request dhcp server reconfigure interface fe-0/0/0.100
```

request dhcpv6 server reconfigure

Syntax	request dhcpv6 server reconfigure (all address client-id interface <i>interface-name</i> logical-system <i>logical-system-name</i> routing-instance <i>routing-instance-name</i> session-id)
Release Information	Command introduced in Junos OS Release 10.4. Command introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	<p>Initiate reconfiguration processing for the specified DHCPv6 clients if they are in the bound state. If the clients are in the reconfiguring state, this command has no effect. If the clients are in any state other than bound or reconfiguring, this command has the same effect as the clear dhcpv6 server binding command.</p> <p>When the local server state machine starts the reconfiguration process on a bound client, the client transitions to the reconfigure state and the local server sends a reconfigure message to the client. Because the client was in the bound state before entering the reconfiguring state, all subscriber (or DHCP client) services, such as forwarding and statistics, continue to work. An exponential back-off timer determines the interval at which the reconfigure message is sent. If the final attempt is unsuccessful, the client is returned to its original state by default. You can optionally include the clear-on-abort statement to configure the client to be cleared when reconfiguration fails.</p>
Options	<p>all—Initiate reconfiguration for all DHCPv6 clients.</p> <p>address—Initiate reconfiguration for DHCPv6 client with the specified IPv6 address.</p> <p>client-id—Initiate reconfiguration for DHCPv6 client with the specified client ID.</p> <p>interface <i>interface-name</i>—Initiate reconfiguration for all DHCPv6 clients on this logical interface (clients whose initial login requests were received over the specified interface).</p> <p>logical-system <i>logical-system-name</i>—Initiate reconfiguration for all DHCPv6 clients on the specified logical system.</p> <p>routing-instance <i>routing-instance-name</i>—Initiate reconfiguration reconfigured for all DHCPv6 clients in the specified routing instance.</p> <p>session-id—Initiate reconfiguration for DHCPv6 client with the specified session ID.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Configuring Dynamic Client Reconfiguration of Extended Local Server Clients on page 244
List of Sample Output	request dhcpv6 server reconfigure on page 1039
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request dhcpv6 server reconfigure

```
user@host> request dhcpv6 server reconfigure 2001::2/16
```

request network-access aaa subscriber set session-id

Syntax	<code>request network-access aaa subscriber set session-id <i>subscriber-session-id</i> provisioning-state none</code>
Release Information	Command introduced in Junos OS Release 12.3.
Description	Release control of the PCRF over the specified subscriber session. In response, AAA clears the subscriber's provisioning state and sends a terminated request to the PCRF indicating the subscriber is no longer available.
Options	<i>subscriber-session-id</i> —ID of the subscriber session.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Disabling PCRF Control of a Subscriber Session on page 581 • Activating and Deactivating Subscriber Services Locally with the CLI on page 332

List of Sample Output [request network-access aaa subscriber set session-id on page 1040](#)

Output Fields When you enter this command, you are provided feedback on the status of your request. [Table 59 on page 1040](#) lists possible error messages that might be returned if the service activation fails.

Table 59: Service Activation/Deactivation Error Messages

Message	Description	Corrective Action
Error: AUTHD ISSU in progress	A unified ISSU operation is active.	Wait until the unified ISSU operation completes and then retry the service activation/deactivation.
Service activation/deactivation already in progress	Another service activation/deactivation operation is currently in progress.	Wait until the active operation completes and then retry the activation/deactivation operation.
Session identifier is not for a subscriber session	The session ID is incorrect.	Verify the correct session ID for the subscriber and then retry the activation/deactivation operation.

Sample Output

`request network-access aaa subscriber set session-id`

```
user@host> request network-access aaa subscriber set session-id session-id 49 provisioning-state none
Successful completion
```

request services static-subscribers login group

Syntax	request services static-subscribers login group <i>group-name</i>
Release Information	Command introduced in Junos OS Release 9.6.
Description	Resets the state of an interface group on which static subscribers were forcibly logged out by the request services static-subscribers logout group command. This action enables static subscriber to login on the interfaces in the group.
Options	group <i>group-name</i> —Group of static subscriber interfaces on which static subscribers have been created.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• Resetting the State of an Interface Group for Static Subscriber Login on page 506• request services static-subscribers logout group on page 1042
List of Sample Output	request services static-subscribers login group on page 1041
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request services static-subscribers login group

```
user@host> request services static-subscribers login group boston
```

[request services static-subscribers logout group](#)

Syntax	<code>request services static-subscribers logout group <i>igroup-name</i></code>
Release Information	Command introduced in Junos OS Release 9.6.
Description	Force static subscribers on the interfaces in the group to be logged out. No subscriber can subsequently log in on the interface group until the interface state is reset by a router reset or the <code>request services static-subscribers login group</code> command.
Options	<code>group <i>group-name</i></code> —Group of static subscriber interfaces on which static subscribers have been created.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• Forcing a Group of Static Subscribers to Be Logged Out on page 506• request services static-subscribers login group on page 1041
List of Sample Output	request services static-subscribers logout group on page 1042
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

[request services static-subscribers logout group](#)

```
user@host> request services static-subscribers logout group boston
```

request services static-subscribers login interface

Syntax	<code>request services static-subscribers login interface <i>interface-name</i></code>
Release Information	Command introduced in Junos OS Release 9.6.
Description	Resets the state of an interface on which a static subscriber was forcibly logged out by the <code>request services static-subscribers logout interface</code> command. This action enables a static subscriber to login on the interface.
Options	<code>interface <i>interface-name</i></code> —Static interface on which a static subscriber has been created.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Resetting the State of an Interface for Static Subscriber Login on page 505 • request services static-subscribers logout interface on page 1044
List of Sample Output	request services static-subscribers login interface on page 1043
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request services static-subscribers login interface

```
user@host> request services static-subscribers login interface ge-2/0/1.5
```

request services static-subscribers logout interface

Syntax	<code>request services static-subscribers logout interface <i>interface-name</i></code>
Release Information	Command introduced in Junos OS Release 9.6.
Description	Force static subscriber on the interface to be logged out. No subscriber can subsequently log in on the interface until the interface state is reset by a router reset or the request services static-subscribers login interface command.
Options	<code>interface <i>interface-name</i></code> —Static interface on which a static subscriber has been created.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• Forcing a Static Subscriber to Be Logged Out on page 505• request services static-subscribers login interface on page 1043
List of Sample Output	request services static-subscribers logout interface on page 1044
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request services static-subscribers logout interface

```
user@host> request services static-subscribers logout interface ge-2/0/1.5
```


request system reboot

List of Syntax	Syntax on page 1045 Syntax (EX Series Switches) on page 1045 Syntax (TX Matrix Router) on page 1045 Syntax (TX Matrix Plus Router) on page 1045 Syntax (MX Series Router) on page 1045
Syntax	<pre>request system reboot <at <i>time</i>> <both-routing-engines> <in <i>minutes</i>> <media (compact-flash disk removable-compact-flash usb)> <message "<i>text</i>"> <other-routing-engine></pre>
Syntax (EX Series Switches)	<pre>request system reboot <all-members> <at <i>time</i>> <both-routing-engines> <in <i>minutes</i>> <local> <media (external internal)> <member <i>member-id</i>> <message "<i>text</i>"> <other-routing-engine> <slice <i>slice</i>></pre>
Syntax (TX Matrix Router)	<pre>request system reboot <all-chassis all-lcc lcc <i>number</i> scc> <at <i>time</i>> <both-routing-engines> <in <i>minutes</i>> <media (compact-flash disk)> <message "<i>text</i>"> <other-routing-engine></pre>
Syntax (TX Matrix Plus Router)	<pre>request system reboot <all-chassis all-lcc lcc <i>number</i> sfc <i>number</i>> <at <i>time</i>> <both-routing-engines> <in <i>minutes</i>> <media (compact-flash disk)> <message "<i>text</i>"> <other-routing-engine> <partition (1 2 alternate)></pre>
Syntax (MX Series Router)	<pre>request system reboot <all-members> <at <i>time</i>> <both-routing-engines> <in <i>minutes</i>> <local></pre>

```
<media (external | internal)>  
<member member-id>  
<message "text">  
<other-routing-engine>
```

Release Information Command introduced before Junos OS Release 7.4.
Option **other-routing-engine** introduced in Junos OS Release 8.0.
Command introduced in Junos OS Release 9.0 for EX Series switches.
Option **sfc** introduced for the TX Matrix Plus router in Junos OS Release 9.6.
Option **both-routing-engines** introduced in Junos OS Release 12.1.

Description Reboot the software.

Options **none**—Reboot the software immediately.

all-chassis—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router or TX Matrix Plus router, reboot all routers connected to the TX Matrix or TX Matrix Plus router, respectively.

all-lcc—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router or TX Matrix Plus router, reboot all line card chassis connected to the TX Matrix or TX Matrix Plus router, respectively.

all-members—(EX4200 switches and MX Series routers only) (Optional) Reboot the software on all members of the Virtual Chassis configuration.

at *time*—(Optional) Time at which to reboot the software, specified in one of the following ways:

- **now**—Stop or reboot the software immediately. This is the default.
- **+*minutes***—Number of minutes from now to reboot the software.
- ***yymmddhhmm***—Absolute time at which to reboot the software, specified as year, month, day, hour, and minute.
- ***hh:mm***—Absolute time on the current day at which to stop the software, specified in 24-hour time.

both-routing-engines—(Optional) Reboot both Routing Engines at the same time.

in *minutes*—(Optional) Number of minutes from now to reboot the software. This option is an alias for the **at +*minutes*** option.

lcc *number*—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Line-card chassis number.

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.

- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(EX4200 switches and MX Series routers only) (Optional) Reboot the software on the local Virtual Chassis member.

media (compact-flash | disk | removable-compact-flash | usb)—(Optional) Boot medium for next boot. (The options **removable-compact-flash** and **usb** pertain to the J Series routers only.)

media (external | internal)—(EX Series switches and MX Series routers only) (Optional) Reboot the boot media:

- **external**—Reboot the external mass storage device.
- **internal**—Reboot the internal flash device.

member *member-id*—(EX4200 switches and MX Series routers only) (Optional) Reboot the software on the specified member of the Virtual Chassis configuration. For EX4200 switches, replace ***member-id*** with a value from 0 through 9. For an MX Series Virtual Chassis, replace ***member-id*** with a value of 0 or 1.

message "*text*"—(Optional) Message to display to all system users before stopping or rebooting the software.

other-routing-engine—(Optional) Reboot the other Routing Engine from which the command is issued. For example, if you issue the command from the master Routing Engine, the backup Routing Engine is rebooted. Similarly, if you issue the command from the backup Routing Engine, the master Routing Engine is rebooted.

partition—(TX Matrix Plus routers only) (Optional) Reboot using the specified partition on the boot media. This option has the following suboptions:

- 1—Reboot from partition 1.
- 2—Reboot from partition 2.
- **alternate**—Reboot from the alternate partition.

scc—(TX Matrix routers only) (Optional) Reboot the Routing Engine on the TX Matrix switch-card chassis. If you issue the command from re0, re0 is rebooted. If you issue the command from re1, re1 is rebooted.

sfc *number*—(TX Matrix Plus routers only) (Optional) Reboot the Routing Engine on the TX Matrix Plus switch-fabric chassis. If you issue the command from re0, re0 is rebooted. If you issue the command from re1, re1 is rebooted. Replace ***number*** with 0.

slice *slice*—(EX Series switches only) (Optional) Reboot a partition on the boot media. This option has the following suboptions:

- 1—Power off partition 1.
- 2—Power off partition 2.
- **alternate**—Reboot from the alternate partition.

Additional Information Reboot requests are recorded in the system log files, which you can view with the **show log** command (see *show log*). Also, the names of any running processes that are scheduled to be shut down are changed. You can view the process names with the **show system processes** command (see *show system processes*).

On a TX Matrix or TX Matrix Plus router, if you issue the **request system reboot** command on the master Routing Engine, all the master Routing Engines connected to the routing matrix are rebooted. If you issue this command on the backup Routing Engine, all the backup Routing Engines connected to the routing matrix are rebooted.



NOTE: Before issuing the **request system reboot** command on a TX Matrix Plus router with no options or the **all-chassis**, **all-lcc**, **lcc number**, or **sfc** options, verify that master Routing Engine for all routers in the routing matrix are in the same slot number. If the master Routing Engine for a line-card chassis is in a different slot number than the master Routing Engine for a TX Matrix Plus router, the line-card chassis might become logically disconnected from the routing matrix after the **request system reboot** command.



NOTE: To reboot a router that has two Routing Engines, reboot the backup Routing Engine (if you have upgraded it) first, and then reboot the master Routing Engine.

Required Privilege Level maintenance

Related Documentation

- *clear system reboot*
- *request system halt*
- *Routing Matrix with a TX Matrix Plus Router Solutions Page*

List of Sample Output

[request system reboot on page 1049](#)
[request system reboot \(at 2300\) on page 1049](#)
[request system reboot \(in 2 Hours\) on page 1049](#)
[request system reboot \(Immediately\) on page 1049](#)
[request system reboot \(at 1:20 AM\) on page 1049](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system reboot

```
user@host> request system reboot
Reboot the system ? [yes,no] (no)
```

request system reboot (at 2300)

```
user@host> request system reboot at 2300 message ?Maintenance time!?
Reboot the system ? [yes,no] (no) yes
```

```
shutdown: [pid 186]
*** System shutdown message from root@berry.network.net ***
System going down at 23:00
```

request system reboot (in 2 Hours)

The following example, which assumes that the time is 5 PM (17:00), illustrates three different ways to request the system to reboot in two hours:

```
user@host> request system reboot at +120
user@host> request system reboot in 120
user@host> request system reboot at 19:00
```

request system reboot (Immediately)

```
user@host> request system reboot at now
```

request system reboot (at 1:20 AM)

To reboot the system at 1:20 AM, enter the following command. Because 1:20 AM is the next day, you must specify the absolute time.

```
user@host> request system reboot at 06060120
request system reboot at 120
Reboot the system at 120? [yes,no] (no) yes
```

set request services subscribers

Syntax	<code>request services subscribers set subscriber-profile <i>profile</i> client-id <i>client-id</i></code>
Release Information	Command introduced in Junos OS Release 11.4.
Description	Set the subscriber profile associated with the given subscriber.
Options	<p><i>profile</i>—Name of the subscriber profile to create or override the currently active subscriber profile for the given subscriber.</p> <p><i>client-id</i>—Client session ID assigned to the subscriber.</p>
Required Privilege Level	view
List of Sample Output	request services subscriber set subscriber-profile tc_act_prof client-id on page 1050

Sample Output

[request services subscriber set subscriber-profile tc_act_prof client-id](#)

```
user@host> request services subscriber set subscriber-profile tc_act_prof client-id
2533274790395909 | display xml
rpc-reply xmlns:junos="http://xml.juniper.net/junos/11.1I0/junos"
  packet-triggered-subscribers-information
    xmlns="http://xml.juniper.net/junos/11.1I0/junos-packet-triggered-subscribers"
      service-subscribers-request-result junos:style="success"
    /service-subscribers-request-result
  /packet-triggered-subscribers-information
cli
  banner/banner
/ccli
/rpc-reply
```

show accounting pending-accounting-stops

Syntax	show accounting pending-accounting-stops <detail terse> <profile-name>
Release Information	Command introduced in Junos OS Release 13.1.
Description	Display all statistics for all pending accounting stop requests, including both service and session requests.
Options	<p>none—Display information for all access profiles.</p> <p>detail terse—(Optional) Display the specified level of output.</p> <p>profile-name—(Optional) Particular access profile for which you want to display accounting stop statistics.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • request network-access aaa replay pending-accounting-stops on page 902 • show network-access aaa statistics pending-accounting-stops on page 1172
List of Sample Output	show accounting pending-accounting-stops detail on page 1053 show accounting pending-accounting-stops (Specific Profile) on page 1053 show accounting pending-accounting-stops terse on page 1053
Output Fields	Table 60 on page 1051 lists the output fields for the show accounting pending-accounting-stops command. Output fields are listed in the approximate order in which they appear.

Table 60: show accounting pending-accounting-stops Output Fields

Field Name	Field Description	Level of Output
Type	Type of client.	All levels
Username	Name of the user logged in to the session.	All levels
Logical system/Routing instance	Logical system and routing instance used for the session.	detail none
Access-profile	Access profile used for AAA services for the session.	detail none
Session ID	ID of the subscriber session; generated when the subscriber logs in. In the Service name block, this is the ID of the service session.	All levels

Table 60: show accounting pending-accounting-stops Output Fields (*continued*)

Field Name	Field Description	Level of Output
Accounting Session ID	ID of the accounting session (RADIUS attribute 44). The ID appears in decimal or description format, as specified by the accounting-session-id-format statement.	detail none
IP Address	IP address of the subscriber.	detail none
IPv6 Prefix	IPv6 address of the subscriber.	detail none
Authentication State	State of the subscriber authentication session: AuthInit, AuthStart, AuthChallenge, AuthRedirect, AuthClntRespWait, AuthAcctVolStatsAckWait, AuthAcctStopAckWait, AuthServCreateRespWait, AuthLogoutStart, AuthStateActive, AuthClntLogoutRespWait, AuthProfileUpdateWait, AuthProvisionRespWait, AuthProvisionServiceCreationWait	detail none
Accounting State	State of the subscriber accounting session: Acc-Init, Acc-Start-Sent, Imm-Update-Stats-Pending, Acc-Interim-Sent, Acc-Stop-Stats-Pending, Acc-Stop-Sent, Acc-Stop-On-Fail-Deny-Sent, Acc-Stop-Ackd	detail none
Service name	Name of the attached service or policy.	detail none
Service State	State of the service provided in the subscriber session.	detail none
Session uptime	How long the session has been up, in <i>HH:MM:SS</i> .	detail none
Accounting status	Status of the accounting configuration for the service, on or off , and the type of accounting, time or volume+time . Configured in RADIUS Service-Statistics VSA [26-69].	detail none
Service accounting session ID	ID of the service accounting session; RADIUS Acct-Session-Id attribute (44). The ID appears in decimal or description format, as specified by the accounting-session-id-format statement.	detail none
Service accounting state	State of the service accounting session: Acc-Init, Acc-Start-Sent, Imm-Update-Stats-Pending, Acc-Interim-Sent, Acc-Stop-Stats-Pending, Acc-Stop-Sent, Acc-Stop-On-Fail-Deny-Sent, Acc-Stop-Ackd	detail none
Accounting interim interval	Amount of time between interim accounting updates for this service, in seconds; RADIUS Service-Interim-Acct-Interval VSA [26-140] or Diameter Acct-Interim-Interval AVP (85).	detail none
Subscriber ID	ID of the subscriber; generated when the subscriber logs in.	detail none
Service ID	ID of the subscriber service.	All levels
Service	Name of the attached service or policy.	terse

Sample Output

show accounting pending-accounting-stops detail

```

user@host> show accounting pending-accounting-stops detail
Type: pppoe
Username: vjshah29@example.com
AAA Logical system/Routing instance: default:default
Access-profile: ce-ppp-profile
Session ID: 84
Accounting Session ID: 84
IP Address: 192.168.0.25
IPv6 Prefix: 2010:9999:18::/48
Authentication State: AuthAcctStopAckWait
Accounting State: Acc-Stop-Stats-Pending
Service name: cos-service
  Service State: SvcInactive
  Session ID: 94
  Session uptime: 00:08:02
  Accounting status: on/time
  Service accounting session ID: 84:94-1352294677
  Service accounting state: Acc-Stop-Stats-Pending
  Accounting interim interval: 600
Service name: filter-service
  Service State: SvcInactive
  Session ID: 93
  Session uptime: 00:08:02
  Accounting status: on/volume+time
  Service accounting session ID: 84:93-1352294677
  Service accounting state: Acc-Stop-Stats-Pending
  Accounting interim interval: 600
Service name: filter-service6
  Service State: SvcInactive
  Session ID: 95
  Session uptime: 00:08:02
  Accounting status: on/volume+time
  Service accounting session ID: 84:95-1352294677
  Service accounting state: Acc-Stop-Stats-Pending
  Accounting interim interval: 600

```

show accounting pending-accounting-stops (Specific Profile)

```
user@host> show accounting pending-accounting-stops ce-ppp-profile
```

Type:	Username:	Session ID:	Service ID:	Service
pppoe	vjshah29@example.com	84		
pppoe	vjshah29@example.com	84	94	cos-service
pppoe	vjshah29@example.com	84	93	filter-service
pppoe	vjshah29@example.com	84	95	filter-service6

show accounting pending-accounting-stops terse

```
user@host> show accounting pending-accounting-stops terse
```

Type:	Username:	Session ID:	Service ID:	Service
pppoe	vjshah29@example.com	84		
pppoe	vjshah29@example.com	84	94	cos-service
pppoe	vjshah29@example.com	84	93	filter-service
pppoe	vjshah29@example.com	84	95	filter-service6
pppoe	larry@example.com	85		
pppoe	larry@example.com	85	94	cos-service

pppoe	larry@example.com	85	93	filter-service
pppoe	larry@example.com	85	95	filter-service6

show ancp cos

Syntax	<code>show ancp cos <i>identifier</i> <last-update> <pending-update></code>
Release Information	Command introduced in Junos OS Release 9.4.
Description	Display information about the CoS state for subscriber traffic.
Options	<p><i>identifier identifier</i>—(Optional) Display information about the local loops for the specified access identifier.</p> <p><i>last-update</i>—(Optional) Display the most recently updated CoS information.</p> <p><i>pending-update</i>—(Optional) Display the pending update of CoS information.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show ancp neighbor on page 1058 • show ancp statistics on page 1066 • show ancp subscriber on page 1071
List of Sample Output	<p>show ancp cos on page 1056</p> <p>show ancp cos last-update on page 1057</p> <p>show ancp cos pending-update on page 1057</p>
Output Fields	Table 61 on page 1055 lists the output fields for the show ancp cos command. Output fields are listed in the approximate order in which they appear.

Table 61: show ancp cos Output Fields

Field Name	Field Description
QoS Adjust Flag	<p>State of QoS adjust: TRUE (configured) or FALSE (not configured).</p> <p>The adjustment factor (percentage) is displayed for each line type: ADSL, ADSL2, ADSL2+, VDSL, VDSL2, SDSL.</p>
Keepalive Timer	Interval between the keepalive messages that the ANCP agent sends to CoS.
Cos State	<p>State of the interaction between the ANCP agent and CoS:</p> <ul style="list-style-type: none"> • ANCPD_COS_CONNECT_NEEDED • ANCPD_COS_CONNECT_PENDING • ANCPD_COS_CONNECT_DONE • ANCPD_COS_SESSION_SENT • ANCPD_COS_WRITE_READY

Table 61: show ancp cos Output Fields (*continued*)

Field Name	Field Description
Connect Time	Time at which the ANCP agent connected to CoS; useful for debugging.
Session Time	Time at which the ANCP agent sent a session connect message to CoS; useful for debugging.
Routing Instance Time	Time at which the ANCP agent sent the routing instance to CoS; useful for debugging.
Keepalive Time	Time at which the last keepalive message was sent.
Update Time	Time at which the shaping rate was last updated.
Type	Subscriber access type: ifl indicates that a single VLAN carries subscriber traffic and iflset indicates that a set of VLANs carries subscriber traffic.
Name	System-wide name of the particular subscriber access.
Index	Access identifier.
Pending Update	Actual downstream data rate to be applied next to this local loop, in Kbps.
Last Update	Actual downstream data rate last applied to this local loop, in Kbps.

Sample Output

show ancp cos

```
user@host> show ancp cos
```

```

Qos Adjust Flag:      TRUE
ADSL adjustment factor: 95
ADSL2 adjustment factor: 90
ADSL2+ adjustment factor:85
VDSL adjustment factor: 80
VDSL2 adjustment factor: 75
SDSL adjustment factor: 70
Keepalive Timer:      45 secs
Cos State:             WRITE_READY
Connect Time:          Not Set
Session Time:          Not Set
Routing Instance Time: Not Set
Keepalive Time:        Not Set
Update Time:           Not Set

```

Type	Name	Index	Pending Update	Last Update
iflset	set-ge-10410	1	None	64 Kbps
iflset	set-ge-10411	2	None	64 Kbps
ifl	ge-1/0/4.2	71	None	64 Kbps
ifl	ge-1/0/4.3	72	None	64 Kbps

show ancp cos last-update

```
user@host> show ancp cos last-update
```

```

Qos Adjust Flag:      TRUE
ADSL adjustment factor: 95
ADSL2 adjustment factor: 90
ADSL2+ adjustment factor:85
VDSL adjustment factor: 80
VDSL2 adjustment factor: 75
SDSL adjustment factor: 70
Keepalive Timer:      45 secs
Cos State:            WRITE_READY
Connect Time:         Mon Nov 17 15:03:01 2008
Session Time:         Mon Nov 17 15:03:13 2008
Routing Instance Time: Mon Nov 17 15:03:14 2008
Keepalive Time:       Wed Nov 19 15:32:14 2008
Update Time:         Mon Nov 17 15:03:15 2008

```

Type	Name	Index	Pending Update	Last Update
iflset	iflset0	1	None	64 Kbps
iflset	iflset1	2	None	64 Kbps

show ancp cos pending-update

```
user@host> show ancp cos pending-update
```

```

Qos Adjust Flag:      TRUE
ADSL adjustment factor: 95
ADSL2 adjustment factor: 90
ADSL2+ adjustment factor:85
VDSL adjustment factor: 80
VDSL2 adjustment factor: 75
SDSL adjustment factor: 70
Keepalive Timer:      45 secs
Cos State:            WRITE_READY
Connect Time:         Not Set
Session Time:         Not Set
Routing Instance Time: Not Set
Keepalive Time:       Not Set
Update Time:         Not Set
Keepalive Timer:      45 secs
Connect Time:         Mon Nov 17 15:03:01 2008
Session Time:         Mon Nov 17 15:03:13 2008
Routing Instance Time: Mon Nov 17 15:03:14 2008
Keepalive Time:       Wed Nov 19 15:32:29 2008
Rate Update Time:     Mon Nov 17 15:03:15 2008

```

show ancp neighbor

Syntax	<code>show ancp neighbor</code> <code><brief detail></code> <code><ip-address <i>ip-address</i>></code> <code><system-name <i>mac-address</i>></code>
Release Information	Command introduced in Junos OS Release 9.4.
Description	Display information about all ANCP neighbors or the specified ANCP neighbor, regardless of operational state.
Options	<p>brief detail—(Optional) Display the specified level of detail.</p> <p>ip-address <i>ip-address</i>—(Optional) IP address of the ANCP neighbor (access node).</p> <p>system-name <i>mac-address</i>—(Optional) MAC address of the ANCP neighbor (access node).</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show ancp cos on page 1055 • show ancp subscriber on page 1071
List of Sample Output	show ancp neighbor on page 1061 show ancp neighbor detail on page 1061 show ancp neighbor ip-address on page 1063 show ancp neighbor system-name on page 1064
Output Fields	Table 62 on page 1058 lists the output fields for the show ancp neighbor command. Output fields are listed in the approximate order in which they appear.

Table 62: show ancp neighbor Output Fields

Field Name	Field Description	Level of Output
Version	Version of the ANCP implementation: <ul style="list-style-type: none"> • 0x31—General Switch Management Protocol (GSMP) version 3, sub-version 1; ANCP version before <i>RFC 6320, Protocol for Access Node Control Mechanism in Broadband Networks</i>. • 0x32—ANCP version 1, defined in <i>RFC 6320, Protocol for Access Node Control Mechanism in Broadband Networks</i>. 	brief detail none
IP Address	IP address of the ANCP neighbor.	brief detail none
PartId	Number that associates the ANCP message with a specific partition.	brief none

Table 62: show ancp neighbor Output Fields (*continued*)

Field Name	Field Description	Level of Output
State	Operational state of the ANCP adjacency: <ul style="list-style-type: none"> Configured—The neighbor has been configured, but has never been in the Established state. An asterisk (*) is prefixed to the neighbor entry for this state. Establishing—Adjacency negotiations are in progress for the neighbor. An asterisk (*) is prefixed to the neighbor entry for this state. This state is rarely seen because the adjacency is established so quickly. Established—Adjacency negotiations have succeeded for the neighbor and an ANCP session has been established. Not Estblshed—Not Established; adjacency negotiations are ready to begin. Indicates that this neighbor previously had been in the Established state; that is, it has lost a previously established adjacency. An asterisk (*) is prefixed to the neighbor entry for this state. 	All levels
Time	How long the adjacency has been up in one of the following formats: <ul style="list-style-type: none"> <i>nwndnh</i>—number of weeks, days, and hours <i>nd hh:mm:ss</i>—number of days, hours, minutes, and seconds 	brief detail none
Subscriber Count	Number of subscribers associated with the ANCP neighbor (access local loop).	brief none
Capabilities	Negotiated ANCP capability: <ul style="list-style-type: none"> Topo—Topology discovery. OAM—Performance of local Operations Administration Maintenance (OAM) procedures on an access loop controlled by the router. 	All levels
System Name	MAC address of the ANCP neighbor.	detail
TCP Port	TCP port on which ANCP messages are exchanged.	detail
System Instance	Number identifying the ANCP link instance from the edge device's perspective.	detail
Peer Instance	Number identifying the ANCP instance from the access node's perspective. This number is unique and changes when the node or link comes back up after going down.	detail
Timer	Adjacency timer value advertised by the ANCP peer in 100 ms increments; the interval between ANCP ACK messages. This value remains constant for the duration of an ANCP session.	detail
Partition Type	Number that identifies whether partitions are used and how the ID is negotiated: <ul style="list-style-type: none"> 0—No partition. 1—Fixed partition requested. 2—Fixed partition assigned. 	detail
Partition Flag	Number that specifies the type of partition requested: 1 (new adjacency) or 2 (recovered adjacency).	detail

Table 62: show ancp neighbor Output Fields (*continued*)

Field Name	Field Description	Level of Output
Partition Identifier	Number that associates the ANCP message with a specific partition.	detail
Partition Adjacencies	Number of adjacencies that share the partition.	detail
Dead Timer	Remaining period that the edge device waits for adjacency packets from a neighbor before declaring the neighbor to be down. The maximum dead time value is three times the configured adjacency timer value. This field displays the current value based on the time that the last adjacency packet was received.	detail
Received Syn Count	Number of synchronization messages received from neighbors to maintain adjacencies.	detail
Received Synack Count	Number of synchronization acknowledgment messages received from neighbors in response to the node's synchronization messages.	detail
Received Rstack Count	Number of messages received from neighbors indicating that the link to the neighbor needs to be reset.	detail
Received Ack Count	Number of acknowledgment messages periodically received from neighbors after an adjacency has been established.	detail
Received Port Up Count	Number of status messages received from neighbors indicating that a port has transitioned to the up state.	detail
Received Port Down Count	Number of status messages received from neighbors indicating that a port has transitioned to the down state.	detail
Received Generic Resp Count	Number of generic response messages received from neighbors.	detail
Received Adjacency Update Count	Number of adjacency update messages received from neighbors.	detail
Received OAM Count	Number of OAM responses received from neighbors in reply to request commands.	detail
Received Other Count	Number of all other ANCP message packets received from neighbors that do not fit into one of the other categories.	detail
Sent Syn Count	Number of synchronization messages sent to neighbors to maintain adjacencies.	detail
Sent Synack Count	Number of synchronization acknowledgment messages sent to neighbors in response to the their synchronization messages.	detail
Sent Rstack Count	Number of messages sent to neighbors indicating that the link to the neighbor needs to be reset.	detail
Sent Ack Count	Number of acknowledgment messages periodically sent to neighbors after an adjacency has been established.	detail

Table 62: show ancp neighbor Output Fields (*continued*)

Field Name	Field Description	Level of Output
Sent Generic Resp Count	Number of generic response messages sent to neighbors.	detail
Sent OAM Count	Number of OAM request commands sent to neighbors.	detail
Max Discovery Limit Exceed Count	Number of times that the maximum number of discovery table entries accepted from the neighbor has been exceeded.	detail
Result Codes	<p>Number of generic response messages sent to neighbors that include each of the following result codes:</p> <ul style="list-style-type: none"> • Invalid Request Message Count—A properly formed request message violated the protocol because of timing (such as a race condition) or direction of transmission. • Specified Port(s) Down Count—One or more of the specified ports are down because of a state mismatch between the router and an ANCP control application. • Out of Resources Count—ANCP is out of resources, probably not related to the access lines. This result code is sent only by an access node. • Request Msg Not Implemented Count— • Malformed Msg Count—Message is malformed because it was corrupted in transit or there was an implementation error at either end of the connection. • TLV Missing Count—One or more mandatory TLVs was missing from a request. • Invalid TLV Contents Count—The contents of one or more TLVs in the request do not match its required specification. • Non-Existent Port(s) Count—One or more of the ports specified in a request do not exist, possibly because of a configuration mismatch between the access node and the router or AAA. 	detail

Sample Output

show ancp neighbor

```

user@host> show ancp neighbor
  Version IP Address      PartID  State      Time      Subscriber
Capabilities
  0x31    10.0.1.3             0       Established 11:24      2          Topo
  0x31    10.0.1.5             0       Not Estblshd 2:45      2          Topo
* 0x0     100.0.0.2            0       Establishing 0          0
* 0x0     192.0.1.0            0       Configured   0          0
* 0x0     192.0.22.1           0       Configured   0          0

```

show ancp neighbor detail

```

user@host> show ancp neighbor detail
Neighbor Information
  Version      : 0x31
  IP Address    : 192.85.1.5
  System Name   : 00:10:94:00:00:01
  Up Time      : 26
  TCP Port     : 32666

```

```

State : Established
Subscriber Count : 4
Capabilities : Topo
System Instance : 2
Peer Instance : 20
Adjacency Timer (in 100ms) : 100
Peer Adjacency Timer (in 100ms) : 100
Partition Type : 0
Partition Flag : 1
Partition Identifier : 0
Partition Adjacencies : 0
Dead Timer : 23
Received Syn Count : 1
Received Synack Count : 1
Received Rstack Count : 0
Received Ack Count : 4
Received Port Up Count : 10
Received Port Down Count : 0
Received Generic Resp Count : 0
Received Adjacency Update Count : 0
Received OAM Count : 0
Received Other Count : 0
Sent Syn Count : 1
Sent Synack Count : 2
Sent Rstack Count : 0
Sent Ack Count : 3
Sent Generic Resp Count : 0
Sent OAM Count : 0
Max Discovery Limit Exceed Count : 0
Result Codes:
Invalid Request Message Count : 0 Received Sent
Specified Port(s) Down Count : 0 0
Out of Resources Count : 0 0
Request Msg Not Implemented Count: 0 0
Malformed Msg Count : 0 0
TLV Missing Count : 0 0
Invalid TLV Contents Count : 0 0
Non-Existent Port(s) Count : 0 0

Version : 0x32
IP Address : 192.168.9.1
System Name : 00:00:64:1c:01:02
Up Time : 36
TCP Port : 61408
State : Not Established
Subscriber Count : 1
Capabilities : Topology Discovery
System Instance : 12
Peer Instance : 1
Adjacency Timer (in 100ms) : 50
Peer Adjacency Timer (in 100ms) : 100
Partition Type : 0
Partition Flag : 1
Partition Identifier : 0
Partition Adjacencies : 0
Dead Timer : 23
Received Syn Count : 24
Received Synack Count : 20
Received Rstack Count : 2
Received Ack Count : 9

```

```

Received Port Up Count      : 5
Received Port Down Count    : 0
Received Generic Resp Count : 0
Received Adjacency Update Count : 0
Received OAM Responses Count : 2
Received Other Count        : 0
Sent Syn Count              : 20
Sent Synack Count           : 24
Sent Rstack Count           : 1
Sent Generic Resp Count     : 0
Sent Ack Count              : 9
Sent OAM Requests Count     : 4
Max Discovery Limit Exceed Count : 0
Result Codes:
Invalid Request Message Count : 0
Specified Port(s) Down Count  : 0
Out of Resources Count        : 0
Request Msg Not Implemented Count: 0
Malformed Msg Count           : 0
TLV Missing Count             : 0
Invalid TLV Contents Count    : 0
Non-Existent Port(s) Count    : 0

```

show ancp neighbor ip-address

```
user@host> show ancp neighbor ip-address 192.85.1.5
```

```

Neighbor Information
Version           : 0x32
IP Address        : 192.85.1.5
System Name       : ba:ad:be:ef:10:10
Up Time           : 26
TCP Port          : 32666
State             : Established
Subscriber Count  : 4
Capabilities      : Topo
System Instance   : 2
Peer Instance     : 20
Adjacency Timer (in 100ms) : 100
Peer Adjacency Timer (in 100ms) : 100
Partition Type    : 0
Partition Flag    : 1
Partition Identifier : 0
Partition Adjacencies : 0
Dead Timer        : 23
Received Syn Count : 1
Received Synack Count : 1
Received Rstack Count : 0
Received Ack Count   : 4
Received Port Up Count : 10
Received Port Down Count : 0
Received Generic Resp Count : 0
Received Adjacency Update Count : 0
Received OAM Count    : 0
Received Other Count  : 0
Sent Syn Count        : 1
Sent Synack Count     : 2
Sent Rstack Count     : 0
Sent Ack Count        : 3
Sent Generic Resp Count : 0
Sent OAM Count        : 0

```

Max Discovery Limit Exceed Count	: 0	
Result Codes:	Received	Sent
Invalid Request Message Count	: 0	0
Specified Port(s) Down Count	: 0	0
Out of Resources Count	: 0	0
Request Msg Not Implemented Count	: 0	0
Malformed Msg Count	: 0	0
TLV Missing Count	: 0	0
Invalid TLV Contents Count	: 0	0
Non-Existent Port(s) Count	: 0	0

show ancp neighbor system-name

user@host> show ancp neighbor ba:ad:be:ef:10:10 detail

Neighbor Information

Version	: 0x31	
IP Address	: 10.100.0.1	
System Name	: 00:00:64:1b:01:02	
Up Time	: 19	
TCP Port	: 1028	
State	: Established	
Subscriber Count	: 2	
Capabilities	: Topology Discovery, OAM	
System Instance	: 1	
Peer Instance	: 10	
Adjacency Timer (in 100ms)	: 100	
Peer Adjacency Timer (in 100ms)	: 250	
Partition Type	: 0	
Partition Flag	: 1	
Partition Identifier	: 0	
Partition Adjacencies	: 0	
Dead Timer	: 55	
Received Syn Count	: 1	
Received Synack Count	: 1	
Received Rstack Count	: 0	
Received Ack Count	: 1	
Received Port Up Count	: 34	
Received Port Down Count	: 0	
Received Generic Resp Count	: 0	
Received Adjacency Update Count	: 0	
Received OAM Responses Count	: 2	
Received Other Count	: 0	
Sent Syn Count	: 1	
Sent Synack Count	: 1	
Sent Rstack Count	: 0	
Sent Ack Count	: 3	
Sent Generic Resp Count	: 0	
Sent OAM Requests Count	: 4	
Max Discovery Limit Exceed Count	: 3	
Result Codes:	Received	Sent
Invalid Request Message Count	: 0	0
Specified Port(s) Down Count	: 0	0
Out of Resources Count	: 0	0
Request Msg Not Implemented Count	: 0	0
Malformed Msg Count	: 0	0
TLV Missing Count	: 0	0
Invalid TLV Contents Count	: 0	0
Non-Existent Port(s) Count	: 0	0

show ancp statistics

Syntax	show ancp statistics <ip-address <i>ip-address</i>> <system-name <i>mac-address</i>>
Release Information	Command introduced in Junos OS Release 13.3.
Description	Display statistics for all ANCP neighbors (access nodes) or the specified ANCP neighbor.
Options	<p>none—Display statistics for all ANCP neighbors, including global statistics not show for individual neighbors.</p> <p>ip-address <i>ip-address</i>—(Optional) Display statistics for only the neighbor with the specified IP address.</p> <p>system-name <i>mac-address</i>—(Optional) Display statistics for only the neighbor with the specified MAC address.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show ancp cos on page 1055 • show ancp neighbor on page 1058 • show ancp subscriber on page 1071
List of Sample Output	show ancp statistics on page 1068 show ancp statistics ip-address on page 1069 show ancp statistics system-name on page 1069
Output Fields	Table 63 on page 1066 lists the output fields for the show ancp statistics command. Output fields are listed in the approximate order in which they appear.

Table 63: show ancp statistics Output Fields

Field Name	Field Description
Number of neighbors	Total count of ANCP neighbors.
Number of subscribers	Total count of ANCP subscribers.
Accept Count	Number of neighbor TCP/IP sessions accepted on listener socket.
Accept Fail Count	Number of neighbor TCP/IP sessions that failed due to one of the following causes: session already exists, maximum number of ANCP connections exceeded, creation of session or neighbor failed, or protocol start failed.

Table 63: show ancp statistics Output Fields (*continued*)

Field Name	Field Description
No Config Accept Deny Count	Number of neighbor TCP/IP sessions that failed because the neighbor was not configured.
Received Syn Count	Number of synchronization messages received from neighbors to maintain adjacencies.
Received Synack Count	Number of synchronization acknowledgment messages received from neighbors in response to the node's synchronization messages.
Received Rstack Count	Number of messages received from neighbors indicating that the link to the neighbor needs to be reset.
Received Ack Count	Number of acknowledgment messages periodically received from neighbors after an adjacency has been established.
Received Port Up Count	Number of status messages received from neighbors indicating that a port has transitioned to the up state.
Received Port Down Count	Number of status messages received from neighbors indicating that a port has transitioned to the down state.
Received Generic Resp Count	Number of generic response messages received from neighbors.
Received Adjacency Update Count	Number of adjacency update messages received from neighbors.
Received OAM Count	Number of OAM responses received from neighbors in reply to request commands.
Received Other Count	Number of all other ANCP message packets received from neighbors that do not fit into one of the other categories.
Sent Syn Count	Number of synchronization messages sent to neighbors to maintain adjacencies.
Sent Synack Count	Number of synchronization acknowledgment messages sent to neighbors in response to the their synchronization messages.
Sent Rstack Count	Number of messages sent to neighbors indicating that the link to the neighbor needs to be reset.
Sent Ack Count	Number of acknowledgment messages periodically sent to neighbors after an adjacency has been established.
Sent Generic Resp Count	Number of generic response messages sent to neighbors.
Sent OAM Count	Number of OAM request commands sent to neighbors.

Table 63: show ancp statistics Output Fields (*continued*)

Field Name	Field Description
Result Codes	<p>Number of generic response messages sent to neighbors that include each of the following result codes:</p> <ul style="list-style-type: none"> • Invalid Request Message Count—A properly formed request messages violated the protocol because of timing (such as a race condition) or direction of transmission. • Specified Port(s) Down Count—One or more of the specified ports are down because of a state mismatch between the router and an ANCP control application. • Out of Resources Count—the ANCP agent is out of resources, probably not related to the access lines. This result code is sent only by an access node. • Request Msg Not Implemented Count— • Malformed Msg Count—Message is malformed because it was corrupted in transit or there was an implementation error at either end of the connection. • TLV Missing Count—One or more mandatory TLVs was missing from a request. • Invalid TLV Contents Count—The contents of one or more TLVs in the request do not match its required specification. • Non-Existent Port(s) Count—One or more of the ports specified in a request do not exist, possibly because of a configuration mismatch between the access node and the router or AAA.

Sample Output

show ancp statistics

```

user@host> show ancp statistics
Statistics
  Number of neighbors           : 4
  Number of subscribers        : 6
  Accept Count                  : 0
  Accept Fail Count             : 0
  No Config Accept Deny Count  : 0
  Received Syn Count            : 2
  Received Synack Count         : 1
  Received Rstack Count         : 0
  Received Ack Count            : 8
  Received Port Up Count        : 7
  Received Port Down Count      : 0
  Received Generic Resp Count   : 0
  Received Adjacency Update Count : 0
  Received OAM Count            : 0
  Received Other Count          : 0
  Sent Syn Count                : 1
  Sent Synack Count             : 1
  Sent Rstack Count             : 0
  Sent Ack Count                : 17
  Sent Generic Resp Count       : 0
  Sent OAM Count                : 4
Result Codes:
  Invalid Request Message Count : 0
  Specified Port(s) Down Count  : 0
  Out of Resources Count        : 0
  Request Msg Not Implemented Count: 0
Received Sent

```


Malformed Msg Count	: 0	0
TLV Missing Count	: 0	0
Invalid TLV Contents Count	: 0	0
Non-Existent Port(s) Count	: 0	0

show ancp statistics ip-address

```

user@host> show ancp statistics ip-address 10.0.0.1
Statistics
  Received Syn Count           : 2
  Received Synack Count       : 1
  Received Rstack Count       : 0
  Received Ack Count          : 8
  Received Port Up Count      : 7
  Received Port Down Count    : 0
  Received Generic Resp Count : 0
  Received Adjacency Update Count : 0
  Received OAM Count          : 0
  Received Other Count        : 0
  Sent Syn Count              : 1
  Sent Synack Count           : 1
  Sent Rstack Count           : 0
  Sent Ack Count              : 17
  Sent Generic Resp Count     : 0
  Sent OAM Count              : 4
Result Codes:
  Received Sent
Invalid Request Message Count : 0 0
Specified Port(s) Down Count : 0 0
Out of Resources Count        : 0 0
Request Msg Not Implemented Count: 0 0
Malformed Msg Count          : 0 0
TLV Missing Count            : 0 0
Invalid TLV Contents Count    : 0 0
Non-Existent Port(s) Count    : 0 0

```

show ancp statistics system-name

```

user@host> show ancp statistics system-name 00:00:64:1b:01:02
Statistics
  Received Syn Count           : 2
  Received Synack Count       : 1
  Received Rstack Count       : 0
  Received Ack Count          : 8
  Received Port Up Count      : 7
  Received Port Down Count    : 0
  Received Generic Resp Count : 0
  Received Adjacency Update Count : 0
  Received OAM Count          : 0
  Received Other Count        : 0
  Sent Syn Count              : 1
  Sent Synack Count           : 1
  Sent Rstack Count           : 0
  Sent Ack Count              : 17
  Sent Generic Resp Count     : 0
  Sent OAM Count              : 4
Result Codes:
  Received Sent
Invalid Request Message Count : 0 0
Specified Port(s) Down Count : 0 0
Out of Resources Count        : 0 0

```

Request Msg Not Implemented Count:	0	0
Malformed Msg Count	: 0	0
TLV Missing Count	: 0	0
Invalid TLV Contents Count	: 0	0
Non-Existent Port(s) Count	: 0	0

show ancp subscriber

Syntax	<code>show ancp subscriber</code> <code><brief detail></code> <code><identifier <i>identifier</i>></code> <code><neighbor <i>ip-address</i>></code>
Release Information	Command introduced in Junos OS Release 9.4.
Description	Display information about active subscribers regardless of the subscriber's operational state, for all subscribers (local access loops), the subscriber associated with the access line specified by an ACL, or the subscriber associated with the specified ANCP neighbor (access node).
Options	<p>brief detail—(Optional) Display the specified level of detail.</p> <p>identifier <i>identifier</i>—(Optional) Display information about the subscriber associated with the access line specified by the access identifier.</p> <p>neighbor <i>ip-address</i>—(Optional) Display information about the subscribers connected to the access node specified by the IP address.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear ancp subscriber on page 1004 • show ancp cos on page 1055 • show ancp neighbor on page 1058
List of Sample Output	show ancp subscriber on page 1074 show ancp subscriber brief on page 1074 show ancp subscriber detail on page 1074 show ancp subscriber identifier identifier-string detail on page 1075
Output Fields	Table 64 on page 1071 lists the output fields for the show ancp subscriber command. Output fields are listed in the approximate order in which they appear.

Table 64: show ancp subscriber Output Fields

Field Name	Field Description	Level of Output
Loop Identifier	<p>Access loop identifier as sent by the access node and configured to map the subscriber to an interface.</p> <p>An asterisk (*) indicates that the information might be stale due to receiving a Port Down message with a DSL Line State of Idle.</p> <p>Two asterisks (**) indicate that the neighbor associated with the subscriber has lost its adjacency. In this case, the DSL Line State might be Established.</p>	brief none
DSL Line State	State of the DSL line: Idle , Showtime , or Silent .	brief detail

Table 64: show ancp subscriber Output Fields (*continued*)

Field Name	Field Description	Level of Output
Type	Type of digital subscriber line employed by the access node: ADSL1 , ADSL2 , ADSL2+ , VDSL1 , VDSL2 , SDSL , or UNKNOWN .	brief none
Interface	Name of the interface set or logical interface.	brief detail none
Rate Kbps	Actual downstream data rate for this local loop.	brief none
Neighbor	IP address of ANCP neighbor (access node).	brief none
Access Loop Circuit Identifier	<p>Access loop circuit identifier as sent by the access node and configured to map the subscriber to an interface.</p> <p>An asterisk (*) indicates that the information might be stale due to receiving a Port Down message with a DSL Line State of Idle.</p> <p>Two asterisks (**) indicate that the neighbor associated with the subscriber has lost its adjacency. In this case, the DSL Line State might be Established.</p>	detail
Neighbor IP Address	IP address of the ANCP neighbor (access node).	detail
Aggregate Circuit Identifier Binary	Binary identifier for the VLAN circuit ID.	detail
DSL Type	Type of digital subscriber line employed by the access node: ADSL1 , ADSL2 , ADSL2+ , VDSL1 , VDSL2 , SDSL , or UNKNOWN .	detail
DSL Line Data Link	Data link protocol employed on the access loop: AAL5 or Ethernet .	detail
DSL Line Encapsulation	<p>Encapsulation type on the access loop, for Ethernet only:</p> <ul style="list-style-type: none"> 0—NA, type not conveyed 1—Untagged Ethernet 2—Single-tagged Ethernet 	detail
DSL Line Encapsulation Payload	<p>Payload carried across the access loop:</p> <ul style="list-style-type: none"> 0—NA, type not conveyed 1—PPPoA LLC 2—PPPoA null 3—IPoA LLC 4—IPoA null 5—Ethernet over AAL5 LLC with FCS 6—Ethernet over AAL5 LLC without FCS 7—Ethernet over AAL5 null with FCS 8—Ethernet over AAL5 null without FCS 	detail
Interface Type	Type of interface employed for subscriber traffic: ifl for a single VLAN or interface-set for a configured group of VLANs.	detail

Table 64: show ancp subscriber Output Fields (*continued*)

Field Name	Field Description	Level of Output
Actual Net Data Upstream	Actual upstream data rate for this local loop, in Kbps.	detail
Actual Net Data Downstream	Actual downstream data rate for this local loop, in Kbps.	detail
Minimum Net Data Upstream	Minimum upstream data rate desired by the operator for this local loop, in Kbps.	detail
Minimum Net Data Downstream	Minimum downstream data rate desired by the operator for this local loop, in Kbps.	detail
Maximum Net Data Upstream	Maximum upstream data rate desired by the operator for this local loop, in Kbps.	detail
Maximum Net Data Downstream	Maximum downstream data rate desired by the operator for this local loop, in Kbps.	detail
Attainable Net Data Upstream	Maximum attainable upstream data rate for this local loop, in Kbps.	detail
Attainable Net Data Downstream	Maximum attainable downstream data rate for this local loop, in Kbps.	detail
Minimum Low Power Data Downstream	Minimum downstream data rate desired by the operator for this local loop in low power state, in Kbps.	detail
Minimum Low Power Data Upstream	Minimum upstream data rate desired by the operator for this local loop in low power state, in Kbps.	detail
Maximum Interleave Delay Downstream	Maximum interleaving delay for downstream data, in milliseconds.	detail
Maximum Interleave Delay Upstream	Maximum interleaving delay for upstream data, in milliseconds.	detail
Actual Interleave Delay Downstream	Actual interleaving delay for downstream data, in milliseconds.	detail
Actual Interleave Delay Upstream	Actual interleaving delay for upstream data, in milliseconds.	detail

Sample Output

show ancp subscriber

```
user@host> show ancp subscriber
```

Loop Identifier	DSL Line State	Type	Interface	Rate Kbps	Neighbor
**circuit 101	Idle	ADSL1	----	32	10.0.1.3
**circuit 102	Idle	ADSL1	----	32	10.0.1.3
circuit 301	Showtime	ADSL1	----	32	10.0.1.5
circuit 302	Showtime	ADSL1	----	32	10.0.1.5

show ancp subscriber brief

```
user@host> show ancp subscriber brief
```

Loop Identifier	Type	Interface	Rate Kbps	Neighbor
port-1-10	VDSL2	set-ge-10410	64	10.10.10.2
port-1-11	VDSL2	set-ge-10411	64	11.11.11.2
port-2-10	VDSL2	ge-1/0/4.12	64	10.12.12.2
port-2-11	VDSL2	ge-1/0/4.13	64	10.13.13.2

show ancp subscriber detail

```
user@host> show ancp subscriber detail
```

Subscriber Information

- * Access Loop Circuit Identifier : circuit 101
 - Neighbor IP Address : 10.0.1.3
 - Aggregate Circuit Identifier Binary : 0/0
 - DSL Type : ADSL1
 - DSL Line State : Idle
 - DSL Line Data Link : Data link 2
 - DSL Line Encapsulation : N/A
 - DSL Line Encapsulation Payload : N/A
 - Interface Type : N/A
 - Interface : ----
 - Actual Net Data Upstream : 32
 - Actual Net Data Downstream : 32
 - Minimum Net Data Upstream : 0
 - Minimum Net Data Downstream : 0
 - Maximum Net Data Upstream : 0
 - Maximum Net Data Downstream : 0
 - Attainable Net Data Upstream : 1024
 - Attainable Net Data Downstream : 8192
 - Minimum Low Power Data Downstream : 32
 - Minimum Low Power Data Upstream : 32
 - Maximum Interleave Delay Downstream : 20
 - Maximum Interleave Delay Upstream : 20
 - Actual Interleave Delay Downstream : 20
 - Actual Interleave Delay Upstream : 20
- * Access Loop Circuit Identifier: circuit 102
 - Neighbor IP Address : 10.0.1.3
 - Aggregate Circuit Identifier Binary : 0/0
 - DSL Type : ADSL1
 - DSL Line State : Idle
 - DSL Line Data Link : Data link 2
 - DSL Line Encapsulation : N/A
 - DSL Line Encapsulation Payload : N/A

```

Interface Type           : N/A
Interface                : ----
Actual Net Data Upstream : 32
Actual Net Data Downstream : 32
Minimum Net Data Upstream : 0
Minimum Net Data Downstream : 0
Maximum Net Data Upstream : 0
Maximum Net Data Downstream : 0
Attainable Net Data Upstream : 1024
Attainable Net Data Downstream : 8192
Minimum Low Power Data Downstream : 32
Minimum Low Power Data Upstream : 32
Maximum Interleave Delay Downstream : 20
Maximum Interleave Delay Upstream : 20
Actual Interleave Delay Downstream : 20
Actual Interleave Delay Upstream : 20
...

```

show ancp subscriber identifier identifier-string detail

```
user@host> show ancp subscriber identifier port-1-11 detail
```

```

Access Loop Identifier : port-1-11
Neighbor IP Address    : 10.11.11.2
Aggregate Circuit Identifier Binary : 0/0
DSL Type               : DSL 0
Interface Type         : interface-set
Interface              : set-ge-10411
DSL Line State         : Show Time
Actual Net Data Upstream : 64
Actual Net Data Downstream : 64
DSL Line Data Link     : AAL5
DSL Line Encapsulation : N/A
DSL Line Encapsulation Payload : N/A
Minimum Net Data Upstream : 64
Minimum Net Data Downstream : 64
Maximum Net Data Upstream : 64
Maximum Net Data Downstream : 64
Attainable Net Data Upstream : 64
Attainable Net Data Downstream : 64
Minimum Low Power Data Downstream : 64
Minimum Low Power Data Upstream : 64
Maximum Interleave Delay Downstream : 50
Maximum Interleave Delay Upstream : 50
Actual Interleave Delay Downstream : 50
Actual Interleave Delay Upstream : 50

```

show ancp summary

Syntax	show ancp summary
Release Information	Command introduced in Junos OS Release 13.1.
Description	Display a summary of the counts and states for all ANCP neighbors and subscribers.
Options	This command has no options.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show ancp neighbor on page 1058 • show ancp summary neighbor on page 1078 • show ancp subscriber on page 1071 • show ancp summary subscriber on page 1080
List of Sample Output	show ancp summary on page 1077
Output Fields	Table 65 on page 1076 lists the output fields for the show ancp summary command. Output fields are listed in the approximate order in which they appear.

Table 65: show ancp summary Output Fields

Field Name	Field Description
Configured	Number of ANCP neighbors in the Configured state; that is, that have been configured but never established.
Establishing	Number of ANCP neighbors in the Establishing state; that is, where negotiations are in progress.
Established	Number of ANCP neighbors in the Established state; that is, where negotiations have succeeded and the ANCP session has been established.
Not Estblshd	Number of ANCP neighbors in the Not Estblshd state; that is, that have lost a previously established adjacency and are ready to begin negotiations.
Total	Total number of ANCP neighbors; sum of neighbors in the Configured , Establishing , Established , and Not Estblshd states.
Showtime	Number of DSL lines in Showtime state.
Idle	Number of DSL lines in Idle state.
Silent	Number of DSL lines in Silent state.
Unknown	Number of DSL lines where the state is not Showtime , Idle , or Silent .

Table 65: show ancp summary Output Fields (*continued*)

Field Name	Field Description
Total	Total number of DSL lines (ANCP subscribers); sum of DSL lines in the Showtime , Idle , Silent , and Unknown states.

Sample Output

show ancp summary

```
user@host> show ancp summary
```

Neighbors Summary:

Configured	Establishing	Established	Not Established	Total
22	0	2	0	24

Subscribers Summary:

Showtime	Idle	Silent	Unknown	Total
4	0	0	0	4

show ancp summary neighbor

Syntax	show ancp summary neighbor <ip-address <i>ip-address</i> system-name <i>mac-address</i> >
Release Information	Command introduced in Junos OS Release 13.1.
Description	Display a summary of the counts and states for all ANCP neighbors and of the neighbor's subscribers when you specify a particular neighbor.
Options	<p>ip-address <i>ip-address</i>—(Optional) IP address of the ANCP neighbor (access node).</p> <p>system-name <i>mac-address</i>—(Optional) MAC address of the ANCP neighbor (access node).</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show ancp summary on page 1076 • show ancp subscriber on page 1071 • show ancp summary subscriber on page 1080
List of Sample Output	show ancp summary neighbor on page 1079 show ancp summary neighbor (IP Address) on page 1079 show ancp summary neighbor (MAC Address) on page 1079
Output Fields	Table 66 on page 1078 lists the output fields for the show ancp summary command. Output fields are listed in the approximate order in which they appear.

Table 66: show ancp summary neighbor Output Fields

Field Name	Field Description
Configured	Number of ANCP neighbors in the Configured state; that is, that have been configured but never established.
Establishing	Number of ANCP neighbors in the Establishing state; that is, where negotiations are in progress.
Established	Number of ANCP neighbors in the Established state; that is, where negotiations have succeeded and the ANCP session has been established.
Not Estblshd	Number of ANCP neighbors in the Not Estblshd state; that is, that have lost a previously established adjacency and are ready to begin negotiations.
Total	Total number of ANCP neighbors; sum of neighbors in the Configured , Establishing , Established , and Not Estblshd states.
Showtime	Number of DSL lines for the neighbor in Showtime state.

Table 66: show ancp summary neighbor Output Fields (*continued*)

Field Name	Field Description
Idle	Number of DSL lines for the neighbor in Idle state.
Silent	Number of DSL lines for the neighbor in Silent state.
Unknown	Number of DSL lines for the neighbor where the state is not Showtime , Idle , or Silent .
Total	Total number of DSL lines (ANCP subscribers); sum of DSL lines in the Showtime , Idle , Silent , and Unknown states.

Sample Output

show ancp summary neighbor

```
user@host> show ancp summary neighbor
```

Neighbors Summary:

Configured	Establishing	Established	Not Established	Total
22	0	2	0	24

show ancp summary neighbor (IP Address)

```
user@host> show ancp summary neighbor ip-address 192.168.10.1
```

Neighbor Summary:192.168.10.1 status Established

Subscribers Summary:

Show Time	Idle	Silent	Unknown	Total
6	0	0	0	6

show ancp summary neighbor (MAC Address)

```
user@host> show ancp summary neighbor system-name 00:00:64:1b:01:02
```

Neighbor Summary:00:00:64:1b:01:02 status Established

Subscribers Summary:

Show Time	Idle	Silent	Unknown	Total
5	1	2	0	8

show ancp summary subscriber

Syntax	show ancp summary subscriber
Release Information	Command introduced in Junos OS Release 13.1.
Description	Display a summary of the counts and states for all ANCP subscribers.
Options	This command has no options.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show ancp summary on page 1076 • show ancp neighbor on page 1058 • show ancp summary neighbor on page 1078
List of Sample Output	show ancp summary subscriber on page 1080
Output Fields	Table 67 on page 1080 lists the output fields for the show ancp summary subscriber command. Output fields are listed in the approximate order in which they appear.

Table 67: show ancp summary subscriber Output Fields

Field Name	Field Description
Showtime	Number of DSL lines in Showtime state.
Idle	Number of DSL lines in Idle state.
Silent	Number of DSL lines in Silent state.
Unknown	Number of DSL lines where the state is not Showtime , Idle , or Silent .
Total	Total number of DSL lines (ANCP subscribers); sum of DSL lines in the Showtime , Idle , Silent , and Unknown states.

Sample Output

show ancp summary subscriber

```
user@host> show ancp summary subscriber
```

```
Subscribers Summary:
Show Time      Idle      Silent      Unknown      Total
-----
              8          1          0          1          10
```

show database-replication statistics

Syntax	show database-replication statistics
Release Information	Command introduced in Junos OS Release 9.3.
Description	Display statistics regarding the replication of the subscriber management session database.
Options	This command has no options.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> show database-replication summary on page 1083
List of Sample Output	show database-replication statistics on page 1081
Output Fields	Table 68 on page 1081 lists the output fields for the show database-replication statistics command. Output fields are listed in the approximate order in which they appear.

Table 68: show database-replication statistics Output Fields

Field Name	Field Description
General	Number of dropped connections and the maximum buffer count.
Message Received	Total size of messages received and the number of received messages that have been processed.
Message Sent	Total size of messages sent and the number of sent messages that have been processed.
Message Queue	Number of messages in the queue and the maximum size of the queue.

Sample Output

show database-replication statistics

```
user@host> show database-replication statistics
```

```
General:
  Dropped connections      0
  Max buffer count        0
Message received:
  Size (bytes)            0
  Processed               0
Message sent:
  Size (bytes)            0
  Processed               0
Message queue:
```

Queue full	0
Max queue size	0

show database-replication summary

Syntax	show database-replication summary
Release Information	Command introduced in Junos OS Release 9.3.
Description	Display summary information regarding database replication for the subscriber management session database.
Options	This command has no options.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show database-replication statistics on page 1081
List of Sample Output	show database-replication summary on page 1084
Output Fields	Table 69 on page 1083 lists the output fields for the show database-replication summary command. Output fields are listed in the approximate order in which they appear.

Table 69: show database-replication summary Output Fields

Field Name	Field Description
Graceful Restart	State of graceful Routing Engine switchover (GRES): <ul style="list-style-type: none"> • Enabled • Disabled
Mastership	State of the Routing Engine: <ul style="list-style-type: none"> • Master • Standby
Connection	State of the connection: <ul style="list-style-type: none"> • Up • Down
Database	State of the subscriber management database: <ul style="list-style-type: none"> • Available • Unavailable • Synchronized
Message Queue	State of the message queue: <ul style="list-style-type: none"> • Full • Init • Not Ready • Ready

Sample Output

show database-replication summary

```
user@host> show database-replication summary
General:
  Graceful Restart      Enabled
  Mastership            Standby
  Connection            Up
  Database              Available
  Message Queue         Ready
```


show network-access aaa accounting

Syntax	show network-access aaa accounting
Release Information	Command introduced in Junos OS Release 12.3.
Description	Display the state of the RADIUS Acct-On response sent from the RADIUS server.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • RADIUS Acct-On and Acct-Off Messages on page 91
List of Sample Output	show network-access aaa accounting on page 1085
Output Fields	Table 70 on page 1085 lists the output fields for the show network-access aaa accounting command. Output fields are listed in the approximate order in which they appear.

Table 70: show network-access aaa accounting Output Fields

Field Name	Field Description
Profile	Name of the profile associated with the RADIUS server. A RADIUS server can be associated with more than one profile.
Logical System	Logical system associated with the access profile.
Routing Instance	Routing instance associated with the access profile.
Acct-On-Response	Status of the RADIUS Acct-On response. <ul style="list-style-type: none"> • ACK—ACK response for the Acct-On message is received from the RADIUS server. • ERROR—An error condition has occurred. • NONE— No Acct-On message is sent. • PENDING—Acct-On message is sent to RADIUS server, but no response has been received yet.

Sample Output

show network-access aaa accounting

```

user@host> show network-access aaa accounting
Profile      Logical System  Routing Instance  Acct-On-Response
ppp-profile  default        default          ACK
l2tp-profile default        l2tp_RI          PENDING

```

show dhcp relay binding

Syntax **show dhcp relay binding**
 <address>
 <brief>
 <detail>
 <interface *interface-name*>
 <interfaces-vlan>
 <interfaces-wildcard>
 <ip-address | mac-address>
 <logical-system *logical-system-name*>
 <routing-instance *routing-instance-name*>
 <summary>

Release Information Command introduced in Junos OS Release 8.3.
 Options **interface** and **mac-address** added in Junos OS Release 8.4.
 Options **interfaces-vlan** and **interfaces-wildcard** added in Junos OS Release 12.1.
 Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Routers.

Description Display the address bindings in the Dynamic Host Configuration Protocol (DHCP) client table.

Options **address**—(Optional) Display DHCP binding information for a specific client identified by one of the following entries:

- *ip-address*—The specified IP address.
- *mac-address*—The specified MAC address.
- *session-id*—The specified session ID.

brief—(Optional) Display brief information about the active client bindings. This is the default, and produces the same output as **show dhcp relay binding**.

detail—(Optional) Display detailed client binding information.

interface *interface-name*—(Optional) Perform this operation on the specified interface. You can optionally filter on VLAN ID and SVLAN ID.

interfaces-vlan—(Optional) Show the binding state information on the interface VLAN ID and S-VLAN ID.

interfaces-wildcard—(Optional) The set of interfaces on which to show binding state information. This option supports the use of the wildcard character (*).

logical-system *logical-system-name*—(Optional) Perform this operation on the specified logical system.

routing-instance *routing-instance-name*—(Optional) Perform this operation on the specified routing instance.

summary—(Optional) Display a summary of DHCP client information.

Required Privilege Level view

Related Documentation

- [Clearing DHCP Bindings for Subscriber Access on page 308](#)
- [clear dhcp relay binding on page 1006](#)

List of Sample Output

- [show dhcp relay binding on page 1088](#)
- [show dhcp relay binding detail on page 1089](#)
- [show dhcp relay binding interface on page 1089](#)
- [show dhcp relay binding interface vlan-id on page 1089](#)
- [show dhcp relay binding interface svlan-id on page 1089](#)
- [show dhcp relay binding ip-address on page 1090](#)
- [show dhcp relay binding mac-address on page 1090](#)
- [show dhcp relay binding session-id on page 1090](#)
- [show dhcp relay binding <interfaces-vlan> on page 1090](#)
- [show dhcp relay binding <interfaces-wildcard> on page 1090](#)
- [show dhcp relay binding summary on page 1090](#)

Output Fields Table 71 on page 1087 lists the output fields for the **show dhcp relay binding** command. Output fields are listed in the approximate order in which they appear.

Table 71: show dhcp relay binding Output Fields

Field Name	Field Description	Level of Output
<i>number</i> clients, (<i>number</i> init, <i>number</i> bound, <i>number</i> selecting, <i>number</i> requesting, <i>number</i> renewing, <i>number</i> rebinding, <i>number</i> releasing)	Summary counts of the total number of DHCP clients and the number of DHCP clients in each state.	summary
IP address	IP address of the DHCP client.	briefdetail
Session Id	Session ID of the subscriber session.	briefdetail
Generated Remote ID	Remote ID generated by the Option 82 Agent Remote ID (suboption 1)	detail
Hardware address	Hardware address of the DHCP client.	briefdetail
Expires	Number of seconds in which the lease expires.	briefdetail

Table 71: show dhcp relay binding Output Fields (*continued*)

Field Name	Field Description	Level of Output
State	State of the DHCP relay address binding table on the DHCP client: <ul style="list-style-type: none"> • BOUND—Client has an active IP address lease. • INIT—Initial state. • REBINDING—Client is broadcasting a request to renew the IP address lease. • RELEASE—Client is releasing the IP address lease. • RENEWING—Client is sending a request to renew the IP address lease. • REQUESTING—Client is requesting a DHCP server. • SELECTING—Client is receiving offers from DHCP servers. 	briefdetail
Interface	Incoming client interface.	brief
Lease Expires	Date and time at which the client's IP address lease expires.	detail
Lease Expires in	Number of seconds in which the lease expires.	detail
Lease Start	Date and time at which the client's IP address lease started.	detail
Lease time violated	Lease time violation has occurred.	detail
Incoming Client Interface	Client's incoming interface.	detail
Server IP Address	IP address of the DHCP server.	detail
Server Interface	Interface of the DHCP server.	detail
Bootp Relay Address	IP address of BOOTP relay.	detail
Type	Type of DHCP packet processing performed on the router: <ul style="list-style-type: none"> • active—Router actively processes and relays DHCP packets. • passive—Router passively snoops DHCP packets passing through the router. 	All levels
Lease expires at	Date and time at which the client's IP address lease expires.	All levels

Sample Output

show dhcp relay binding

```

user@host> show dhcp relay binding
IP address      Session Id  Hardware address  Expires   State   Interface
100.20.32.11    41         00:10:94:00:00:01 86371     BOUND   ge-1/0/0.0
100.20.32.12    42         00:10:94:00:00:02 86371     BOUND   ge-1/0/0.0

```

100.20.32.13	43	00:10:94:00:00:03	86371	BOUND	ge-1/0/0.0
100.20.32.14	44	00:10:94:00:00:04	86371	BOUND	ge-1/0/0.0
100.20.32.15	45	00:10:94:00:00:05	86371	BOUND	ge-1/0/0.0

show dhcp relay binding detail

user@host> show dhcp relay binding detail

Client IP Address: 100.20.32.11

Hardware Address:	00:10:94:00:00:01
State:	BOUND(DHCP_RELAY_STATE_BOUND_ON_INTF_DELETE)
Lease Expires:	2009-07-21 11:00:06 PDT
Lease Expires in:	86361 seconds
Lease Start:	2009-07-20 11:00:06 PDT
Lease time violated:	yes
Last Packet Received:	2009-07-20 11:00:06 PDT
Incoming Client Interface:	ge-1/0/0.0
Server Ip Address:	100.20.22.2
Server Interface:	none
Bootp Relay Address:	100.20.32.2
Session Id:	41

Client IP Address: 100.20.32.12

Hardware Address:	00:10:94:00:00:02
State:	BOUND(DHCP_RELAY_STATE_BOUND_ON_INTF_DELETE)
Lease Expires:	2009-07-21 11:00:06 PDT
Lease Expires in:	86361 seconds
Lease Start:	2009-07-20 11:00:06 PDT
Last Packet Received:	2009-07-20 11:00:06 PDT
Incoming Client Interface:	ge-1/0/0.0
Server Ip Address:	100.20.22.2
Server Interface:	none
Bootp Relay Address:	100.20.32.2
Session Id:	42
Generated Remote ID	host:ge-1/0/0:100

show dhcp relay binding interface

user@host> show dhcp relay binding interface fe-0/0/2

IP address	Hardware address	Type	Lease expires at
100.20.32.1	90:00:00:01:00:01	active	2007-03-27 15:06:20 EDT

show dhcp relay binding interface vlan-id

user@host> show dhcp relay binding interface ge-1/1/0:100

IP address	Session Id	Hardware address	Expires	State	Interface
200.20.20.15	6	00:10:94:00:00:01	86124	BOUND	ge-1/1/0:100

show dhcp relay binding interface svlan-id

user@host> show dhcp relay binding interface ge-1/1/0:10-100

IP address	Session Id	Hardware address	Expires	State	Interface
------------	------------	------------------	---------	-------	-----------

200.20.20.16	7	00:10:94:00:00:02	86124	BOUND
ge-1/1/0:10-100				

show dhcp relay binding ip-address

```
user@host> show dhcp relay binding 100.20.32.13
```

IP address	Session Id	Hardware address	Expires	State	Interface
100.20.32.13	43	00:10:94:00:00:03	86293	BOUND	ge-1/0/0.0

show dhcp relay binding mac-address

```
user@host> show dhcp relay binding 00:10:94:00:00:05
```

IP address	Session Id	Hardware address	Expires	State	Interface
100.20.32.15	45	00:10:94:00:00:05	86279	BOUND	ge-1/0/0.0

show dhcp relay binding session-id

```
user@host> show dhcp relay binding 41
```

IP address	Session Id	Hardware address	Expires	State	Interface
100.20.32.11	41	00:10:94:00:00:01	86305	BOUND	ge-1/0/0.0

show dhcp relay binding <interfaces-vlan>

```
user@host> show dhcp relay binding ge-1/0/0:100-200
```

IP address	Session Id	Hardware address	Expires	State	Interface
192.168.0.17	42	00:10:94:00:00:02	86346	BOUND	ge-1/0/0.1073741827
192.168.0.16	41	00:10:94:00:00:01	86346	BOUND	

show dhcp relay binding <interfaces-wildcard>

```
user@host> show dhcp relay binding ge-1/3/*
```

IP address	Session Id	Hardware address	Expires	State	Interface
192.168.0.9	24	00:10:94:00:00:04	86361	BOUND	ge-1/3/0.110
192.168.0.8	23	00:10:94:00:00:03	86361	BOUND	
192.168.0.7	22	00:10:94:00:00:02	86361	BOUND	ge-1/3/0.110

show dhcp relay binding summary

```
user@host> show dhcp relay binding summary
```

3 clients, (2 init, 1 bound, 0 selecting, 0 requesting, 0 renewing, 0 rebinding, 0 releasing)

show dhcp relay statistics

Syntax	<pre>show dhcp relay statistics <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>></pre>
Syntax	<p>Syntax for EX Series switches:</p> <pre>show dhcp relay statistics <routing-instance <i>routing-instance-name</i>></pre>
Release Information	<p>Command introduced in Junos OS Release 8.3.</p> <p>Command introduced in Junos OS Release 12.1 for EX Series switches.</p> <p>Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Routers.</p>
Description	Display Dynamic Host Configuration Protocol (DHCP) relay statistics.
Options	<p>logical-system <i>logical-system-name</i>—(On routers only) (Optional) Perform this operation on the specified logical system. If you do not specify a logical system name, statistics are displayed for the default logical system.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Perform this operation on the specified routing instance. If you do not specify a routing instance name, statistics are displayed for the default routing instance.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear dhcp relay statistics on page 1008
List of Sample Output	show dhcp relay statistics on page 1093
Output Fields	<p>Table 72 on page 1092 lists the output fields for the show dhcp relay statistics command. Output fields are listed in the approximate order in which they appear.</p>

Table 72: show dhcp relay statistics Output Fields

Field Name	Field Description
Packets dropped	<p>Number of packets discarded by the extended DHCP relay agent application due to errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.</p> <ul style="list-style-type: none"> • Total—Total number of packets discarded by the extended DHCP relay agent application. • Bad hardware address—Number of packets discarded because an invalid hardware address was specified. • Bad opcode—Number of packets discarded because an invalid operation code was specified. • Bad options—Number of packets discarded because invalid options were specified. • Invalid server address—Number of packets discarded because an invalid server address was specified. • Lease Time Violation—Number of packets discarded because of a lease time violation • No available addresses—Number of packets discarded because there were no addresses available for assignment. • No interface match—Number of packets discarded because they did not belong to a configured interface. • No routing instance match—Number of packets discarded because they did not belong to a configured routing instance. • No valid local address—Number of packets discarded because there was no valid local address. • Packet too short—Number of packets discarded because they were too short. • Read error—Number of packets discarded because of a system read error. • Send error—Number of packets that the extended DHCP relay application could not send. • Option 60—Number of packets discarded containing DHCP option 60 vendor-specific information. • Option 82—Number of packets discarded because DHCP option 82 information could not be added.
Messages received	<p>Number of DHCP messages received.</p> <ul style="list-style-type: none"> • BOOTREQUEST—Number of BOOTP protocol data units (PDUs) received • DHCPDECLINE—Number of DHCP PDUs of type DECLINE received • DHCPDISCOVER—Number of DHCP PDUs of type DISCOVER received • DHCPINFORM—Number of DHCP PDUs of type INFORM received • DHCPRELEASE—Number of DHCP PDUs of type RELEASE received • DHCPREQUEST—Number of DHCP PDUs of type REQUEST received
Messages sent	<p>Number of DHCP messages sent.</p> <ul style="list-style-type: none"> • BOOTREPLY—Number of BOOTP PDUs transmitted • DHCPOFFER—Number of DHCP OFFER PDUs transmitted • DHCPACK—Number of DHCP ACK PDUs transmitted • DHCPNACK—Number of DHCP NACK PDUs transmitted • DHCPFORCERENEW—Number of DHCP FORCERENEW PDUs transmitted
External Server Response	State of the external DHCP server responsiveness.
Packets forwarded	<p>Number of packets forwarded.</p> <ul style="list-style-type: none"> • BOOTREQUEST—Number of BOOTREQUEST protocol data units (PDUs) forwarded • BOOTREPLY—Number of BOOTREPLY protocol data units (PDUs) forwarded

Table 72: show dhcp relay statistics Output Fields (*continued*)

Field Name	Field Description
External Server Response	State of the external DHCP server responsiveness.

Sample Output

show dhcp relay statistics

```

user@host> show dhcp relay statistics
Packets dropped:
    Total                               34
    Bad hardware address                 1
    Bad opcode                           1
    Bad options                          3
    Invalid server address               5
    Lease Time Violation                 1
    No available addresses               1
    No interface match                   2
    No routing instance match            9
    No valid local address               4
    Packet too short                     2
    Read error                           1
    Send error                           1
    Option 60                            1
    Option 82                            2

Messages received:
    BOOTREQUEST                         116
    DHCPDECLINE                          0
    DHCPDISCOVER                        11
    DHCPINFORM                           0
    DHCPRELEASE                          0
    DHCPREQUEST                         105

Messages sent:
    BOOTREPLY                           0
    DHCPOFFER                           2
    DHCPACK                              1
    DHCPNAK                              0
    DHCPFORCERENEW                       0

Packets forwarded:
    Total                               4
    BOOTREQUEST                          2
    BOOTREPLY                            2

External Server Response:
    State                               Responding

```

show dhcp server binding

Syntax `show dhcp server binding`
 `<address>`
 `<interfaces-vlan><brief | detail | summary>`
 `<interface interface-name>`
 `<interfaces-vlan>`
 `<interfaces-wildcard>`
 `<logical-system logical-system-name>`
 `<routing-instance routing-instance-name>`

Release Information Command introduced in Junos OS Release 9.0.
 Options *interfaces-vlan* and *interfaces-wildcard* added in Junos OS Release 12.1.

Description Display the address bindings in the client table on the extended Dynamic Host Configuration Protocol (DHCP) local server.



NOTE: If you delete the DHCP server configuration, DHCP server bindings might still remain. To ensure that DHCP bindings are removed, issue the `clear dhcp server binding` command before you delete the DHCP server configuration.

Options **address**—(Optional) Display DHCP binding information for a specific client identified by one of the following entries:

- *ip-address*—The specified IP address.
- *mac-address*—The specified MAC address.
- *session-id*—The specified session ID.

brief | detail | summary—(Optional) Display the specified level of output about active client bindings. The default is **brief**, which produces the same output as **show dhcp server binding**.

interface interface-name—(Optional) Display information about active client bindings on the specified interface. You can optionally filter on VLAN ID and SVLAN ID.

interfaces-vlan—(Optional) Show the binding state information on the interface VLAN ID and S-VLAN ID.

interfaces-wildcard—(Optional) The set of interfaces on which to show the binding state information. This option supports the use of the wildcard character (*).

logical-system logical-system-name—(Optional) Display information about active client bindings for DHCP clients on the specified logical system.

routing-instance routing-instance-name—(Optional) Display information about active client bindings for DHCP clients on the specified routing instance.

Required Privilege Level view

Related Documentation

- [Clearing DHCP Bindings for Subscriber Access on page 308](#)
- [Verifying and Managing Agent Circuit Identifier-Based Dynamic VLAN Configuration](#)
- [clear dhcp server binding on page 1016](#)

List of Sample Output

[show dhcp server binding on page 1097](#)
[show dhcp server binding detail on page 1097](#)
[show dhcp server binding detail \(ACI Interface Set Configured\) on page 1097](#)
[show dhcp server binding interface <vlan-id> on page 1098](#)
[show dhcp server binding interface <svlan-id> on page 1098](#)
[show dhcp server binding <ip-address> on page 1098](#)
[show dhcp server binding <session-id> on page 1098](#)
[show dhcp server binding summary on page 1098](#)
[show dhcp server binding <interfaces-vlan> on page 1098](#)
[show dhcp server binding <interfaces-wildcard> on page 1098](#)

Output Fields [Table 73 on page 1095](#) lists the output fields for the **show dhcp server binding** command. Output fields are listed in the approximate order in which they appear.

Table 73: show dhcp server binding Output Fields

Field Name	Field Description	Level of Output
<i>number</i> clients, (<i>number</i> init, <i>number</i> bound, <i>number</i> selecting, <i>number</i> requesting, <i>number</i> renewing, <i>number</i> releasing)	Summary counts of the total number of DHCP clients and the number of DHCP clients in each state.	summary
IP address	IP address of the DHCP client.	brief detail
Session Id	Session ID of the subscriber session.	brief detail
Hardware address	Hardware address of the DHCP client.	brief detail
Expires	Number of seconds in which lease expires.	brief detail

Table 73: show dhcp server binding Output Fields (*continued*)

Field Name	Field Description	Level of Output
State	State of the address binding table on the extended DHCP local server: <ul style="list-style-type: none"> • BOUND—Client has active IP address lease. • FORCERENEW—Client has received forcerenew message from server. • INIT—Initial state. • RELEASE—Client is releasing IP address lease. • RENEWING—Client sending request to renew IP address lease. • REQUESTING—Client requesting a DHCP server. • SELECTING—Client receiving offers from DHCP servers. 	brief detail
Interface	Interface on which the request was received.	brief
Lease Expires	Date and time at which the client's IP address lease expires.	detail
Lease Expires in	Number of seconds in which lease expires.	detail
Lease Start	Date and time at which the client's IP address lease started.	detail
Lease time violated	Lease time violation has occurred.	detail
Last Packet Received	Date and time at which the router received the last packet.	detail
Incoming Client Interface	Client's incoming interface.	detail
Client Interface Svlan Id	S-VLAN ID of the client's incoming interface.	detail
Client Interface Vlan Id	VLAN ID of the client's incoming interface.	detail
Demux Interface	Name of the IP demultiplexing (demux) interface.	detail
Server IP Address or Server Identifier	IP address of DHCP server.	detail
Server Interface	Interface of DHCP server.	detail
Client Pool Name	Name of address pool used to assign client IP address lease.	detail
ACI Interface Set Name	Internally generated name of the dynamic agent circuit identifier (ACI) interface set.	detail
ACI Interface Set Index	Index number of the dynamic ACI interface set.	detail
ACI Interface Set Session ID	Identifier of the dynamic ACI interface set entry in the session database.	detail

Sample Output

show dhcp server binding

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

IP address	Session Id	Hardware address	Expires	State	Interface
100.20.20.15	6	00:10:94:00:00:01	86180	BOUND	ge-1/0/0.0
100.20.20.16	7	00:10:94:00:00:02	86180	BOUND	ge-1/0/0.0
100.20.20.17	8	00:10:94:00:00:03	86180	BOUND	ge-1/0/0.0
100.20.20.18	9	00:10:94:00:00:04	86180	BOUND	ge-1/0/0.0
100.20.20.19	10	00:10:94:00:00:05	86180	BOUND	ge-1/0/0.0

show dhcp server binding detail

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

Client IP Address: 100.20.20.15

```

Hardware Address:      00:10:94:00:00:01
State:                 BOUND(LOCAL_SERVER_STATE_BOUND_ON_INTF_DELETE)

Lease Expires:         2009-07-21 10:10:25 PDT
Lease Expires in:      86151 seconds
Lease Start:           2009-07-20 10:10:25 PDT
Incoming Client Interface: ge-1/0/0.0
Server Ip Address:     100.20.20.9
Server Interface:      none
Session Id:            6
Client Pool Name:      6
Client IP Address:     100.20.20.16
Hardware Address:      00:10:94:00:00:02
State:                 BOUND(LOCAL_SERVER_STATE_BOUND_ON_INTF_DELETE)

Lease Expires:         2009-07-21 10:10:25 PDT
Lease Expires in:      86151 seconds
Lease Start:           2009-07-20 10:10:25 PDT
Lease time violated:   yes
Incoming Client Interface: ge-1/0/0.0
Server Ip Address:     100.20.20.9
Server Interface:      none
Session Id:            7
Client Pool Name:      7

```

show dhcp server binding detail (ACI Interface Set Configured)

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

Client IP Address: 100.20.22.14

```

Hardware Address:      00:00:64:34:01:02
State:                 BOUND(LOCAL_SERVER_STATE_BOUND)
Lease Expires:         2012-03-13 09:53:32 PDT
Lease Expires in:      82660 seconds
Lease Start:           2012-03-12 10:23:32 PDT
Last Packet Received:  2012-03-12 10:23:32 PDT
Incoming Client Interface: demux0.1073741827
Client Interface Svlan Id: 1802
Client Interface Vlan Id: 302
Demux Interface:       demux0.1073741832
Server Identifier:     100.20.200.202
Session Id:            11

```

```

Client Pool Name:          poolA
Client Profile Name:       DEMUXprofile
ACI Interface Set Name:    aci-1002-demux0.1073741827
ACI Interface Set Index:   2
ACI Interface Set Session ID: 6

```

show dhcp server binding interface <vlan-id>

```

user@host> show dhcp server binding interface ge-1/1/0:100
IP address      Session Id  Hardware address  Expires  State  Interface
200.20.20.15    6          00:10:94:00:00:01 86124    BOUND  ge-1/1/0:100

```

show dhcp server binding interface <svlan-id>

```

user@host> show dhcp server binding interface ge-1/1/0:10-100
IP address      Session Id  Hardware address  Expires  State  Interface
200.20.20.16    7          00:10:94:00:00:02 86124    BOUND  ge-1/1/0:10-100

```

show dhcp server binding <ip-address>

```

user@host> show dhcp server binding 100.20.20.19
IP address      Session Id  Hardware address  Expires  State  Interface
100.20.20.19    10         00:10:94:00:00:05 86081    BOUND  ge-1/0/0.0

```

show dhcp server binding <session-id>

```

user@host> show dhcp server binding 6
IP address      Session Id  Hardware address  Expires  State  Interface
200.20.20.15    6          00:10:94:00:00:01 86124    BOUND  ge-1/0/0.0

```

show dhcp server binding summary

```

user@host> show dhcp server binding summary
3 clients, (2 init, 1 bound, 0 selecting, 0 requesting, 0 renewing, 0 releasing)

```

show dhcp server binding <interfaces-vlan>

```

user@host> show dhcp server binding ge-1/0/0:100-200
IP address      Session Id  Hardware address  Expires  State  Interface
192.168.0.17    42         00:10:94:00:00:02 86346    BOUND  ge-1/0/0.1073741827
192.168.0.16    41         00:10:94:00:00:01 86346    BOUND  ge-1/0/0.1073741827

```

show dhcp server binding <interfaces-wildcard>

```

user@host> show dhcp server binding ge-1/3/*
IP address      Session Id  Hardware address  Expires  State  Interface
192.168.0.9     24         00:10:94:00:00:04 86361    BOUND  ge-1/3/0.110
192.168.0.8     23         00:10:94:00:00:03 86361    BOUND  ge-1/3/0.110
192.168.0.7     22         00:10:94:00:00:02 86361    BOUND  ge-1/3/0.110

```

show dhcp server statistics

Syntax	show dhcp server statistics <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>>
Release Information	Command introduced in Junos OS Release 9.0.
Description	Display extended Dynamic Host Configuration Protocol (DHCP) local server statistics.
Options	<p>logical-system <i>logical-system-name</i>—(Optional) Display information about extended DHCP local server statistics on the specified logical system. If you do not specify a logical system, statistics are displayed for the default logical system.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Display information about extended DHCP local server statistics on the specified routing instance. If you do not specify a routing instance, statistics are displayed for the default routing instance.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear dhcp server statistics on page 1019
List of Sample Output	show dhcp server statistics on page 1100
Output Fields	Table 74 on page 1100 lists the output fields for the show dhcp server statistics command. Output fields are listed in the approximate order in which they appear.

Table 74: show dhcp server statistics Output Fields

Field Name	Field Description
Packets dropped	<p>Number of packets discarded by the extended DHCP local server because of errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.</p> <ul style="list-style-type: none"> • Total—Total number of packets discarded by the extended DHCP local server • Authentication—Number of packets discarded because they could not be authenticated • Bad hardware address—Number of packets discarded because an invalid hardware address was specified • Bad opcode—Number of packets discarded because an invalid operation code was specified • Bad options—Number of packets discarded because invalid options were specified • Dynamic profile—Number of packets discarded due to dynamic profile information • Invalid server address—Number of packets discarded because an invalid server address was specified • Lease Time Violation—Number of packets discarded because of a lease time violation • No available addresses—Number of packets discarded because there were no addresses available for assignment • No interface match—Number of packets discarded because they did not belong to a configured interface • No routing instance match—Number of packets discarded because they did not belong to a configured routing instance • No valid local address—Number of packets discarded because there was no valid local address • Packet too short—Number of packets discarded because they were too short • Read error—Number of packets discarded because of a system read error • Send error—Number of packets that the extended DHCP local server could not send
Messages received	<p>Number of DHCP messages received.</p> <ul style="list-style-type: none"> • BOOTREQUEST—Number of BOOTP protocol data units (PDUs) received • DHCPDECLINE—Number of DHCP PDUs of type DECLINE received • DHCPDISCOVER—Number of DHCP PDUs of type DISCOVER received • DHCPINFORM—Number of DHCP PDUs of type INFORM received • DHCPRELEASE—Number of DHCP PDUs of type RELEASE received • DHCPREQUEST—Number of DHCP PDUs of type REQUEST received
Messages sent	<p>Number of DHCP messages sent.</p> <ul style="list-style-type: none"> • BOOTREPLY—Number of BOOTP PDUs transmitted • DHCPOFFER—Number of DHCP OFFER PDUs transmitted • DHCPACK—Number of DHCP ACK PDUs transmitted • DHCPNACK—Number of DHCP NACK PDUs transmitted • DHCPFORCERENEW—Number of DHCP FORCERENEW PDUs transmitted

Sample Output

show dhcp server statistics

```

user@host> show dhcp server statistics
Packets dropped:
    Total                  1

```


Lease Time Violation	1
Messages received:	
BOOTREQUEST	25
DHCPDECLINE	0
DHCPDISCOVER	10
DHCPINFORM	0
DHCPRELEASE	4
DHCPREQUEST	10
Messages sent:	
BOOTREPLY	20
DHCPOFFER	10
DHCPACK	10
DHCPNAK	0
DHCPFORCERENEW	0

show dhcpv6 relay binding

Syntax	show dhcpv6 relay binding <address> <brief> <detail> <interface <i>interface-name</i>> <interfaces-vlan> <interfaces-wildcard> <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>> <summary>
Release Information	Command introduced in Junos OS Release 11.4. <i>interfaces-vlan</i> and <i>interfaces-wildcard</i> options introduced in Junos OS Release 12.1.
Description	Display the DHCPv6 address bindings in the Dynamic Host Configuration Protocol (DHCP) client table.
Options	<p>address—(Optional) One of the following identifiers for the DHCPv6 client whose binding state you want to show:</p> <ul style="list-style-type: none">• <i>CID</i>—The specified Client ID (CID).• <i>ipv6-prefix</i>—The specified IPv6 prefix.• <i>session-id</i>—The specified session ID. <p>brief—(Optional) Display brief information about the active client bindings. This is the default, and produces the same output as show dhcpv6 relay binding.</p> <p>detail—(Optional) Display detailed client binding information.</p> <p>interface <i>interface-name</i>—(Optional) Perform this operation on the specified interface. You can optionally filter on VLAN ID and S-VLAN ID.</p> <p>interfaces-vlan—(Optional) Interface VLAN ID or S-VLAN ID interface on which to show binding state information.</p> <p>interfaces-wildcard—(Optional) Set of interfaces on which to show binding state information. This option supports the use of the wildcard character (*).</p> <p>logical-system <i>logical-system-name</i>—(Optional) Perform this operation on the specified logical system.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Perform this operation on the specified routing instance.</p> <p>summary—(Optional) Display a summary of DHCPv6 client information.</p>
Required Privilege Level	view

- Related Documentation**
- [Clearing DHCP Bindings for Subscriber Access on page 308](#)
 - [clear dhcpv6 relay binding on page 1011](#)

- List of Sample Output**
- [show dhcpv6 relay binding on page 1104](#)
 - [show dhcpv6 relay binding \(Address\) on page 1105](#)
 - [show dhcpv6 relay binding detail \(Client ID\) on page 1105](#)
 - [show dhcpv6 relay binding detail on page 1105](#)
 - [show dhcpv6 relay binding detail \(Multi-Relay Topology\) on page 1106](#)
 - [show dhcpv6 relay binding \(Session ID\) on page 1106](#)
 - [show dhcpv6 relay binding \(Interfaces VLAN\) on page 1106](#)
 - [show dhcpv6 relay binding \(Interfaces Wildcard\) on page 1106](#)
 - [show dhcpv6 relay binding \(Interfaces Wildcard\) on page 1107](#)
 - [show dhcpv6 relay binding summary on page 1107](#)

- Output Fields** [Table 75 on page 1103](#) lists the output fields for the **show dhcpv6 relay binding** command. Output fields are listed in the approximate order in which they appear.

Table 75: show dhcpv6 relay binding Output Fields

Field Name	Field Description	Level of Output
<i>number clients, (number init, number bound, number selecting, number requesting, number renewing, number rebinding, number releasing)</i>	Summary counts of the total number of DHCPv6 clients and the number of DHCPv6 clients in each state.	summary
Client IPv6 Prefix	Prefix of the DHCPv6 client.	brief detail
Client DUID	DHCP for IPv6 Unique Identifier (DUID) of the client.	brief detail
Session Id	Session ID of the subscriber session.	brief detail
Expires	Number of seconds in which the lease expires.	brief detail
State	State of the DHCPv6 relay address binding table on the DHCPv6 client: <ul style="list-style-type: none"> • BOUND—Client has an active IP address lease. • INIT—Initial state. • REBINDING—Client is broadcasting a request to renew the IP address lease. • RELEASE—Client is releasing the IP address lease. • RENEWING—Client is sending a request to renew the IP address lease. • REQUESTING—Client is requesting a DHCPv6 server. • SELECTING—Client is receiving offers from DHCPv6 servers. 	brief detail
Interface	Incoming client interface.	brief
Lease Expires	Date and time at which the client's IP address lease expires.	detail

Table 75: show dhcpv6 relay binding Output Fields (*continued*)

Field Name	Field Description	Level of Output
Lease Expires in	Number of seconds in which the lease expires.	detail
Preferred Lease Expires	Date and UTC time at which the client's IPv6 prefix expires.	detail
Preferred Lease Expires in	Number of seconds at which the client's IPv6 prefix expires.	detail
Lease Start	Date and time at which the client's IP address lease started.	detail
Lease time violated	Lease time violation has occurred.	detail
Incoming Client Interface	Client's incoming interface.	detail
Server Address	IP address of the DHCPv6 server. Displays unknown for a DHCPv6 relay agent in a multi-relay topology that is not directly adjacent to the DHCPv6 server and does not detect the IP address of the server. In that case, the output instead displays the Next Hop Server Facing Relay field.	detail
Next Hop Server Facing Relay	Next-hop address in the direction of the DHCPv6 server.	detail
Server Interface	Interface of the DHCPv6 server.	detail
Relay Address	IP address of the relay.	detail
Client Pool Name	Address pool that granted the client lease.	detail
Client ID Length	Length of client ID.	All levels
Client Id	Client ID.	All levels
Generated Circuit ID	Circuit ID generated by the DHCPv6 Interface-ID option (option 18)	detail
Generated Remote ID Enterprise Number	The Juniper Networks IANA private enterprise number	detail
Generated Remote ID	Remote ID generated by the DHCPv6 Remote-ID option (option 37)	detail

Sample Output

show dhcpv6 relay binding

```

user@host> show dhcpv6 relay binding
Prefix                Session Id  Expires  State  Interface  Client DUID
2001:bd8:3c4d:15::/64  1          83720    BOUND  ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01
2001:bd8:3c4d:16::/64  2          83720    BOUND  ge-1/0/0.0

```

```

LL_TIME0x1-0x4bfa26af-00:10:94:00:00:02
2001:bd8:3c4d:17::/64      3      83720      BOUND      ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:03
2001:bd8:3c4d:18::/64      4      83720      BOUND      ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:04
2001:bd8:3c4d:19::/64      5      83720      BOUND      ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:05
2001:bd8:3c4d:20::/64      6      83720      BOUND      ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:06

```

show dhcpv6 relay binding (Address)

```

user@host> show dhcpv6 relay binding 2001:bd8:1111:2222::/64 detail
Session Id: 1
  Client IPv6 Prefix:      2001:bd8:3c4d:15::/64
  Client DUID:             LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01

  State:                   BOUND(RELAY_STATE_BOUND)
  Lease Expires:           2011-05-25 07:12:09 PDT
  Lease Expires in:        77115 seconds
  Preferred Lease Expires: 2012-07-24 00:18:14 UTC
  Preferred Lease Expires in: 600 seconds
  Lease Start:             2011-05-24 07:12:09 PDT
  Incoming Client Interface: ge-1/0/0.0
  Server Address:          2008:aaaa:bbbb::1
  Server Interface:        none
  Relay Address:           2001:bd8:1111:2222::
  Client Pool Name:        pool-25
  Client Id Length:        14
  Client Id:
/0x00010001/0x4bfa26af/0x00109400/0x0001

```

show dhcpv6 relay binding detail (Client ID)

```

user@host> show dhcpv6 relay binding 14/0x00010001/0x4bfa26af/0x00109400/0x0001
detail
Session Id: 1
  Client IPv6 Prefix:      2001:bd8:3c4d:15::/64
  Client DUID:             LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01

  State:                   BOUND(RELAY_STATE_BOUND)
  Lease Expires:           2011-05-25 07:12:09 PDT
  Lease Expires in:        77115 seconds
  Preferred Lease Expires: 2012-07-24 00:18:14 UTC
  Preferred Lease Expires in: 600 seconds
  Lease Start:             2011-05-24 07:12:09 PDT
  Lease time violated:      yes
  Incoming Client Interface: ge-1/0/0.0
  Server Address:          2008:aaaa:bbbb::1
  Server Interface:        none
  Relay Address:           2001:bd8:1111:2222::
  Client Pool Name:        pool-25
  Client Id Length:        14
  Client Id:
/0x00010001/0x4bfa26af/0x00109400/0x0001

```

show dhcpv6 relay binding detail

```

user@host> show dhcpv6 relay binding detail
Session Id: 1
  Client IPv6 Prefix:      2001:bd8:3c4d:15::/64

```

```

Client DUID:                               LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01

State:                                     BOUND(RELAY_STATE_BOUND)
Lease Expires:                             2011-05-25 07:12:09 PDT
Lease Expires in:                           77115 seconds
Preferred Lease Expires:                     2012-07-24 00:18:14 UTC
Preferred Lease Expires in:                   600 seconds
Lease Start:                                2011-05-24 07:12:09 PDT
Lease time violated:                          yes
Incoming Client Interface:                   ge-1/0/0.0
Server Address:                              2008:aaaa:bbbb::1
Server Interface:                            none
Relay Address:                               2001:bd8:1111:2222::
Client Pool Name:                            pool-25
Client Id Length:                            14
Client Id:                                   /0x00010001/0x4bfa26af/0x00109400/0x0001
Generated Remote ID Enterprise Number:       1411
Generated Remote ID:                         host:ge-1/0/0:100

```

show dhcpv6 relay binding detail (Multi-Relay Topology)

```

user@host > show dhcpv6 relay binding detail
Session Id: 13
  Client IPv6 Prefix:                       3000:0:0:8001::5/128
  Client DUID:                               LL0x1-00:00:65:03:01:02
  State:                                     BOUND(DHCPV6_RELAY_STATE_BOUND)
  Lease Expires:                             2011-11-21 06:14:50 PST
  Lease Expires in:                           293 seconds
  Preferred Lease Expires:                     2012-07-24 00:18:14 UTC
  Preferred Lease Expires in:                   600 seconds
  Lease Start:                                2011-11-21 06:09:50 PST
  Incoming Client Interface:                   ge-1/0/0.0
  Server Address:                              unknown
  Next Hop Server Facing Relay:                 4000::2
  Server Interface:                            none
  Client Id Length:                            10
  Client Id:                                   /0x00030001/0x00006503/0x0102

```

show dhcpv6 relay binding (Session ID)

```

user@host> show dhcpv6 relay binding 41
Prefix          Session Id Expires   State   Interface   Client DUID
2001:bd8:3c4d:15::/64  41      78837    BOUND   ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01

```

show dhcpv6 relay binding (Interfaces VLAN)

```

user@host> show dhcpv6 relay binding ge-1/0/0:100-200
Prefix          Session Id Expires   State   Interface   Client DUID
2001:DB8::/32   11        87583    BOUND   ge-1/0/0.1073741827
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:DB9::/32   12        87583    BOUND   ge-1/0/0.1073741827
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01

```

show dhcpv6 relay binding (Interfaces Wildcard)

```

user@host> show dhcpv6 relay binding demux0
Prefix          Session Id Expires   State   Interface   Client DUID
2001:DB8::/32   30        79681    BOUND   demux0.1073741824
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:DB9::/32   31        79681    BOUND   demux0.1073741825

```

```

LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:CB9::/32      32      79681    BOUND    demux0.1073741826
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01

```

show dhcpv6 relay binding (Interfaces Wildcard)

```

user@host> show dhcpv6 relay binding ge-1/3/*
Prefix          Session Id Expires State Interface Client DUID
2001:DB8::/32   22      79681    BOUND ge-1/3/0.110
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:DB9::/32   33      79681    BOUND ge-1/3/0.110
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:CB9::/32   24      79681    BOUND ge-1/3/0.110
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01

```

show dhcpv6 relay binding summary

```

user@host> show dhcpv6 relay binding summary
5 clients, (0 init, 5 bound, 0 selecting, 0 requesting, 0 renewing, 0 releasing)

```

show dhcpv6 relay statistics

Syntax	show dhcpv6 relay statistics <code><logical-system <i>logical-system-name</i>></code> <code><routing-instance <i>routing-instance-name</i>></code>
Release Information	Command introduced in Junos OS Release 11.4. Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Switches. Command introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Display Dynamic Host Configuration Protocol for IPv6 (DHCPv6) relay statistics.
Options	<p>logical-system <i>logical-system-name</i>—(Optional) Perform this operation on the specified logical system. If you do not specify a logical system name, statistics are displayed for the default logical system.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Perform this operation on the specified routing instance. If you do not specify a routing instance name, statistics are displayed for the default routing instance.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear dhcpv6 relay statistics on page 1014
List of Sample Output	show dhcpv6 relay statistics on page 1109
Output Fields	Table 76 on page 1108 lists the output fields for the show dhcpv6 relay statistics command. Output fields are listed in the approximate order in which they appear.

Table 76: show dhcpv6 relay statistics Output Fields

Field Name	Field Description
DHCPv6 Packets dropped	<p>Number of packets discarded by the extended DHCPv6 relay agent application due to errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.</p> <ul style="list-style-type: none"> Total—Total number of packets discarded by the DHCPv6 relay agent application. Bad options—Number of packets discarded because invalid options were specified. Bad send—Number of packets that the extended DHCP relay application could not send. Bad src address—Number of packets discarded because the family type was not AF_INET6. No client id—Number of packets discarded because they could not be matched to a client. Lease Time Violation—Number of packets discarded because of a lease time violation No safd—Number of packets discarded because they arrived on an unconfigured interface. Short packet—Number of packets discarded because they were too short. Relay hop count—Number of packets discarded because the hop count in the packet exceeded 32.

Table 76: show dhcpv6 relay statistics Output Fields (*continued*)

Field Name	Field Description
Messages received	<p>Number of DHCPv6 messages received.</p> <ul style="list-style-type: none"> DHCPV6_DECLINE—Number of DHCPv6 PDUs of type DECLINE received DHCPV6_SOLICIT—Number of DHCPv6 PDUs of type SOLICIT received DHCPV6_INFORMATION_REQUEST—Number of DHCPv6 PDUs of type INFORMATION-REQUEST received DHCPV6_RELEASE—Number of DHCPv6 PDUs of type RELEASE received DHCPV6_REQUEST—Number of DHCPv6 PDUs of type REQUEST received DHCPV6_CONFIRM—Number of DHCPv6 PDUs of type CONFIRM received DHCPV6_RENEW—Number of DHCPv6 PDUs of type RENEW received DHCPV6_REBIND—Number of DHCPv6 PDUs of type REBIND received DHCPV6_RELAY_REPL—Number of DHCPv6 PDUs of type RELAY-REPL received
Messages sent	<p>Number of DHCPv6 messages sent.</p> <ul style="list-style-type: none"> DHCPV6_ADVERTISE—Number of DHCPv6 ADVERTISE PDUs transmitted DHCP_REPLY—Number of DHCPv6 REPLY PDUs transmitted DHCP_RECONFIGURE—Number of DHCPv6 RECONFIGURE PDUs transmitted DHCP_RELAY_FORW—Number of DHCPv6 RELAY-FORW PDUs transmitted
Packets forwarded	<p>Number of packets forwarded by the extended DHCPv6 relay agent application.</p> <ul style="list-style-type: none"> FWD REQUEST—Number of DHCPv6 REQUEST packets forwarded FWD REPLY—Number of DHCPv6 REPLY packets forwarded
External Server Response	<p>State of the external DHCP server responsiveness.</p>

Sample Output

show dhcpv6 relay statistics

```

user@host> show dhcpv6 relay statistics
DHCPv6 Packets dropped:
    Total 1
    Lease Time Violation 1

Messages received:
    DHCPV6_DECLINE 0
    DHCPV6_SOLICIT 10
    DHCPV6_INFORMATION_REQUEST 0
    DHCPV6_RELEASE 0
    DHCPV6_REQUEST 10
    DHCPV6_CONFIRM 0
    DHCPV6_RENEW 0
    DHCPV6_REBIND 0
    DHCPV6_RELAY_REPL 0

Messages sent:
    DHCPV6_ADVERTISE 0
    DHCPV6_REPLY 0

```

DHCPV6_RECONFIGURE	0
DHCPV6_RELAY_FORW	0
Packets forwarded:	
Total	4
FWD REQUEST	2
FWD REPLY	2
External Server Response:	
State	Responding

show dhcpv6 server binding

Syntax	<pre>show dhcpv6 server binding <address> <brief detail summary> <interface interface-name> <interfaces-vlan> <interfaces-wildcard> <logical-system logical-system-name> <routing-instance routing-instance-name></pre>
Release Information	<p>Command introduced in Junos OS Release 9.6.</p> <p>Options <i>interfaces-vlan</i> and <i>interfaces-wildcard</i> added in Junos OS Release 12.1.</p>
Description	Display the address bindings in the client table on the extended Dynamic Host Configuration Protocol for IPv6 (DHCPv6) local server.
Options	<p>address—(Optional) One of the following identifiers for the DHCPv6 client whose binding state you want to show:</p> <ul style="list-style-type: none"> • <i>CID</i>—The specified Client ID (CID). • <i>ipv6-prefix</i>—The specified IPv6 prefix. • <i>session-id</i>—The specified session ID. <p>brief detail summary—(Optional) Display the specified level of output about active client bindings. The default is brief, which produces the same output as show dhcpv6 server binding.</p> <p>interface interface-name—(Optional) Display information about active client bindings on the specified interface. You can optionally filter on VLAN ID and SVLAN ID.</p> <p>interfaces-vlan—(Optional) Interface VLAN ID or S-VLAN ID interface on which to show binding state information.</p> <p>interfaces-wildcard—(Optional) Set of interfaces on which to show binding state information. This option supports the use of the wildcard character (*).</p> <p>logical-system logical-system-name—(Optional) Display information about active client bindings for DHCPv6 clients on the specified logical system.</p> <p>routing-instance routing-instance-name—(Optional) Display information about active client bindings for DHCPv6 clients on the specified routing instance.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Clearing DHCP Bindings for Subscriber Access on page 308 • clear dhcpv6 server binding on page 1021

List of Sample Output

- [show dhcpv6 server binding on page 1113](#)
- [show dhcpv6 server binding detail on page 1113](#)
- [show dhcpv6 server binding interface on page 1114](#)
- [show dhcpv6 server binding interface detail on page 1114](#)
- [show dhcpv6 server binding \(IPv6 Prefix\) on page 1115](#)
- [show dhcpv6 server binding \(Session ID\) on page 1115](#)
- [show dhcpv6 server binding \(Interfaces VLAN\) on page 1115](#)
- [show dhcpv6 server binding \(Interfaces Wildcard\) on page 1115](#)
- [show dhcpv6 server binding \(Interfaces Wildcard\) on page 1115](#)
- [show dhcpv6 server binding summary on page 1116](#)

Output Fields [Table 77 on page 1112](#) lists the output fields for the **show dhcpv6 server binding** command. Output fields are listed in the approximate order in which they appear.

Table 77: show dhcpv6 server binding Output Fields

Field Name	Field Description	Level of Output
<i>number clients</i> , (<i>number init</i> , <i>number bound</i> , <i>number selecting</i> , <i>number requesting</i> , <i>number renewing</i> , <i>number releasing</i>)	Summary counts of the total number of DHCPv6 clients and the number of DHCPv6 clients in each state.	summary
Prefix	Client's DHCPv6 prefix, or prefix used to support multiple address assignment.	brief detail
Session Id	Session ID of the subscriber session.	brief detail
Expires	Number of seconds in which lease expires.	brief detail
State	State of the address binding table on the extended DHCPv6 local server: <ul style="list-style-type: none"> • BOUND—Client has active IP address lease. • INIT—Initial state. • RECONFIGURE—Server has sent reconfigure message to client. • RELEASE—Client is releasing IP address lease. • RENEWING—Client sending request to renew IP address lease. • REQUESTING—Client requesting a DHCPv6 server. • SELECTING—Client receiving offers from DHCPv6 servers. 	brief detail
Interface	Interface on which the DHCPv6 request was received.	brief
Client IPv6 Address	Client's IPv6 address.	detail
Client IPv6 Prefix	Client's IPv6 prefix.	detail
Client DUID	Client's DHCP Unique Identifier (DUID).	brief detail
Lease expires	Date and time at which the client's IP address lease expires.	detail

Table 77: show dhcpv6 server binding Output Fields (*continued*)

Field Name	Field Description	Level of Output
Lease expires in	Number of seconds in which lease expires.	detail
Preferred Lease Expires	Date and UTC time at which the client's IPv6 prefix expires.	detail
Preferred Lease Expires in	Number of seconds at which client's IPv6 prefix expires.	detail
Lease Start	Date and time at which the client's address lease was obtained.	detail
Lease time violated	Lease time violation has occurred.	detail
Incoming Client Interface	Client's incoming interface.	detail
Server IP Address	IP address of DHCPv6 server.	detail
Server Interface	Interface of DHCPv6 server.	detail
Client Pool Name	Address pool used to assign IPv6 address.	detail
Client Prefix Pool Name	Address pool used to assign IPv6 prefix.	detail
Client Id length	Length of the DHCPv6 client ID, in bytes.	detail
Client Id	ID of the DHCPv6 client.	detail

Sample Output

show dhcpv6 server binding

```

user@host> show dhcpv6 server binding
Prefix          Session Id Expires State Interface Client DUID
2001:bd8:1111:2222::/64 6 86321 BOUND ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:01
2001:bd8:1111:2222::/64 7 86321 BOUND ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:02
2001:bd8:1111:2222::/64 8 86321 BOUND ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:03
2001:bd8:1111:2222::/64 9 86321 BOUND ge-1/0/0.0
LL_TIME0x1-0x2e159c1-00:10:94:00:00:04
2001:bd8:1111:2222::/64 10 86321 BOUND ge-1/0/0.0
LL_TIME0x1-0x2e159c1-00:10:94:00:00:05
2002::1/74 11 86321 BOUND ge-1/0/0.0
LL_TIME0x1-0x2e159c1-00:10:94:00:00:06

```

show dhcpv6 server binding detail

```

user@host> show dhcpv6 server binding detail

```

```

Session Id: 6
  Client IPv6 Prefix:      2001:bd8:1111:2222::/64
  Client DUID:             LL_TIME0x1-0x2e159c0-00:10:94:00:00:01

  State:
  BOUND(LOCAL_SERVER_STATE_BOUND_ON_INTF_DELETE)
    Lease Expires:         2009-07-21 10:41:15 PDT
    Lease Expires in:      86308 seconds
    Preferred Lease Expires: 2012-07-24 00:18:14 UTC
    Preferred Lease Expires in: 600 seconds
    Lease Start:           2009-07-20 10:41:15 PDT
    Lease time violated:    yes
    Incoming Client Interface: ge-1/0/0.0
    Server Ip Address:       0.0.0.0
    Server Interface:        none
    Client Id Length:        14
    Client Id:
    /0x00010001/0x02e159c0/0x00109400/0x0001

```

```

Session Id: 7
  Client IPv6 Address:      2002::1/128
  Client IPv6 Prefix:      2001:bd8:1111:2222::/64
  Client DUID:             LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

  State:
  BOUND(LOCAL_SERVER_STATE_BOUND_ON_INTF_DELETE)
    Lease Expires:         2009-07-21 10:41:15 PDT
    Lease Expires in:      86308 seconds
    Preferred Lease Expires: 2012-07-24 00:18:14 UTC
    Preferred Lease Expires in: 600 seconds
    Lease Start:           2009-07-20 10:41:15 PDT
    Incoming Client Interface: ge-1/0/0.0
    Server Ip Address:       0.0.0.0
    Client Pool Name:        bos-v6-pool
    Client Prefix Pool Name: bos-v6-prefix-pool
    Client Id Length:        14
    Client Id:
    /0x00010001/0x02e159c0/0x00109400/0x0002

```

show dhcpv6 server binding interface

```

user@host> show dhcpv6 server binding interface ge-1/0/0:10-101
Prefix          Session Id Expires State Interface Client DUID
2001:bd8:1111:2222::/64 1      86055   BOUND   ge-1/0/0.100
LL_TIME0x1-0x4b0a53b9-00:10:94:00:00:01

```

show dhcpv6 server binding interface detail

```

user@host> show dhcpv6 server binding interface ge-1/0/0:10-101 detail
Session Id: 7
  Client IPv6 Prefix:      2001:bd8:1111:2222::/64
  Client DUID:             LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

  State:
  BOUND(bound)
    Lease Expires:         2009-07-21 10:41:15 PDT
    Lease Expires in:      86136 seconds
    Preferred Lease Expires: 2012-07-24 00:18:14 UTC
    Preferred Lease Expires in: 600 seconds
    Lease Start:           2009-07-20 10:41:15 PDT
    Incoming Client Interface: ge-1/0/0.0
    Server Ip Address:       0.0.0.0

```

```

Server Interface:          none
Client Id Length:         14
Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0002

```

show dhcpv6 server binding (IPv6 Prefix)

```

user@host> show dhcpv6 server binding 14/0x00010001/0x02b3be8f/0x00109400/0x0005
detail
Session Id: 7
Client IPv6 Prefix:        2001:bd8:1111:2222::/64
Client DUID:               LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

State:                     BOUND(bound)
Lease Expires:             2009-07-21 10:41:15 PDT
Lease Expires in:          86136 seconds
Preferred Lease Expires:   2012-07-24 00:18:14 UTC
Preferred Lease Expires in: 600 seconds
Lease Start:               2009-07-20 10:41:15 PDT
Incoming Client Interface: ge-1/0/0.0
Server Ip Address:         0.0.0.0
Server Interface:         none
Client Id Length:         14
Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0002

```

show dhcpv6 server binding (Session ID)

```

user@host> show dhcpv6 server binding 8
Prefix          Session Id Expires State Interface Client DUID
2001:DB8::/32  8          86235  BOUND ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:03

```

show dhcpv6 server binding (Interfaces VLAN)

```

user@host> show dhcpv6 server binding ge-1/0/0:100-200
Prefix          Session Id Expires State Interface Client DUID
2001:DB8::/32  11          87583  BOUND ge-1/0/0.1073741827
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:DB9::/32  12          87583  BOUND ge-1/0/0.1073741827
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01

```

show dhcpv6 server binding (Interfaces Wildcard)

```

user@host> show dhcpv6 server binding demux0
Prefix          Session Id Expires State Interface Client DUID
2001:DB8::/32  30          79681  BOUND demux0.1073741824
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:DB9::/32  31          79681  BOUND demux0.1073741825
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:CB9::/32  32          79681  BOUND demux0.1073741826
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01

```

show dhcpv6 server binding (Interfaces Wildcard)

```

user@host> show dhcpv6 server binding ge-1/3/*
Prefix          Session Id Expires State Interface Client DUID
2001:DB8::/32  22          79681  BOUND ge-1/3/0.110
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:DB9::/32  33          79681  BOUND ge-1/3/0.110
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01

```

```
2001:CB9::/32      24      79681    BOUND    ge-1/3/0.110
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
```

show dhcpv6 server binding summary

```
user@host> show dhcpv6 server binding summary
5 clients, (0 init, 5 bound, 0 selecting, 0 requesting, 0 renewing, 0 releasing)
```


show dhcpv6 server statistics

Syntax	show dhcpv6 server statistics <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>>
Release Information	Command introduced in Junos OS Release 9.6.
Description	Display extended Dynamic Host Configuration Protocol for IPv6 (DHCPv6) local server statistics.
Options	<p>logical-system <i>logical-system-name</i>—(Optional) Display information about extended DHCPv6 local server statistics on the specified logical system. If you do not specify a logical system, statistics are displayed for the default logical system.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Display information about extended DHCPv6 local server statistics on the specified routing instance. If you do not specify a routing instance, statistics are displayed for the default routing instance.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear dhcpv6 server statistics on page 1023
List of Sample Output	show dhcpv6 server statistics on page 1118
Output Fields	Table 78 on page 1118 lists the output fields for the show dhcpv6 server statistics command. Output fields are listed in the approximate order in which they appear.

Table 78: show dhcpv6 server statistics Output Fields

Field Name	Field Description
Packets dropped	<p>Number of packets discarded by the extended DHCPv6 local server because of errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.</p> <ul style="list-style-type: none"> • Total—Total number of packets discarded by the extended DHCPv6 local server • Strict Reconfigure—Number of solicit messages discarded because the client does not support reconfiguration • Bad hardware address—Number of packets discarded because an invalid hardware address was specified • Bad opcode—Number of packets discarded because an invalid operation code was specified • Bad options—Number of packets discarded because invalid options were specified • Invalid server address—Number of packets discarded because an invalid server address was specified • Lease Time Violation—Number of packets discarded because of a lease time violation • No available addresses—Number of packets discarded because there were no addresses available for assignment • No interface match—Number of packets discarded because they did not belong to a configured interface • No routing instance match—Number of packets discarded because they did not belong to a configured routing instance • No valid local address—Number of packets discarded because there was no valid local address • Packet too short—Number of packets discarded because they were too short • Read error—Number of packets discarded because of a system read error • Send error—Number of packets that the extended DHCPv6 local server could not send
Messages received	<p>Number of DHCPv6 messages received.</p> <ul style="list-style-type: none"> • DHCPV6_CONFIRM—Number of DHCPv6 CONFIRM PDUs received. • DHCPV6_DECLINE—Number of DHCPv6 DECLINE PDUs received. • DHCPV6_INFORMATION_REQUEST—Number of DHCPv6 INFORMATION-REQUEST PDUs received. • DHCPV6_REBIND—Number of DHCPv6 REBIND PDUs received. • DHCPV6_RELAY_FORW—Number of DHCPv6 RELAY-FORW PDUs received. • DHCPV6_RELAY_REPL—Number of DHCPv6 RELAY-REPL PDUs received. • DHCPV6_RELEASE—Number of DHCPv6 RELEASE PDUs received. • DHCPV6_RENEW—Number of DHCPv6 RENEW PDUs received. • DHCPV6_REQUEST—Number of DHCPv6 REQUEST PDUs received. • DHCPV6_SOLICIT—Number of DHCPv6 SOLICIT PDUs received.
Messages sent	<p>Number of DHCPv6 messages sent.</p> <ul style="list-style-type: none"> • DHCPV6_ADVERTISE—Number of DHCPv6 ADVERTISE PDUs transmitted. • DHCPV6_REPLY—Number of DHCPv6 ADVERTISE PDUs transmitted. • DHC6_RECONFIGURE—Number of DHCPv6 RECONFIGURE PDUs transmitted.

Sample Output

show dhcpv6 server statistics

```
user@host> show dhcpv6 server statistics
```

Dhcpv6 Packets dropped:

Total	1
Lease Time Violation	1

Messages received:

DHCPV6_DECLINE	0
DHCPV6_SOLICIT	9
DHCPV6_INFORMATION_REQUEST	0
DHCPV6_RELEASE	0
DHCPV6_REQUEST	5
DHCPV6_CONFIRM	0
DHCPV6_RENEW	0
DHCPV6_REBIND	0
DHCPV6_RELAY_FORW	0
DHCPV6_RELAY_REPL	0

Messages sent:

DHCPV6_ADVERTISE	9
DHCPV6_REPLY	5
DHCPV6_RECONFIGURE	0

show diameter

Syntax	show diameter <brief detail summary>
Release Information	Command introduced in Junos OS Release 9.6.
Description	Display information about the Diameter node.
Options	brief detail summary —(Optional) Display the specified level of output. The summary output is displayed by default and includes Diameter node status. The brief output adds summary information about functions, instances, network elements, and peers. The detail output adds summary information about routes.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear diameter function statistics on page 1024 • clear diameter peer on page 1025 • show diameter function on page 1126 • show diameter instance on page 1133 • show diameter network-element on page 1135 • show diameter peer on page 1141 • show diameter route on page 1153
List of Sample Output	show diameter brief on page 1123 show diameter detail on page 1124 show diameter summary on page 1124
Output Fields	Table 79 on page 1120 lists the output fields for the show diameter command. Output fields are listed in the approximate order in which they appear.

Table 79: show diameter Output Fields

Field Name	Field Description	Level of Output
Diameter process id	ID number of the Diameter process.	All levels
Functions	Number of functions associated with Diameter.	All levels
Connected functions	Number of functions with active Diameter connections.	All levels
Instances	Number of configured Diameter instances.	All levels

Table 79: show diameter Output Fields (*continued*)

Field Name	Field Description	Level of Output
Network elements (NEs)	Number of configured Diameter network elements.	All levels
Connected NEs	Number of Diameter network elements with active connections.	All levels
Peers	Number of Diameter peer nodes.	All levels
Activated peers	Number of Diameter peers with active connections.	All levels
Open peers	Number of peers in the open state, without active network element connections but available for a connection.	All levels
Transports	Number of transports configured.	All levels
Requests queued for network transmit	Number of requests waiting to be sent to the Diameter peers.	All levels
Answers queued for network transmit	Number of replies waiting to be sent to the Diameter peers.	All levels
Expected answers from network	Number of replies expected to be received from the Diameter peers.	All levels
Requests queued for function transmit	Number of requests waiting to be sent to the functions associated with Diameter.	All levels
Answers queued for function transmit	Number of replies waiting to be sent to the functions associated with Diameter.	All levels
Expected answers from functions	Number of replies expected to be received from the functions associated with Diameter.	All levels
Memory used by network transmit queues	Amount of memory consumed by network transmit queues.	All levels
Memory used by function transmit queues	Amount of memory consumed by function transmit queues.	All levels
Origin-state-id	Value of the Origin-State-ID AVP.	All levels
Function	Name of the function for which information is displayed.	brief detail
State	State of the Diameter connection with the function: Connected or Disconnec (disconnected).	brief detail

Table 79: show diameter Output Fields (*continued*)

Field Name	Field Description	Level of Output
Upstream Transaction Utilization	Percent of upstream traffic used for this function.	brief detail
Downstream Transaction Utilization	Percent of downstream traffic used for this function.	brief detail
Net Queue Buffer Utilization	Percent of network transmission buffer used for this function.	brief detail
Func Queue Buffer Utilization	Percent of function transmission buffer used for this function.	brief detail
Routed Dests	Number of destinations that have this function associated with their routes.	brief detail
Name	Name of the Diameter instance.	brief detail
Origin-Realm	Value of Origin-Realm attribute-value pair (AVP).	brief detail
Origin Host	Value of Origin-Host AVP.	brief detail
NE-Total	Number of configured network elements.	brief detail
NE-Connected	Number of network elements with active Diameter connections.	brief detail
Name	Name of the Diameter network element.	brief detail
Instance	Name of the Diameter instance in which the network element is configured.	brief detail
State	State of the network element: <ul style="list-style-type: none"> Connecting—None of the network element peers are in the open state and available for connection. Selecting—One network element peer is connected and the network element is waiting for another peer to reach the open state so that it can be connected. Partially-Connected—One network element peer is in the open state and connected. Post-selection-delay—Three or more peers are in the open state and the network element is waiting to deactivate the peers in excess of two. Fully-connected—Two network element peers are in the open state and connected. 	brief detail
Primary Peer	Primary peer for the network element, based on the configured peer priority.	brief detail
Secondary Peer	Secondary peer for the network element, based on the configured peer priority.	brief detail
Peer	Name of the peer.	brief detail

Table 79: show diameter Output Fields (*continued*)

Field Name	Field Description	Level of Output
Instance	Name of the Diameter instance in which the peer is configured.	brief detail
State	State of the peer: <ul style="list-style-type: none"> • Bad-Config—Misconfiguration. • Bad-Remote—Remote side does not conform to one of the decisions or is sending malformed messages. • Closed—Normal disconnect due to a request from the remote site or due to excessive watchdog timeouts. • Destructing—Peer to be deleted on the next timer tick. Until then, it performs no actions. • Disabled—Peer is administratively disabled. • Internal-error—Internal error has been detected and the peer is in the process of restarting. • No-Activation—Peer is not used by any Diameter network element. • Rejected—Connection was rejected by remote side of the connection. • Suspended—All other reasons to be suspended. 	brief detail
NE-Count	Number of network elements associated with the peer.	brief detail
Activated Count	Activation status of the peer: <ul style="list-style-type: none"> • 1—Peer is activated. • 0—Peer is not activated. 	brief detail
Primary Count	Status of the peer: primary (1) or secondary (0).	brief detail
Secondary Count	Status of the peer: secondary (0) or primary (1).	brief detail
Route	Name of the Diameter route.	detail
NE	Name of the Diameter network element in which the route is configured	detail
Instance	Name of the Diameter instance in which the route is configured.	detail
Valid	Determination of whether the route is valid: yes or no .	detail
Up	State of the route: yes for an active route, no for an inactive route.	detail

Sample Output

show diameter brief

```
user@host> show diameter brief
```

```
Diameter node:
Diameter process id      :    1446
Functions                 :      4
Connected functions      :      2
```

```

Instances                               : 1
Network elements(NEs)                  : 1
Connected NEs                           : 0
Peers                                   : 2
Activated peers                         : 1
Open peers                             : 0
Transports                             : 1
Requests queued for network transmit   : 0
Answers queued for network transmit     : 0
Expected answers from network           : 0
Requests queued for function transmit   : 0
Answers queued for function transmit     : 0
Expected answers from functions         : 0
Memory used by network transmit queues  : 0
Memory used by function transmit queues : 0
Origin-state-id                        : 0

```

Diameter function list:

Function	State	Upstream Transaction Utilization %	Downstream Transaction Utilization %	Net Queue Buffer Utilization %	Func Queue Buffer Utilization %	Routed Dests
charging-	Disconnec	0	0	0	0	0
gx-plus	Connected	0	0	0	0	1
jsrc	Connected	0	0	0	0	0
packet-tr	Disconnec	0	0	0	0	0

Diameter instances:

Name	Origin-Realm	Origin-Host	NE-Total	NE-Connected
master	orrr	ohhh	1	0

Diameter network-elements:

Name	Instance	State	Primary Peer	Secondary Peer
n0	master	Connecting	<NONE>	<NONE>

Diameter peer list:

Peer	Instance	State	NE-Count	Activated Count	Primary Count	Secondary Count
p0	master	Suspended	1	1	0	0
p100	master	No-Activation	0	0	0	0

show diameter detail

```
user@host> show diameter detail
```

```
...
```

Diameter routes:

Route	NE	Instance	Valid	Up
dne-route1	dne1	master	yes	no

show diameter summary

```
user@host> show diameter summary
```

Diameter node:

```

Diameter process id      : 1446
Functions                 : 4
Connected functions       : 2
Instances                 : 1
Network elements(NEs)    : 1
Connected NEs             : 0
Peers                     : 2

```


Activated peers	:	1
Open peers	:	0
Transports	:	1
Requests queued for network transmit	:	0
Answers queued for network transmit	:	0
Expected answers from network	:	0
Requests queued for function transmit	:	0
Answers queued for function transmit	:	0
Expected answers from functions	:	0
Memory used by network transmit queues	:	0
Memory used by function transmit queues	:	0
Origin-state-id	:	0

show diameter function

Syntax	show diameter function <brief detail summary> <function-name>
Release Information	Command introduced in Junos OS Release 9.6. Support for PTSP introduced in Junos OS Release 10.2. Support for Gx-Plus introduced in Junos OS Release 11.2.
Description	Display information about all functions associated with Diameter instances or only the specified function.
Options	<p>brief detail summary—(Optional) Display the specified level of output. The summary output is displayed by default and includes basic function information. The brief output displays the summary information in a different format. The detail output adds information to the brief output.</p> <p>function-name—(Optional) Display information for only the specified function. Currently, Gx-Plus, JSRC, and packet-triggered-subscribers are supported functions.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear diameter function statistics on page 1024 • show diameter on page 1120 • show diameter function statistics on page 1130
List of Sample Output	show diameter function on page 1128 show diameter function brief on page 1128 show diameter function detail (JSRC) on page 1128 show diameter function detail (Gx-Plus) on page 1129
Output Fields	Table 80 on page 1126 lists the output fields for the show diameter function command. Output fields are listed in the approximate order in which they appear.

Table 80: show diameter function Output Fields

Field Name	Field Description	Level of Output
Function name	Name of the function for which information is displayed.	All levels
State	State of the Diameter connection with the function.	All levels
Upstream transaction utilization	Percent of upstream traffic used for this function.	All levels

Table 80: show diameter function Output Fields (*continued*)

Field Name	Field Description	Level of Output
Downstream transaction utilization	Percent of downstream traffic used for this function.	All levels
Network transmit buffer utilization	Percent of network transmission buffer used for this function.	All levels
Function transmit buffer utilization	Percent of function transmission buffer used for this function.	All levels
Routed destinations	Number of destinations that have this function associated with their routes.	All levels
Requests queued for network tx	Number of requests waiting to be sent to the Diameter peers for this function.	detail
Pending answers from network	Number of replies expected from the Diameter peers for this function.	detail
Answers queued for function tx	Number of replies waiting to be sent to this function.	detail
Total upstream transactions pending	Total number of messages queued for this function.	detail
Upstream transactions limit	Total number of messages queued for this function.	detail
Requests queued for function tx	Number of requests waiting to be sent to this function.	detail
Pending answers from function	Number of replies expected to be received from this function.	detail
Answers queued for network tx	Number of replies waiting to be sent to this function.	detail
Total downstream transactions pending	Total number of messages queued for the Diameter peers.	detail
Downstream transactions limit	Maximum number of messages that can be queued for the Diameter peers.	detail
Buffers used by network tx queue	Number of buffers used by messages queued for the Diameter peers.	detail
Limit on network tx queue buffers	Maximum buffer capacity available for messages queued for the Diameter peers.	detail

Table 80: show diameter function Output Fields (*continued*)

Field Name	Field Description	Level of Output
Buffers used by function tx queue	Number of buffers used by messages queued for this function.	detail
Limit on function tx queue buffers	Maximum buffer capacity available for messages queued for this function.	detail
Origin-state-id	Value of the Origin-State-ID AVP.	detail

Sample Output

show diameter function

```
user@host> show diameter function
```

```
Diameter function list:
```

Function	State	Upstream Transaction Utilization %	Downstream Transaction Utilization %	Net Queue Buffer Utilization %	Func Queue Buffer Utilization %	Routed Dests
jsrc	Disconnect	0	0	0	0	0

show diameter function brief

```
user@host> show diameter function brief
```

```
Diameter function:
```

```
Function name           : gx-plus
State                   : Connected
Upstream transaction utilization : 0 %
Downstream transaction utilization : 0 %
Network transmit buffer utilization : 0 %
Function transmit buffer utilization : 0 %
Routed destinations     : 1

Function name           : jsrc
State                   : Disconnected
Upstream transaction utilization : 0 %
Downstream transaction utilization : 0 %
Network transmit buffer utilization : 0 %
Function transmit buffer utilization : 0 %
Routed destinations     : 0
```

show diameter function detail (JSRC)

```
user@host> show diameter function detail
```

```
Diameter function:
```

```
Function name           : jsrc
State                   : Disconnected
Upstream transaction utilization : 0 %
Downstream transaction utilization : 0 %
Network transmit buffer utilization : 0 %
```

```

Function transmit buffer utilization : 0 %
Routed destinations                 : 0
Requests queued for network tx      : 0
Pending answers from network        : 0
Answers queued for function tx       : 0
Total upstream transactions pending  : 0
Upstream transactions limit          : 1024
Requests queued for function tx      : 0
Pending answers from function        : 0
Answers queued for network tx        : 0
Total downstream transactions pending : 0
Downstream transactions limit        : 1024
Buffers used by network tx queue     : 0
Limit on network tx queue buffers    : 10485760
Buffers used by function tx queue    : 0
Limit on function tx queue buffers   : 10485760

```

show diameter function detail (Gx-Plus)

```
user@host> show diameter function gx-plus detail
```

```

Diameter function:
Function name           : gx-plus
State                   : Connected
Upstream transaction utilization : 0 %
Downstream transaction utilization : 0 %
Network transmit buffer utilization : 0 %
Function transmit buffer utilization : 0 %
Routed destinations     : 1
Requests queued for network tx : 0
Pending answers from network : 0
Answers queued for function tx : 0
Total upstream transactions pending : 0
Upstream transactions limit : 1024
Requests queued for function tx : 0
Pending answers from function : 0
Answers queued for network tx : 0
Total downstream transactions pending : 0
Downstream transactions limit : 1024
Buffers used by network tx queue : 0
Limit on network tx queue buffers : 10485760
Buffers used by function tx queue : 0
Limit on function tx queue buffers : 10485760
Origin-state-id         : 0

```

show diameter function statistics

Syntax	show diameter function statistics <brief detail summary> <function-name>
Release Information	Command introduced in Junos OS Release 9.6. Support for PTSP introduced in Junos OS Release 10.2. Support for Gx-Plus introduced in Junos OS Release 11.2.
Description	Display statistics about all functions associated with Diameter instances or only the specified function.
Options	<p>brief detail summary—(Optional) Display the specified level of output. The summary output is displayed by default and includes basic function statistics. The brief output displays the summary information in a different format and adds numbers accumulated since the Diameter node was started. The detail output adds information to the brief output.</p> <p>function-name—(Optional) Display information for only the specified function. Currently, Gx-Plus, JSRC, and packet-triggered-subscribers are supported functions. When you specify a function, the brief output is displayed by default, even when you explicitly specify summary.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear diameter function statistics on page 1024 • show diameter on page 1120 • show diameter function on page 1126
List of Sample Output	show diameter function statistics on page 1132 show diameter function statistics brief on page 1132 show diameter function statistics detail on page 1132
Output Fields	Table 81 on page 1130 lists the output fields for the show diameter function statistics command. Output fields are listed in the approximate order in which they appear.

Table 81: show diameter function statistics Output Fields

Field Name	Field Description	Level of Output
Function	Name of the function for which information is displayed.	All levels
Delivered Requests	Number of requests delivered by Diameter to the application.	All levels
Delivered Answers	Number of answers delivered by Diameter to the application.	All levels
Delivered Messages	Total number of messages delivered by Diameter to the application.	All levels

Table 81: show diameter function statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
Forwarded Requests	Number of requests sent by Diameter to the network.	All levels
Forwarded Answers	Number of answers sent by Diameter to the network.	All levels
Forwarded Messages	Number of messages sent by Diameter to the network.	All levels
Function name	Name of the function for which information is displayed.	All levels
Over-limit network requests	Number of requests sent to Diameter peers that exceeded the limit on the network transmit queue.	detail
Over-limit network answers	Number of answers sent to Diameter peers that exceeded the limit on the network transmit queue.	detail
Over-limit network messages	Total number of messages sent to Diameter peers that exceeded the limit on the network transmit queue.	detail
Failed to deliver requests	Number of requests sent by Diameter to its application that were not successfully delivered.	detail
Failed to deliver answers	Number of answers sent by Diameter to its application that were not successfully delivered.	detail
Failed to deliver messages	Total number of messages sent by Diameter to its application that were not successfully delivered.	detail
Over-limit function requests	Number of requests sent to Diameter peers that exceeded the limit on the function transmit queue.	detail
Over-limit function answers	Number of answers sent to Diameter peers that exceeded the limit on the function transmit queue.	detail
Over-limit function messages	Total number of messages sent to Diameter peers that exceeded the limit on the function transmit queue.	detail
Failed to forward requests	Number of requests that were not successfully sent by Diameter to the network.	detail
Failed to forward answers	Number of answers that were not successfully sent by Diameter to the network.	detail
Failed to forward messages	Total number of messages that were not successfully sent by Diameter to the network.	detail

Sample Output

show diameter function statistics

```
user@host> show diameter function statistics
Diameter function statistics:
      Delivered Delivered Delivered Forwarded Forwarded Forwarded
Function Requests Answers Messages Requests Answers Messages
jsrc           0         0         0         0         0         0
```

show diameter function statistics brief

```
user@host> show diameter function statistics brief

Diameter function statistics:
Function name           : jsrc

Delivered requests      :          0          0
Delivered answers       :          0          0
Delivered messages      :          0          0
Forwarded requests      :          0          0
Forwarded answers       :          0          0
Forwarded messages      :          0          0
```

show diameter function statistics detail

```
user@host> show diameter function statistics detail

Diameter function statistics:
Function name           : jsrc

Delivered requests      :          0          0
Delivered answers       :          0          0
Delivered messages      :          0          0
Forwarded requests      :          0          0
Forwarded answers       :          0          0
Forwarded messages      :          0          0
Over-limit network requests :          0          0
Over-limit network answers :          0          0
Over-limit network messages :          0          0
Failed to deliver requests :          0          0
Failed to deliver answers  :          0          0
Failed to deliver messages :          0          0
Over-limit function requests :          0          0
Over-limit function answers :          0          0
Over-limit function messages :          0          0
Failed to forward requests :          0          0
Failed to forward answers  :          0          0
Failed to forward messages :          0          0
```


show diameter instance

Syntax	show diameter instance <brief detail summary> <instance-name>
Release Information	Command introduced in Junos OS Release 9.6.
Description	Display information about all Diameter instances or only the specified instance.
Options	<p>brief detail summary—(Optional) Display the specified level of output. The summary output is displayed by default and includes basic instance information. The brief output displays the summary information in a different format. The detail output is the same as the brief output.</p> <p>instance-name—(Optional) Display information for only the specified Diameter instance.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show diameter on page 1120
List of Sample Output	<p>show diameter instance on page 1134</p> <p>show diameter instance detail on page 1134</p>
Output Fields	Table 82 on page 1133 lists the output fields for the show diameter instance command. Output fields are listed in the approximate order in which they appear.

Table 82: show diameter instance Output Fields

Field Name	Field Description	Level of Output
name	Name of the Diameter instance.	summary
Origin-realm	Value of Origin-Realm AVP.	summary
Origin-host	Value of Origin-Host AVP.	summary
NE-total	Total number of network elements configured for this instance.	summary
NE-connected	Number of network elements with active Diameter connections.	summary
Instance name	Name of the Diameter instance.	brief detail
Origin realm	Value of Origin-Realm AVP.	brief detail
Origin host	Value of Origin-Host AVP.	brief detail
NEs	Total number of network elements configured for this instance.	brief detail

Table 82: show diameter instance Output Fields (*continued*)

Field Name	Field Description	Level of Output
Connected NEs	Number of network elements with active Diameter connections.	brief detail

Sample Output

show diameter instance

```
user@host> show diameter instance
```

```
Diameter instances:
  Name      Origin-Realm  Origin-Host  NE-Total  NE-Connected
  master    rrrr         hhhh        1         1
```

show diameter instance detail

```
user@host> show diameter instance detail
```

```
Diameter instance:
  Instance name : master

  Origin realm  : rrrr

  Origin host   : hhhh

  NEs           : 1
  Connected NEs : 1
```

show diameter network-element

Syntax	show diameter network-element <brief detail summary> <element-name>
Release Information	Command introduced in Junos OS Release 9.6.
Description	Display information about all Diameter network elements or only the specified network element.
Options	<p>brief detail summary—(Optional) Display the specified level of output. The summary output is displayed by default and includes basic network element information. The brief output displays the summary information in a different format. The detail output adds information to the brief output.</p> <p>element-name—(Optional) Display information for only the specified network element.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show diameter on page 1120 • show diameter function on page 1126 • show diameter network-element map on page 1138 • show diameter peer on page 1141 • show diameter route on page 1153
List of Sample Output	<p>show diameter network-element on page 1136</p> <p>show diameter network-element detail on page 1137</p>
Output Fields	Table 83 on page 1135 lists the output fields for the show diameter network-element command. Output fields are listed in the approximate order in which they appear.

Table 83: show diameter network-element Output Fields

Field Name	Field Description	Level of Output
Name	Name of the Diameter network element.	summary
Instance	Name of the Diameter instance in which the network element is configured.	summary

Table 83: show diameter network-element Output Fields (*continued*)

Field Name	Field Description	Level of Output
State	State of the network element: <ul style="list-style-type: none"> Connecting—None of the network element peers are in the open state and available for connection. Selecting—One network element peer is connected and the network element is waiting for another peer to reach the open state so that it can be connected. Partially-Connected—One network element peer is in the open state and connected. Post-selection-delay—Three or more peers are in the open state and the network element is waiting to deactivate the peers in excess of two. Fully-connected—Two network element peers are in the open state and connected. 	All levels
Primary peer	Primary peer for the network element, based on the configured peer priority.	All levels
Secondary peer	Secondary peer for the network element, based on the configured peer priority.	All levels
NE name	Name of the Diameter network element.	brief detail
Instance name	Name of the Diameter instance in which the network element is configured.	brief detail
Peers	Number of configured peers.	brief detail
Activated peers	Number of peers that have been activated.	brief detail
Open peers	Number of peers in the open state, without active network element connections but available for a connection.	brief detail
Routes	Number of routes configured for the network element.	brief detail
Invalid routes	Number of routes that are invalid because they lack one or more of the following: application and partition, Diameter instance, or destination realm.	brief detail
Activation delay	Period in milliseconds between peer activations by the network element.	brief detail
First selection delay	Period in milliseconds that the network element waited after connecting to the first peer to allow other peers to reach the open state.	brief detail
Postselection delay	Period in milliseconds that the network element waited after having two peers in the open state before deactivating all lower-priority peers.	brief detail

Sample Output

show diameter network-element

```
user@host> show diameter network-element
```

```
Diameter network-elements:
```

```
Primary      Secondary
```

Name	Instance	State	Peer	Peer
ne0	master	Fully-connected	p0	p1

show diameter network-element detail

```
user@host> show diameter network-element detail
```

Diameter network-element:

NE name : ne0

Instance name : master

State : Fully-connected

Primary peer : p0

Secondary peer : p1

Peers : 5

Activated peers : 4

Open peers : 2

Routes : 1

Invalid routes : 0

Activation delay : 10000 ms

First selection delay : 0 ms

Post selection delay : 30000 ms

show diameter network-element map

Syntax	show diameter network-element map <brief detail summary> <element-name>
Release Information	Command introduced in Junos OS Release 9.6.
Description	Display network-element-to-peer mapping information for all Diameter network elements or only the specified network element.
Options	<p>brief detail summary—(Optional) Display the specified level of output. The summary output is displayed by default. The brief output and detail output display the summary information in a different format.</p> <p>element-name—(Optional) Display information for only the specified network element.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show diameter on page 1120 • show diameter network-element on page 1135
List of Sample Output	<p>show diameter network-element map on page 1139</p> <p>show diameter network-element map detail on page 1139</p>
Output Fields	Table 84 on page 1138 lists the output fields for the show diameter network-element map command. Output fields are listed in the approximate order in which they appear.

Table 84: show diameter network-element map Output Fields

Field Name	Field Description	Level of Output
Name	Name of the Diameter network element.	summary
Instance	Name of the Diameter instance in which the network element is configured.	summary
Peer	Name of the peer.	All levels
Priority	Priority configured for the peer. A lower number indicates a higher priority.	All levels
State	State of the peer: <ul style="list-style-type: none"> • Activated—Peer has been activated (selected) by the network element. • Not-Activated—Peer has not been selected by the network element. • Primary—Peer that is connected to the network element and has the higher priority of the two connected peers. • Secondary—Peer that is connected to the network element and has the lower priority of the two connected peers. 	summary
NE name	Name of the Diameter network element.	brief detail

Table 84: show diameter network-element map Output Fields (*continued*)

Field Name	Field Description	Level of Output
Instance name	Name of the Diameter instance in which the network element is configured.	brief detail
Usage	State of the peer: <ul style="list-style-type: none"> Activated—Peer has been activated (selected) by the network element. Not-Activated—Peer has not been selected by the network element. Primary—Peer that is connected to the network element and has the higher priority of the two connected peers. Secondary—Peer that is connected to the network element and has the lower priority of the two connected peers. 	brief detail

Sample Output

show diameter network-element map

```
user@host> show diameter network-element map
```

```
Diameter network-element peers:
  Name      Instance  Peer      Priority  State
  ne0       master    p288      30       Activated
  ne0       master    p0        20       Primary
  ne0       master    pA        15       Activated
  ne0       master    p1        10       Secondary
  ne0       master    pB        5       Not-Activated
```

show diameter network-element map detail

```
user@host> show diameter network-element map detail
```

```
Diameter network-element peers:
  NE name      : ne0

  Instance name : master

  Peer          : p288

  Priority      :      30
  Usage        : Activated

  NE name      : ne0

  Instance name : master

  Peer          : p0

  Priority      :      20
  Usage        : Primary

  NE name      : ne0

  Instance name : master

  Peer          : pA
```

Priority	:	15
Usage	:	Activated
NE name	:	ne0
Instance name	:	master
Peer	:	p1
Priority	:	10
Usage	:	Secondary
NE name	:	ne0
Instance name	:	master
Peer	:	pB
Priority	:	5
Usage	:	Not-Activated

show diameter peer

Syntax	<code>show diameter peer</code> <code><brief detail summary></code> <code><peer-name></code>
Release Information	Command introduced in Junos OS Release 9.6.
Description	Display information about all peers associated with Diameter instances or only the specified peer.
Options	<p>brief detail summary—(Optional) Display the specified level of output. The summary output is displayed by default and includes basic peer information. The brief output displays the summary information in a different format. The detail output adds information to the brief output.</p> <p>peer-name—(Optional) Display information for only the specified peer.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear diameter peer on page 1025 • show diameter on page 1120 • show diameter peer map on page 1146 • show diameter peer statistics on page 1149
List of Sample Output	<p>show diameter peer on page 1143</p> <p>show diameter peer detail on page 1144</p>
Output Fields	Table 85 on page 1141 lists the output fields for the show diameter peer command. Output fields are listed in the approximate order in which they appear.

Table 85: show diameter peer Output Fields

Field Name	Field Description	Level of Output
Peer	Name of the peer.	brief summary
Instance	Name of the Diameter instance in which the peer is configured.	brief summary

Table 85: show diameter peer Output Fields (*continued*)

Field Name	Field Description	Level of Output
State	State of the peer: <ul style="list-style-type: none"> • Bad-Config—Misconfiguration. • Bad-Remote—Remote side does not conform to one of the decisions or is sending malformed messages. • Closed—Normal disconnect due to a request from the remote site or due to excessive watchdog timeouts. • Destructing—Peer to be deleted on the next timer tick; until then, it performs no actions. • Disabled—Peer is administratively disabled. • Internal-error—Internal error has been detected and the peer is in the process of restarting. • No-Activation—Peer is not used by any Diameter network element. • Rejected—Connection was rejected by remote side of the connection. • Reopen—Connection has been unexpectedly closed and Diameter is attempting to reopen the connection. • Suspended—All other reasons to be suspended. 	All levels
NE-Count	Number of network elements associated with the peer.	brief summary
Activated Count	Activation status of the peer: <ul style="list-style-type: none"> • 1—Peer is activated. • 0—Peer is not activated. 	All levels
Primary Count	Status of the peer, primary (1) or secondary (0).	All levels
Secondary Count	Secondary (0) versus Primary (1) status of the peer.	All levels
Peer name	Name of the peer.	detail
NEs	Number of network elements associated with the peer.	detail
Vrf	Logical system:routing instance of the configuration.	detail
Remote address	Remote IP address of the peer.	detail
Remote port	Remote port on the peer on which the connection is made.	detail
Remote end origin realm	Name of the realm of the Diameter node that originates messages to the peer.	detail
Remote end origin host	Name of the host of the Diameter node that originates messages to the peer.	detail
Local address	Local IP address on the Diameter origin node.	detail
Local port	Local port on the Diameter origin node.	detail

Table 85: show diameter peer Output Fields (*continued*)

Field Name	Field Description	Level of Output
Local transport	Number of transports configured.	detail
Time since last enable	Period since peer was enabled in <i>hh:mm:ss</i> format.	detail
In state time	Period that peer has been in present state in <i>hh:mm:ss</i> format.	detail
Remaining in state time	Period that peer will remain in present state in <i>hh:mm:ss</i> format.	detail
Missing wd events	Number of missed watchdog events.	detail
Tx queue length	Number of messages in the transmit queue.	detail
Answer waiting count	Number of answers on which the peer is waiting.	detail
Time since last rx	Number of milliseconds since the last message was received by the peer.	detail
Time until wd timeout	Time remaining until next watchdog event.	detail
Operation timeout	Watchdog timeout period.	detail
Suspended timeout base	Base timeout period in suspended states (suspended, rejected, bad-remonte, bad-config). This timeout doubles after each consecutive suspension, until the maximum value of 600 seconds is reached.	detail
Closed timeout	Timeout period in normal closed state, such as when an external peer requested a disconnect.	detail
Connection timeout	Timeout period for establishing a connection.	detail
Waiting origin state id	Whether the peer is waiting for the Origin-State-Id AVP, yes or no .	detail

Sample Output

show diameter peer

```
user@host> show diameter peer
```

```
Diameter peer list:
```

Peer	Instance	State	NE-Count	Activated Count	Primary Count	Secondary Count
p0	master	I-Open	1	1	1	0
p1	master	I-Open	1	1	0	1
p288	master	Suspended	1	1	0	0
pA	master	Suspended	1	1	0	0
pB	master	No-Activation	1	0	0	0

pc	master	No-Activation	0	0	0	0
pd	master	No-Activation	0	0	0	0

show diameter peer detail

```
user@host> show diameter peer detail
```

```
Diameter peer:
Peer name       : p0
State           : I-Open
NEs             : 1
Activated count : 1
Primary count   : 1
Secondary count : 0
Vrf             : default:master
Remote address  : 10.10.5.28
Remote port     : 62917
Remote end origin realm : rrrrA
Remote end origin host : hhhhA
Local address   : 10.6.128.155
Local port      : 57095
Local transport : <NO-TRANSPORT>
Time since last enable : 08:56.200
In state time   : 08:56.200
Remaining in state time : no limit
Missed wd events : 0
Tx queue length : 0
Answer waiting count : 0
Time since last rx : 2200 ms
Time until wd timeout : 3800 ms
Operation timeout : 6000 ms
Suspended timeout base : 30000 ms
Closed timeout   : 30000 ms
Connection timeout : 6000 ms
Waiting origin state id : no

Peer name       : p1
State           : I-Open
NEs             : 1
Activated count : 1
Primary count   : 0
Secondary count : 1
Vrf             : default:master
Remote address  : 10.10.5.28
Remote port     : 58490
Remote end origin realm : rrrrA
Remote end origin host : hhhhB
Local address   : 10.6.128.155
Local port      : 49293
Local transport : <NO-TRANSPORT>
Time since last enable : 08:56.200
In state time   : 08:36.000
Remaining in state time : no limit
Missed wd events : 0
Tx queue length : 0
Answer waiting count : 0
Time since last rx : 0 ms
Time until wd timeout : 6000 ms
Operation timeout : 6000 ms
Suspended timeout base : 30000 ms
```

```
Closed timeout      :      30000 ms
Connection timeout  :      6000 ms
Waiting origin state id : no
```

show diameter peer map

Syntax	show diameter peer map <brief detail summary> <peer-name>
Release Information	Command introduced in Junos OS Release 9.6.
Description	Display peer-to-network-element mapping information for all peers associated with Diameter instances or with the specified peer.
Options	<p>brief detail summary—(Optional) Display the specified level of output. The summary output is displayed by default and includes basic peer information. The brief output displays the summary information in a different format. The detail output adds information to the brief output.</p> <p>peer-name—(Optional) Display mapping information for only the specified peer.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear diameter peer on page 1025 • show diameter on page 1120 • show diameter peer on page 1141 • show diameter peer statistics on page 1149
List of Sample Output	<p>show diameter peer map on page 1147</p> <p>show diameter peer map detail on page 1147</p>
Output Fields	Table 86 on page 1146 lists the output fields for the show diameter peer map command. Output fields are listed in the approximate order in which they appear.

Table 86: show diameter peer map Output Fields

Field Name	Field Description	Level of Output
Peer	Name of the peer.	All levels
Instance	Name of the Diameter instance in which the network element is configured.	All levels
NE	Name of the Diameter network element.	All levels
Priority	Priority configured for the peer. A lower number indicates a higher priority.	All levels

Table 86: show diameter peer map Output Fields (*continued*)

Field Name	Field Description	Level of Output
State	State of the peer: <ul style="list-style-type: none"> Activated—Peer has been activated (selected) by the network element. Not-Activated—Peer has not been selected by the network element. Primary—Peer that is connected to the network element and has the higher priority of the two connected peers. Secondary—Peer that is connected to the network element and has the lower priority of the two connected peers. 	All levels
Instance name	Name of the Diameter instance in which the network element is configured.	brief detail
NE name	Name of the Diameter network element.	brief detail
Usage	Role of the peer for the network element, Primary or Secondary .	brief detail

Sample Output

show diameter peer map

```
user@host> show diameter peer map
```

```
Diameter peer usage by network elements:
```

Peer	Instance	NE	Priority	State
p0	master	ne0	20	Primary
p1	master	ne0	10	Secondary
p288	master	ne0	30	Activated
pA	master	ne0	15	Activated
pB	master	ne0	5	Not-Activated

show diameter peer map detail

```
user@host> show diameter peer map detail
```

```
Diameter network-element peers:
```

```
Peer                : p0

Instance name       : master

NE name             : ne0

Priority             :      20
Usage               : Primary

Peer                : p1

Instance name       : master

NE name             : ne0

Priority             :      10
Usage               : Secondary

Peer                : p288
```

```
Instance name      : master
NE name            : ne0
Priority            :      30
Usage              : Activated
Peer               : pA
Instance name      : master
NE name            : ne0
Priority            :      15
Usage              : Activated
Peer               : pB
Instance name      : master
NE name            : ne0
Priority            :       5
Usage              : Not-Activated
```


show diameter peer statistics

Syntax	show diameter peer statistics <brief detail summary> <peer-name>
Release Information	Command introduced in Junos OS Release 9.6.
Description	Display statistics about all peers associated with Diameter instances or only the specified peer.
Options	<p>brief detail summary—(Optional) Display the specified level of output. The summary output is displayed by default and includes basic function statistics. The brief output displays the summary information in a different format and adds numbers accumulated since the peer was connected. The detail output adds information to the brief output.</p> <p>peer-name—(Optional) Display information for only the specified peer. When you specify a peer, the brief output is displayed by default, even when you explicitly specify summary.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear diameter peer on page 1025 • show diameter on page 1120 • show diameter peer on page 1141 • show diameter peer map on page 1146
List of Sample Output	show diameter peer statistics on page 1150 show diameter peer statistics detail on page 1150
Output Fields	Table 87 on page 1149 lists the output fields for the show diameter peer statistics command. Output fields are listed in the approximate order in which they appear.

Table 87: show diameter peer statistics Output Fields

Field Name	Field Description	Level of Output
Peer	Name of the peer.	summary brief
Instance	Name of the Diameter instance in which the network element is configured.	summary brief
Rx	Total number of messages received.	summary brief
Rx-Peer	Number of messages received by the peer.	summary brief
Rx-node	Number of messages received by the Diameter node.	summary brief

Table 87: show diameter peer statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
Forw	Total number of forwarded messages.	summary brief
Tx-Peer	Number of messages transmitted by the peer.	summary brief
Tx	Total number of transmitted messages.	summary brief
Peer name	Name of the peer.	detail
Instance name	Name of the Diameter instance in which the network element is configured.	detail

Sample Output

show diameter peer statistics

```
user@host> show diameter peer statistics
```

```
Diameter peer statistics:
```

Peer	Instance	Rx	Rx-Peer	Rx-Node	Forw	Tx-Peer	Tx
p0	master	113	113	0	0	113	
113							
p1	master	110	110	0	0	110	
110							
p288	master	0	0	0	0	0	
0							
pA	master	0	0	0	0	0	
0							
pB	master	0	0	0	0	0	
0							
pc	master	0	0	0	0	0	
0							
pd	master	0	0	0	0	0	
0							

show diameter peer statistics detail

```
user@host> show diameter peer statistics detail
```

```
Diameter peer statistics:
```

Peer name	:	p0	
Instance name	:	master	
		Current	Since last enable
Rx errors	:	0	0
Rx messages	:	114	114
Rx handled by peer	:	114	114
Rx dropped msgs	:	0	0
Rx unmatched answers	:	0	0
Rx answers	:	0	0
Rx requests	:	0	0
Rx total	:	0	0
Forw to connection	:	0	0
Forw to peer	:	0	0

```

Forw to routed dest      :      0      0
Total forwarding         :      0      0
Forwarding failures     :      0      0
Forwarding success      :      0      0
Moved-in messages       :      0      0
Moved-out messages      :      0      0
Rerouted messages       :      0      0
Dropped tx messages     :      0      0
Tx by peer              :     114    114
Tx errors               :      0      0
Tx total                :     114    114
Connection attempts     :      0      1
Connection fails        :      0      0
Connections             :      0      1
Passive terminations    :      0      0
Active terminations     :      0      0
Passive disconnects     :      0      0
Active disconnects      :      0      0
Rx block requests       :      0      0
Rx block timeoutss      :      0      0
Connection management messages
      Rx current      Rx since      Tx current      Tx since
                        last enable      last enable

CER                     :      0      0      1      1
CEA                     :      1      1      0      0
DWR                     :      0      0     113     113
DWA                     :     113     113      0      0
DPR                     :      0      0      0      0
DPA                     :      0      0      0      0

Peer name                : p1
Instance name            : master
      Current      Since last enable
Rx errors               :      0      0
Rx messages             :     110     110
Rx handled by peer      :     110     110
Rx dropped msgs         :      0      0
Rx unmatched answers    :      0      0
Rx answers              :      0      0
Rx requests             :      0      0
Rx total               :      0      0
Forw to connection     :      0      0
Forw to peer           :      0      0
Forw to routed dest     :      0      0
Total forwarding        :      0      0
Forwarding failures     :      0      0
Forwarding success      :      0      0
Moved-in messages       :      0      0
Moved-out messages      :      0      0
Rerouted messages       :      0      0
Dropped tx messages     :      0      0
Tx by peer              :     110     110
Tx errors               :      0      0
Tx total               :     110     110
Connection attempts     :      0      1
Connection fails        :      0      0
Connections             :      0      1
Passive terminations    :      0      0
Active terminations     :      0      0
Passive disconnects     :      0      0

```

Active disconnects	:	0	0		
Rx block requests	:	0	0		
Rx block timeoutss	:	0	0		
Connection management messages					
		Rx current	Rx since last enable	Tx current	Tx since last enable
CER	:	0	0	1	1
CEA	:	1	1	0	0
DWR	:	0	0	109	109
DWA	:	109	109	0	0
DPR	:	0	0	0	0
DPA	:	0	0	0	0

show diameter route

Syntax	show diameter route <brief detail summary> <route-name>
Release Information	Command introduced in Junos OS Release 9.6.
Description	Display information about all routes associated with Diameter instances or only the specified route.
Options	<p>brief detail summary—(Optional) Display the specified level of output. The summary output is displayed by default and includes basic function information. The brief output displays the summary information in a different format. The detail output adds information to the brief output.</p> <p>route-name—(Optional) Display information for only the specified route.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show diameter on page 1120 • show diameter network-element on page 1135
List of Sample Output	<p>show diameter route on page 1154</p> <p>show diameter route detail on page 1154</p>
Output Fields	Table 88 on page 1153 lists the output fields for the show diameter route command. Output fields are listed in the approximate order in which they appear.

Table 88: show diameter route Output Fields

Field Name	Field Description	Level of Output
Route	Name of the route.	summary brief
NE	Name of the network element associated with the route.	summary brief
Instance	Name of the Diameter instance in which the route is configured.	summary brief
NE name	Name of the network element associated with the route.	brief detail
Instance name	Name of the Diameter instance in which the route is configured.	brief detail
Valid	Determination whether the route is valid, yes or no .	All levels
Up	State of the route, yes (up) or no (down).	All levels
Function	Name of the function associated with the route.	brief detail

Table 88: show diameter route Output Fields (*continued*)

Field Name	Field Description	Level of Output
Partition	Partition associated with the function.	brief detail
Dest-realm	Destination realm configured for the route.	brief detail
Dest-host	Destination hostname configured for the route.	brief detail
Metric	Metric associated with the destination and function to create the route.	brief detail
Score	<p>Value that represents how a route is configured. The basic score is 0. Points are added according to the following scheme:</p> <ul style="list-style-type: none"> • Function is specified—Add 3. • Function partition is specified—Add 1. • Destination realm is specified—Add 1. • Destination host is specified—Add 1. 	brief detail

Sample Output

show diameter route

```
user@host> show diameter route
```

```
Diameter routes:
```

```
Route      NE          Instance  Valid Up
rA         ne0         master    yes  yes
```

show diameter route detail

```
user@host> show diameter route detail
```

```
Diameter route:
```

```
Route name      : rA
NE name         : ne0
Instance name   : master
Valid           : yes
Up              : yes
Function        : jsrc
Partition       : jsrc-a
Dest-realm      : outer-realm
Dest-host       : outer-host
Metric          :      50
Score           :      6
```

show ipv6 router-advertisement

Syntax	<pre>show ipv6 router-advertisement <conflicts> <interface <i>interface</i>> <logical-system (all <i>logical-system-name</i>)> <prefix <i>prefix/prefix length</i>></pre>
Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Command introduced in Junos OS Release 12.2 for the QFX Series.</p> <p>Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Display information about IPv6 router advertisements, including statistics about messages sent and received on interfaces, and information received from advertisements from other routers.
Options	<p>none—Display all IPv6 router advertisement information for all interfaces.</p> <p>conflicts—(Optional) Display only the IPv6 router advertisement information that is conflicting.</p> <p>interface <i>interface</i>—(Optional) Display IPv6 router advertisement information for the specified interface.</p> <p>logical-system (all <i>logical-system-name</i>)—(Optional) Perform this operation on all logical systems or on a particular logical system.</p> <p>prefix <i>prefix/prefix length</i>—(Optional) Display IPv6 router advertisement information for the specified prefix.</p>
Additional Information	The display identifies conflicting information by enclosing the value the router is advertising in brackets.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> clear ipv6 router-advertisement on page 1026
List of Sample Output	<p>show ipv6 router-advertisement on page 1156</p> <p>show ipv6 router-advertisement conflicts on page 1157</p> <p>show ipv6 router-advertisement prefix on page 1157</p>
Output Fields	Table 89 on page 1155 describes the output fields for the show ipv6 router-advertisement command. Output fields are listed in the approximate order in which they appear.

Table 89: show ipv6 router-advertisement Output Fields

Field Name	Field Description
Interface	Name of the interface.

Table 89: show ipv6 router-advertisement Output Fields (*continued*)

Field Name	Field Description
Advertisements sent	Number of router advertisements sent and the elapsed time since they were sent.
Solicits received	Number of solicitation messages received.
Advertisements received	Number of router advertisements received.
Advertisements from	Names of interfaces from which router advertisements have been received and the elapsed time since the last one was received.
Managed	Managed address configuration flag: 0 (stateless) or 1 (stateful).
Other configuration	Other stateful configuration flag: 0 (stateless) or 1 (stateful).
Reachable time	Time that a node identifies a neighbor as reachable after receiving a reachability confirmation, in milliseconds.
Default lifetime	Default lifetime, in seconds: from 0 seconds to 18.2 hours. A setting of 0 indicates that the router is not a default router.
Retransmit timer	Time between retransmitted Neighbor Solicitation messages, in milliseconds.
Current hop limit	Configured current hop limit.
Prefix	Name and length of the prefix.
Valid lifetime	How long the prefix remains valid for onlink determination.
Preferred lifetime	How long the prefix generated by stateless autoconfiguration remains preferred.
On link	Onlink flag: 0 (not onlink) or 1 (onlink).
Autonomous	Autonomous address configuration flag: 0 (not autonomous) or 1 (autonomous).

Sample Output

show ipv6 router-advertisement

```

user@host> show ipv6 router-advertisement
Interface: fe-0/1/1.0
  Advertisements sent: 0
  Solicits received: 0
  Advertisements received: 0
Interface: fxp0.0
  Advertisements sent: 0
  Solicits received: 0
  Advertisements received: 1
  Advertisement from fe80::2d0:b7ff:fe1e:7b0e, heard 00:00:13 ago
  Managed: 0

```



```
Other configuration: 0 [1]
Reachable time: 0 ms
Default lifetime: 1800 sec
Retransmit timer: 0 ms
Current hop limit: 64
```

show ipv6 router-advertisement conflicts

```
user@host> show ipv6 router-advertisement conflicts
Interface: fxp0.0
Advertisement from fe80::2d0:b7ff:fe1e:7b0e, heard 00:01:08 ago
Other configuration: 0 [1]
```

show ipv6 router-advertisement prefix

```
user@host> show ipv6 router-advertisement prefix 8040::/16
Interface: fe-0/1/3.0
Advertisements sent: 3, last sent 00:04:11 ago
Solicits received: 0
Advertisements received: 3
Advertisement from fe80::290:69ff:fe9a:5403, heard 00:00:05 ago
Managed: 0
Other configuration: 0
Reachable time: 0 ms
Default lifetime: 180 sec [1800 sec]
Retransmit timer: 0 ms
Current hop limit: 64
Prefix: 8040:1::/64
Valid lifetime: 2592000 sec
Preferred lifetime: 604800 sec
On link: 1
Autonomous: 1
```

show network-access aaa accounting

Syntax	show network-access aaa accounting
Release Information	Command introduced in Junos OS Release 12.3.
Description	Display the state of the RADIUS Acct-On response sent from the RADIUS server.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • RADIUS Acct-On and Acct-Off Messages on page 91
List of Sample Output	show network-access aaa accounting on page 1158
Output Fields	Table 70 on page 1085 lists the output fields for the show network-access aaa accounting command. Output fields are listed in the approximate order in which they appear.

Table 90: show network-access aaa accounting Output Fields

Field Name	Field Description
Profile	Name of the profile associated with the RADIUS server. A RADIUS server can be associated with more than one profile.
Logical System	Logical system associated with the access profile.
Routing Instance	Routing instance associated with the access profile.
Acct-On-Response	Status of the RADIUS Acct-On response. <ul style="list-style-type: none"> • ACK—ACK response for the Acct-On message is received from the RADIUS server. • ERROR—An error condition has occurred. • NONE— No Acct-On message is sent. • PENDING—Acct-On message is sent to RADIUS server, but no response has been received yet.

Sample Output

show network-access aaa accounting

```

user@host> show network-access aaa accounting
Profile      Logical System  Routing Instance  Acct-On-Response
ppp-profile  default        default          ACK
l2tp-profile default        l2tp_RI          PENDING

```

show network-access aaa radius-servers

Syntax	show network-access aaa radius-servers <detail>
Release Information	Command introduced in Junos OS Release 12.1.
Description	Display RADIUS server status and information.
Options	detail —(Optional) Display detailed level of information.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Verifying and Managing Subscriber AAA Information on page 181
List of Sample Output	show network-access aaa radius-servers on page 1162 show network-access aaa radius-servers on page 1162 show network-access aaa radius-servers detail on page 1163
Output Fields	Table 91 on page 1159 lists the output fields for the show network-access aaa radius-servers command. Output fields are listed in the approximate order in which they appear.

Table 91: show network-access aaa radius-servers Output Fields

Field Name	Field Description	Level of Output
Profile	Name of the profile associated with the RADIUS server. A RADIUS server can be associated with more than one profile.	All levels
Server address	IP address of the RADIUS server.	All levels
Authentication port	RADIUS server authentication port number.	All levels
Accounting port	RADIUS server accounting port number.	All levels
Accounting retry	Number of times the router retransmits RADIUS accounting messages when no response is received from the server.	Detail
Accounting timeout	Period the local router waits to receive a response from a RADIUS accounting server before retransmitting the message.	Detail

Table 91: show network-access aaa radius-servers Output Fields (continued)

Field Name	Field Description	Level of Output
Status	<p>RADIUS server status, UP (Alive), UNREACHABLE, or DOWN (DEAD).</p> <p>If status is DOWN, the Status field includes the number of seconds configured by the revert-interval statement. The router does not send request to servers in the DOWN state, but does send requests to servers with a status of either UP or UNREACHABLE.</p> <p>NOTE:</p> <p>After requests to a server or set of servers time out after 10 seconds, the status of the servers changes. The following guidelines apply to server status:</p> <ul style="list-style-type: none"> All servers cannot be marked as DOWN; instead, the unresponsive servers are marked as UNREACHABLE. For example, if only one RADIUS server is configured and that server is unresponsive, the server status is marked as UNREACHABLE rather than DOWN. If at least one server has a status of UP, the status of all unresponsive servers is set to DOWN for the remainder of the configured revert-interval setting. If no server has a status of UP, then the status of the unresponsive servers is set to UNREACHABLE for the remainder of the revert-interval setting or for 30 seconds, whichever is less. The status of unresponsive servers is returned to UP from DOWN or UNREACHABLE at the end of the revert-interval setting (or the 30-second interval). If no requests are sent to a server, the server's status is always UP. 	All levels
RADIUS servers	Details for specific RADIUS server, identified by IP address.	Detail
Authentication requests	Number of authentication requests received by the authentication server.	Detail
Authentication rollover requests	Number of requests coming into the server as a result of the previous server timing out.	Detail
Authentication retransmissions	Number of retransmissions.	Detail
Accepts	Number of authentication requests accepted by the authentication server.	Detail
Rejects	Number of authentication requests rejected by the authentication server.	Detail

Table 91: show network-access aaa radius-servers Output Fields (*continued*)

Field Name	Field Description	Level of Output
Challenges	Number of authentication requests challenged by the authentication server.	Detail
Authentication malformed responses	Number of responses with attributes having an invalid length or unexpected attributes (such as two attributes when the response is required to have at most one).	Detail
Authentication bad authenticators	Number of responses in which the authenticator is incorrect for the authentication request. This can occur if the RADIUS secrets for the client and server do not match.	Detail
Authentication requests pending	Number of authentication requests waiting for a response.	Detail
Authentication request timeouts	Number of times an authentication request to the server timed out.	Detail
Authentication unknown responses	Number of unknown responses. The RADIUS response type in the header is invalid or unsupported.	Detail
Authentication packets dropped	Number of packets dropped because they are too short or because the router receives a response for which there is no corresponding request.	Detail
Accounting start requests	Number of accounting start requests received.	Detail
Accounting interim requests	Number of accounting interim requests received.	Detail
Accounting stop requests	Number of accounting stop requests received.	Detail
Accounting rollover requests	Number of requests coming into the server as a result of the previous server timing out.	Detail
Accounting retransmissions	Number of retransmissions.	Detail
Accounting start responses	Number of accounting start responses sent by the server.	Detail
Accounting interim responses	Number of accounting interim responses sent by the server.	Detail
Accounting stop responses	Number of accounting stop responses sent by the server.	Detail

Table 91: show network-access aaa radius-servers Output Fields (*continued*)

Field Name	Field Description	Level of Output
Accounting malformed responses	Number of responses with attributes having an invalid length or unexpected attributes (such as two attributes when the response is required to have at most one).	Detail
Accounting bad authenticators	Number of responses in which the authenticator is incorrect for the accounting request. This can occur if the RADIUS secrets for the client and server do not match.	Detail
Accounting requests pending	Number of accounting requests waiting for a response.	Detail
Accounting request timeouts	Number of accounting requests to the accounting server that timed out.	Detail
Accounting unknown responses	Number of unknown responses. The RADIUS response type in the header is invalid or unsupported.	Detail
Accounting packets dropped	Number of packets dropped because they are too short or because the router receives a response for which there is no corresponding request.	Detail

Sample Output

show network-access aaa radius-servers

```

user@host> show network-access aaa radius-servers
Profile: xyz-profile1
  Server address: 192.168.30.188
  Authentication port: 1645
  Accounting port: 1646
  Status: UP
Profile: xyz-profile2
  Server address: 192.168.30.190
  Authentication port: 1812
  Accounting port: 1813
  Status: DOWN ( 60 seconds )

```

show network-access aaa radius-servers

```

user@host> show network-access aaa radius-servers
Profile: xyz-profile3
  Server address: 192.168.30.188
  Authentication port: 1645
  Accounting port: 1646
  Status: UNREACHABLE
Profile: xyz-profile3
  Server address: 192.168.30.190
  Authentication port: 1812
  Accounting port: 1813
  Status: UNREACHABLE

```

show network-access aaa radius-servers detail

```
user@host> show network-access aaa radius-servers detail
Profile: xyz_profile5
  Server address: 192.168.30.188
    Authentication port: 1812
    Accounting port: 1813
    Status: UP
  Server address: 192.168.30.190
    Authentication port: 1812
    Accounting port: 1813
    Accounting retry: 5
    Accounting port: 60
    Status: UP
  Server address: 192.168.30.192
    Authentication port: 1812
    Accounting port: 1813
    Status: UP

RADIUS Servers
192.168.30.188
  Authentication requests: 7658
  Authentication rollover requests: 0
  Authentication retransmissions: 3600
  Accepts: 6458
  Rejects: 0
  Challenges: 0
  Authentication malformed responses: 0
  Authentication bad authenticators: 0
  Authentication requests pending: 0
  Authentication request timeouts: 4800
  Authentication unknown responses: 0
  Authentication packets dropped: 0
  Accounting start requests: 1
  Accounting interim requests: 1
  Accounting stop requests: 0
  Accounting rollover requests: 0
  Accounting retransmissions: 0
  Accounting start responses: 1
  Accounting interim responses: 1
  Accounting stop responses: 0
  Accounting malformed responses: 0
  Accounting bad authenticators: 0
  Accounting requests pending: 0
  Accounting request timeouts: 0
  Accounting unknown responses: 0
  Accounting packets dropped: 0
```

show network-access aaa statistics

Syntax	<pre>show network-access aaa statistics <accounting (detail)> <address-assignment (client pool <i>pool-name</i>)> <dynamic-requests> <radius></pre>
Release Information	<p>Command introduced in Junos OS Release 9.1.</p> <p>Option address-assignment introduced in Junos OS Release 10.0.</p> <p>Option radius introduced in Junos OS Release 11.4.</p> <p>Option detail introduced in Junos OS Release 13.3.</p>
Description	Display AAA accounting, address-assignment, dynamic request statistics, and RADIUS settings and statistics.
Options	<p>accounting (detail)—(Optional) Display AAA accounting statistics. The detail keyword displays additional accounting information</p> <p>address-assignment (client pool <i>pool-name</i>)—(Optional) Display AAA address-assignment client and pool statistics.</p> <p>dynamic-requests—(Optional) Display AAA dynamic requests.</p> <p>radius—(Optional) Display RADIUS settings and statistics.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Verifying and Managing Subscriber AAA Information on page 181
List of Sample Output	<p>show network-access aaa statistics accounting on page 1167</p> <p>show network-access aaa statistics accounting detail on page 1167</p> <p>show network-access aaa statistics address-assignment client on page 1167</p> <p>show network-access aaa statistics address-assignment pool on page 1167</p> <p>show network-access aaa statistics dynamic-requests on page 1168</p> <p>show network-access aaa statistics radius on page 1168</p>
Output Fields	<p>Table 92 on page 1164 lists the output fields for the show network-access aaa statistics command. Output fields are listed in the approximate order in which they appear.</p>

Table 92: show network-access aaa statistics Output Fields

Field Name	Field Description
Requests received	<ul style="list-style-type: none"> • Number of accounting requests generated by the AAA framework. • Number of dynamic requests received from the external server.
Accounting on requests	Number of accounting on requests sent from a client to a RADIUS accounting server.

Table 92: show network-access aaa statistics Output Fields (*continued*)

Field Name	Field Description
Accounting start requests	Number of accounting start requests sent from a client to a RADIUS accounting server.
Accounting interim requests	Number of accounting interim requests sent from a client to a RADIUS accounting server.
Accounting stop requests	Number of accounting stop requests sent from a client to a RADIUS accounting server.
Accounting Response failures	Number of accounting requests not acknowledged (NAK) by the accounting server.
Accounting Response Success	Number of accounting requests acknowledged by the accounting server.
Timed out requests	Number of accounting requests to the accounting server that timed out.
Accounting on responses	Number of accounting on requests acknowledged by the RADIUS accounting server.
Accounting start responses	Number of accounting start requests acknowledged by the RADIUS accounting server.
Accounting interim responses	Number of accounting interim requests acknowledged by the RADIUS accounting server.
Accounting stop responses	Number of accounting stop requests acknowledged by the RADIUS accounting server.
Accounting rollover requests	Number of accounting requests coming to a RADIUS accounting server after a previous server timing out.
Accounting unknown requests	Number of unknown accounting requests sent from a client to a RADIUS accounting server (for example, the header has invalid or unsupported information).
Accounting pending account requests	Number of accounting requests sent from a client to a RADIUS accounting server that are waiting for a response from the server.
Accounting malformed responses	Number of accounting responses from a RADIUS accounting server that have invalid or unexpected attributes.
Accounting retransmissions	Number of accounting requests made by a client to the RADIUS sever that were retransmitted.
Accounting bad authenticators	Number of accounting responses from a RADIUS accounting server that have an incorrect authenticator (for example, the client and server RADIUS secret do not match).
Accounting packets dropped	Number of accounting responses from a RADIUS accounting server that are dropped by a client.

Table 92: show network-access aaa statistics Output Fields (*continued*)

Field Name	Field Description
Client	Client type; for example, DHCP, Mobile IP, PPP.
Out of Memory	Number of times an address was not given to the client due to memory issues.
No Matches	Number of times there were no network matches for the pool.
Pool Name	Name of the address-assignment pool for this client.
Out of Addresses	Number of times there were no available addresses in the pool.
Address total	Number of addresses in the pool.
Addresses in use	Number of addresses in use.
Address Usage (percent)	Percentage of total addresses in use.
processed successfully	Number of dynamic requests processed successfully by the AAA framework.
errors during processing	Number of dynamic requests that resulted in processing errors by the AAA framework.
Link Name	Name of the secondary address-assignment pool to which the primary pool is linked.
Pool Usage	Percentage of allocated addresses in the specified address pool.
silently dropped	Number of dynamic requests dropped by the AAA framework due to multiple back-to-back or duplicate requests.
RADIUS Server	IP address of the RADIUS server to which the router is sending requests.
Profile	Name of the RADIUS profile associated with the RADIUS server. A RADIUS server can be associated with more than one RADIUS profile.
Configured	Configured maximum number of outstanding requests from the router to the RADIUS server for a specific profile. An outstanding request is a request to which the RADIUS server has not yet responded. The range of values is 0 through 2000 outstanding requests. The default value is 1000.
Current	Current number of outstanding requests from the router to the RADIUS server for a specific profile. An outstanding request is a request to which the RADIUS server has not yet responded.
Peak	Highest number of outstanding requests from the router to the RADIUS server for a specific profile at any point in time since the router was started or since the counter was last cleared. NOTE: If the value of this field is equal to the value of the Configured field, you may want to increase the value of the Configured field.

Table 92: show network-access aaa statistics Output Fields (*continued*)

Field Name	Field Description
Exceeded	Number of times that the router attempted to send requests to the RADIUS server in excess of the configured maximum value for a specific profile. NOTE: If the value of this field is nonzero, you may want to increase the value of the Configured field.

Sample Output

show network-access aaa statistics accounting

```
user@host> show network-access aaa statistics accounting
Accounting module statistics
  Requests received: 0
  Accounting Response failures: 0
  Accounting Response Success: 0
  Timed out requests: 0
```

show network-access aaa statistics accounting detail

```
user@host> show network-access aaa statistics accounting detail
Accounting module statistics
  Requests received: 261
    Accounting on requests: 261
    Accounting start requests: 0
    Accounting interim requests: 0
    Accounting stop requests: 0
  Accounting response failures: 0
  Accounting response success: 0
    Accounting on responses: 0
    Accounting start responses: 0
    Accounting interim responses: 0
    Accounting stop responses: 0
  Timed out requests: 260
  Accounting rollover requests: 0
  Accounting unknown responses: 0
  Accounting pending account requests: 1
  Accounting malformed responses: 0
  Accounting retransmissions: 783
  Accounting bad authenticators: 0
  Accounting packets dropped: 0
```

show network-access aaa statistics address-assignment client

```
user@host> show network-access aaa statistics address-assignment client
Address-assignment statistics
  Client: jdhcpd
  Out of Memory: 0
  No Matches: 2
```

show network-access aaa statistics address-assignment pool

```
user@host> show network-access aaa statistics address-assignment pool isp_1
Address-assignment statistics
  Pool Name: isp_1
  Pool Name: (all pools in chain)
  Out of Memory: 0
  Out of Addresses: 9
```

```
Address total: 47
Addresses in use: 47
Address Usage (percent): 100
```

show network-access aaa statistics dynamic-requests

```
user@host> show network-access aaa statistics dynamic-requests
requests received: 0
processed successfully: 0
errors during processing: 0
silently dropped: 0
```

show network-access aaa statistics radius

```
user@host> show network-access aaa statistics radius
Outstanding Requests
RADIUS Server    Profile    Configured    Current    Peak    Exceeded
172.28.32.239    prof1      1000          0          1000    14
                  prof2      500           17         432     0
171.27.82.211    myprof     200           0          200     27
12.1.11.254      pppoe-auth 111           0          1       0
```

show network-access aaa statistics authentication

Syntax	show network-access aaa statistics authentication <detail>
Release Information	Command introduced in Junos OS Release 9.1. Option detail introduced in Junos OS Release 12.1.
Description	Display AAA authentication statistics.
Options	detail —(Optional) Displays detailed information about authentication.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Verifying and Managing Subscriber AAA Information on page 181
List of Sample Output	show network-access aaa statistics authentication on page 1171 show network-access aaa statistics authentication detail on page 1171
Output Fields	Table 93 on page 1169 lists the output fields for the show network-access aaa statistics authentication command. Output fields are listed in the approximate order in which they appear.

Table 93: show network-access aaa statistics authentication Output Fields

Field Name	Field Description	Level of Output
Requests received	Number of authentication requests received from clients.	All levels
Accepts	Number of authentication requests accepted by the authentication server.	All levels
Rejects	Number of authentication requests rejected by the authentication server.	All levels
Challenges	Number of authentication requests challenged by the authentication server.	All levels
Timed out requests	Number of authentication requests that timed out.	All levels
RADIUS authentication failures	Number of RADIUS authentication requests that have failed.	Detail
Queue request deleted	Number of queue requests that have been deleted.	Detail
Malformed reply	Number of malformed replies received from the RADIUS authentication server.	Detail

Table 93: show network-access aaa statistics authentication Output Fields (*continued*)

Field Name	Field Description	Level of Output
No server configured	Number of authentication requests that failed because no authentication server is configured.	Detail
Access Profile configuration not found	Number of authentication requests that failed because no access profile is configured.	Detail
Unable to create client record	Number of times that the router is unable to create the client record for the authentication request.	Detail
Unable to create client request	Number of times that the router is unable to create the client request for the authentication request.	Detail
Unable to build authentication request	Number of times that the router is unable to build the authentication request.	Detail
No server found	Number of requests to the authentication server that have timed out; the server is then considered to be down.	Detail
Unable to create handle	Number of authentication requests that have failed because of an internal allocation failure.	Detail
Unable to queue request	Number of times the router was unable to queue the request to the authentication server.	Detail
Invalid credentials	Number of times the router did not have proper authorization to access the authentication server.	Detail
Malformed request	Number of times the router request to the authentication server is malformed.	Detail
License unavailable	Number of times the router did not have a license to access the authentication server.	Detail
Redirect requested	Number of authentication requests that have been redirected based on routing instance.	Detail
Internal failure	Number of internal failures.	Detail
Local authentication failures	Number of times local authentication failed.	Detail
LDAP lookup failures	Number of times the LDAP lookup operation failed.	Detail

Sample Output

show network-access aaa statistics authentication

```
user@host> show network-access aaa statistics authentication
Authentication module statistics
  Requests received: 2118
  Accepts: 261
  Rejects: 975
  Challenges: 0
  Timed out requests: 882
```

show network-access aaa statistics authentication detail

```
user@host> show network-access aaa statistics authentication detail
Authentication module statistics
  Requests received: 2118
  Accepts: 261
  Rejects: 975
    RADIUS authentication failures: 975
      Queue request deleted: 0
      Malformed reply: 0
      No server configured: 0
      Access Profile configuration not found: 0
      Unable to create client record: 0
      Unable to create client request: 0
      Unable to build authentication request: 0
      No server found: 975
      Unable to create handle: 0
      Unable to queue request: 0
      Invalid credentials: 0
      Malformed request: 0
      License unavailable: 0
      Redirect requested: 0
      Internal failure: 0
    Local authentication failures: 0
    LDAP lookup failures: 0
  Challenges: 0
  Timed out requests: 882
```

show network-access aaa statistics pending-accounting-stops

Syntax	show network-access aaa statistics pending-accounting-stops
Release Information	Command introduced in Junos OS Release 13.1.
Description	Display the number of pending accounting stop requests.
Options	This command has no options.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• request network-access aaa replay pending-accounting-stops on page 902• show accounting pending-accounting-stops on page 1051
List of Sample Output	show network-access aaa statistics pending-accounting-stops on page 1172
Output Fields	Table 94 on page 1172 lists the output field for the show network-access aaa statistics pending-accounting-stops command.

Table 94: show network-access aaa statistics pending-accounting-stops Output Fields

Field Name	Field Description
Pending accounting stops	Total number of accounting stop messages queued.

Sample Output

show network-access aaa statistics pending-accounting-stops

```
user@host> show network-access aaa statistics pending-accounting-stops
Pending accounting stops: 10,000
```


show network-access aaa statistics preauthentication

Syntax	show network-access aaa statistics preauthentication
Release Information	Command introduced in Junos OS Release 13.3.
Description	Display AAA preauthentication statistics.
Options	detail —(Optional) Displays detailed information about authentication.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • RADIUS Logical Line Identifier (LLID) Overview on page 121 • Configuring Logical Line Identification (LLID) Preauthentication on page 124
List of Sample Output	show network-access aaa statistics preauthentication on page 1173
Output Fields	Table 95 on page 1173 lists the output fields for the show network-access aaa statistics preauthentication command. Output fields are listed in the approximate order in which they appear.

Table 95: show network-access aaa statistics preauthentication Output Fields

Field Name	Field Description	Level of Output
Requests received	Number of preauthentication requests received from clients.	All levels
Multistack requests	Number of preauthentication requests for dual-stack subscribers.	All levels
Accepts	Number of preauthentication requests accepted by the preauthentication server.	All levels
Rejects	Number of preauthentication requests rejected by the preauthentication server.	All levels
Challenges	Number of preauthentication requests challenged by the preauthentication server.	All levels
Timed out requests	Number of preauthentication requests that timed out.	All levels

Sample Output

show network-access aaa statistics preauthentication

```

user@host> show network-access aaa statistics preauthentication
Preauthentication module statistics
Requests received: 2118

```

Multistack requests: 0
Accepts: 261
Rejects: 975
Challenges: 0
Timed out requests: 882

show network-access aaa subscribers

Syntax	<code>show network-access aaa subscribers</code> <code><logical-system <i>logical-system-name</i>></code> <code><routing-instance <i>routing-instance-name</i>></code> <code><statistics></code> <code><username></code>
Release Information	Command introduced in Junos OS Release 9.1.
Description	Display subscriber-specific AAA statistics.
Options	<p><code>logical-system <i>logical-system-name</i></code>—(Optional) List subscribers in the specific logical system.</p> <p><code>routing-instance <i>routing-instance-name</i></code>—(Optional) List subscribers for the specific routing instance. If you do not specify a routing instance name, the default routing instance is assumed.</p> <p><code>statistics</code>—(Optional) Display statistics for the subscriber events.</p> <p><code>username</code>—(Optional) Display information for the specified subscriber.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Verifying and Managing Subscriber AAA Information on page 181
List of Sample Output	show network-access aaa subscribers logical-system on page 1176 show network-access aaa subscribers logical-system routing-instance on page 1176 show network-access aaa subscribers statistics username on page 1177 show network-access aaa subscribers username on page 1177
Output Fields	Table 96 on page 1175 lists the output fields for the show network-access aaa subscribers command. Output fields are listed in the approximate order in which they appear.

Table 96: show network-access aaa subscribers Output Fields

Field Name	Field Description
Challenge requests	Number of authentication requests challenged by the authentication server for this subscriber.
Challenge responses	Number of challenge responses sent by the subscriber to the authentication server.
START sent successfully	Number of accounting start requests generated by the AAA framework for this subscriber.
START send failures	Number of accounting start requests that failed to make it to the accounting server for this subscriber.
START ack received	Number of accounting start requests acknowledged by the accounting server for this subscriber.

Table 96: show network-access aaa subscribers Output Fields (*continued*)

Field Name	Field Description
INTERIM sent successfully	Number of accounting interim requests generated by the AAA framework for this subscriber.
INTERIM send failures	Number of accounting interim requests that failed to make it to the accounting server for this subscriber.
INTERIM ack received	Number of accounting interim requests acknowledged by the accounting server for this subscriber.
Requests received	Number of reauthentication requests received by the authentication server.
Successful responses	Number of successful reauthentication requests granted by the authentication server.
Aborts handled	Number of reauthentication requests aborted by the authentication server.
Service name	Name of the subscriber service.
Creation requests	Number of requests to create the service.
Deletion requests	Number of requests to delete the service.
Request timeouts	Number of times the service request was timed out.
Client type	Type of client; for example, DHCP, Mobile IP, PPP.
Session-ID	ID of the subscriber session.
Session uptime	How long the session has been up, in <i>HH:MM:SS</i> .
Accounting	Status of accounting, and type of accounting if accounting is on.

Sample Output

show network-access aaa subscribers logical-system

```

user@host> show network-access aaa subscribers logical-system
Username           Client type      Logical system/Routing instance
cbenson@addr.net   ppp             default
00010e020304.1231 dhcp            isp-bos-metro-12:isp-cmborg-12
conley@isp3.com    dhcp            default:isp-gtown-r3-00
0020df980102.2334 dhcp            isp-bos-metro-16:isp-cmborg-12

```

show network-access aaa subscribers logical-system routing-instance

```

user@host> show network-access aaa subscribers logical-system isp-bos-metro-16
routing-instance isp-cmborg-12-32
Username           Client type      Logical system/Routing instance
00010e020304.1231 dhcp            isp-bos-metro-12:isp-cmborg-12
conley@isp3.com    dhcp            default:isp-gtown-r3-00
0020df980102.2334 dhcp            isp-bos-metro-16:isp-cmborg-12

```

show network-access aaa subscribers statistics username

```

user@host> show network-access aaa subscribers statistics username 00010e020304.1231
Authentication statistics
  Challenge requests: 0
  Challenge responses: 0
Accounting statistics
  START sent successfully: 1
  START send failures: 0
  START ack received: 1
  INTERIM sent successfully: 0
  INTERIM send failures: 0
  INTERIM ack received: 0
Re-authentication statistics
  Requests received: 0
  Successful responses: 0
  Aborts handled: 0
Service statistics
  Service name: filter-serv
  Creation requests: 1
  Deletion requests: 0
  Request timeouts: 0
  Service name: filter-serv2
  Creation requests: 144
  Deletion requests: 0
  Request timeouts: 144

```

show network-access aaa subscribers username

```

user@host> show network-access aaa subscribers username fred@isp5.net
Logical system/Routing instance  Client type  Session-ID  Session uptime
Accounting
isp-bos-metro-16:isp-cmbrg-12    dhcp        7            01:12:56
on/volume
Service name      Service type  Quota        Accounting
I-Cast            volume        1200 Mbps    on/volume+time
Voip               time          6000 secs    on/volume
GamingBurst

```

show network-access aaa subscribers session-id

Syntax	show network-access aaa subscribers session-id <i>session-id</i> <brief detail>
Release Information	Command introduced in Junos OS Release 10.0.
Description	Display information about the specified subscriber session.
Options	<i>session-id</i> —ID of the subscriber session. brief detail —(Optional) Display the specified level of information.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Verifying and Managing Subscriber AAA Information on page 181 • Activating and Deactivating Subscriber Services Locally with the CLI on page 332 • Deactivating a Single Instance of a Subscriber Service with Multiple Instances on page 341 • Deactivating All Instances of a Subscriber Service with Multiple Instances on page 343 • Verifying and Managing Subscriber Services with Multiple Instances on page 347
List of Sample Output	show network-access aaa subscribers session-id brief on page 1181 show network-access aaa subscribers session-id detail on page 1181 show network-access aaa subscribers session-id detail (Service with Multiple Instances) on page 1181
Output Fields	Table 97 on page 1178 lists the output fields for the show network-access aaa subscribers session-id command. Output fields are listed in the approximate order in which they appear.

Table 97: show network-access aaa subscribers session-id Output Fields

Field Name	Field Description	Level of Output
Type and Client type	Type of client.	All levels
Accounting	Status of accounting, and type of accounting if accounting is on.	brief
Service type	Type of accounting: volume , time , volume+time , or na .	brief
Quota	Quota for service: volume (in Mbps) or time (seconds).	brief
Username	Name of the user logged in to the session.	detail

Table 97: show network-access aaa subscribers session-id Output Fields (*continued*)

Field Name	Field Description	Level of Output
Stripped username	Username after the domain has been removed.	detail
Logical system/Routing instance and AAA Logical system/Routing instance	Name of the routing instance, logical system name, or both used for the session.	All levels
Target Logical system/Routing instance	Logical system/routing instance to which the session is mapped.	detail
Access-profile	Access profile used for AAA services for the session.	detail
Session ID	ID of the subscriber session. The session ID value displayed under Service name is the service session ID.	detail
Accounting Session ID	ID of the accounting session (RADIUS attribute 44). The ID appears in decimal or description format, as specified by the accounting-session-id-format statement.	detail
Multi Accounting Session ID	Bundle ID for MLPPP sessions. Acct-Multi-Session-Id (RADIUS attribute 50) uses the value of the session database bundle session ID to enable RADIUS to link together multiple related sessions. The value of this field is zero when no MLPPP sessions exist.	detail
IP Address	IP address of the subscriber.	detail
Authentication State	State of the subscriber authentication session: AuthInit , AuthStart , AuthChallenge , AuthRedirect , AuthClntRespWait , AuthAcctVolStatsAckWait , AuthAcctStopAckWait , AuthServCreateRespWait , AuthLogoutStart , AuthStateActive , AuthClntLogoutRespWait , AuthProfileUpdateWait , AuthProvisionRespWait , AuthProvisionServiceCreationWait	detail

Table 97: show network-access aaa subscribers session-id Output Fields (*continued*)

Field Name	Field Description	Level of Output
Gx-Plus Provisioning State	State of Gx-Plus provisioning: <ul style="list-style-type: none"> ignored—Subscriber has no IPv4 address or NAS-Port-ID. in-progress—Provisioning is in progress. logout—Subscriber logout is in progress. logout-done—Logout response has been received. response-received—Provisioning response has been received. 	detail
Accounting State	State of the subscriber accounting session: Acc-Init, Acc-Start-Sent, Imm-Update-Stats-Pending, Acc-Interim-Sent, Acc-Stop-Stats-Pending, Acc-Stop-Sent, Acc-Stop-On-Fail-Deny-Sent, Acc-Stop-Ackd	detail
Provisioning-type	Provisioning type for this session: <ul style="list-style-type: none"> gx-plus—Subscriber service uses Gx-Plus provisioning. jsrc—Subscriber service uses JSRC provisioning. none—Provisioning is not enabled. 	detail
Service name	Name of the attached service or policy. <ul style="list-style-type: none"> For RADIUS-activated and CLI-activated services, displays the full activation string for the service. If the activation string includes service parameters, then both the service name and service parameters are displayed. For JSRC-activated policies—displays the policy name. 	All levels
Service State	State of the service provided in the subscriber session.	detail
Session uptime	How long the session has been up, in <i>HH:MM:SS</i> .	All levels
Accounting status	Status of the accounting configuration for the service, on or off , and the type of accounting, time or volume+time . Configured in RADIUS Service-Statistics VSA [26-69].	detail
Service accounting session ID	ID of the service accounting session; RADIUS Acct-Session-Id attribute (44). The ID appears in decimal or description format, as specified by the accounting-session-id-format statement.	detail
Service accounting state	State of the service accounting session: Acc-Init, Acc-Start-Sent, Imm-Update-Stats-Pending, Acc-Interim-Sent, Acc-Stop-Stats-Pending, Acc-Stop-Sent, Acc-Stop-On-Fail-Deny-Sent, Acc-Stop-Ackd	detail

Table 97: show network-access aaa subscribers session-id Output Fields (continued)

Field Name	Field Description	Level of Output
Accounting interim interval	Amount of time between interim accounting updates for this service, in seconds; RADIUS Service-Interim-Acct-Interval VSA [26-140] or Diameter Acct-Interim-Interval AVP (85).	detail

Sample Output

show network-access aaa subscribers session-id brief

```
user@host> show network-access aaa subscribers session-id 6 brief
Logical system/Routing instance  Client type  Session uptime  Accounting
default:default                 dhcp      00:01:29       on/time
Service name                    Service type  Quota          Accounting
filter-service                  -na-         -na-           off
filter-service-2                volume+time  77.00MB/120secs off
1337994190863204450            -na-         -na-           off
```

show network-access aaa subscribers session-id detail

```
user@host> show network-access aaa subscribers session-id 5 detail
Type: dhcp
Username: larry@isp5.net
Stripped username: larry
AAA Logical system/Routing instance: default:default
Target Logical system/Routing instance: default:retail-onlinecompany-ca
Access-profile:retailer-onlinecompany-sjc
Session ID: 5
Accounting Session ID: jnpr ge-1/0/0.101:1
Multi Accounting Session ID: 0
IP Address: 192.168.44.104
Authentication State: AuthStateActive
Gx-Plus Provisioning State: response-received
Accounting State: Acc-Interim-Sent
Provisioning-type: jsrsc
Service name: filter-service-1
Service State: SvcActive
Session ID: 7
Session uptime: 00:01:33
Service name: 1337994190863204450
Service State: SvcActive
Session ID: 8
Session uptime: 00:01:33
Accounting status: on/volume+time
Service accounting session ID: 1:2-1322506006
Service accounting state: Acc-Interim-Sent
Accounting interim interval: 600
```

show network-access aaa subscribers session-id detail (Service with Multiple Instances)

```
user@host> show network-access aaa subscribers session-id 6 detail
Type: dhcp
Stripped username: fms2
AAA Logical system/Routing instance: default:default
Target Logical system/Routing instance: default:default
```

Access-profile: attr_test_profile1
Session ID: 6
Accounting Session ID: 6
Multi Accounting Session ID: 0
IP Address: 100.20.0.10
Authentication State: AuthStateActive
Accounting State: Acc-Interim-Sent
Provisioning Type: None
Service name: economy-service(up-filter,down-filter)
Service State: SvcActive
Service Family: inet
Service Activation Source: Radius
Session ID: 7
Session uptime: 00:04:36
Accounting status: on/volume+time
Service accounting session ID: 6:7-1354811427
Service accounting state: Acc-Start-Sent
Accounting interim interval: 600
Service name: economy-service(upstrm-filter,dwnstrm-filter)
Service State: SvcActive
Service Family: inet
Service Activation Source: Radius
Session ID: 8
Session uptime: 00:04:36
Accounting status: on/volume+time
Service accounting session ID: 6:8-1354811427
Service accounting state: Acc-Start-Sent
Accounting interim interval: 600

show network-access aaa terminate-code

Syntax	<pre>show network-access aaa terminate-code <brief detail summary> <reverse> <(aaa dhcp l2tp ppp)></pre>
Release Information	Command introduced in Junos OS Release 11.4.
Description	Display the count for termination cause types and the current mapping between session termination cause types and code values.
Options	<p>none—Display all mappings.</p> <p>brief detail summary—(Optional) Display the specified level of output. The summary output is displayed by default and includes base count information about mappings. The brief output displays mappings with non-zero usage count and custom mappings. The detail output displays all mappings.</p> <p>aaa—(Optional) Limit display to AAA mappings only.</p> <p>dhcp—(Optional) Limit display to DHCP mappings only.</p> <p>l2tp—(Optional) Limit display to L2TP mappings only.</p> <p>ppp—(Optional) Limit display to PPP mappings only.</p> <p>reverse—(Optional) Display mapping of the code value conveyed in the RADIUS Acct-Terminate-Cause attribute (49) to the termination cause type.</p>
Required Privilege Level	view
List of Sample Output	show network-access aaa terminate-code on page 1184 show network-access aaa terminate-code reverse on page 1184 show network-access aaa terminate-code dhcp on page 1185 show network-access aaa terminate-code detail on page 1185 show network-access aaa terminate-code brief on page 1185 show network-access aaa terminate-code summary on page 1185
Output Fields	Table 93 on page 1169 lists the output fields for the show network-access aaa terminate-code command. Output fields are listed in the approximate order in which they appear.

Table 98: show network-access aaa terminate-code Output Fields

Field Name	Field Description	Level of Output
RADIUS	RFC-defined code value conveyed in the RADIUS Acct-Terminate-Cause attribute (49) or a nonstandard, customized value that you configure with the terminate-code aaa statement at the [edit access] hierarchy level.	brief detail None (with reverse option)

Table 98: show network-access aaa terminate-code Output Fields (*continued*)

Field Name	Field Description	Level of Output
Custom	Whether or not the termination cause is a customized mapping or the default mapping.	All levels
Mapping-Count	Number of mappings that occurred for a specific terminate cause type or category (standard or summary output) or per termination cause (reverse output).	summary None
Usage-Count	Number of times the terminate code mapping was used.	All levels
Type	Termination cause type—null, aaa, dhcp, l2tp, or ppp. NOTE: The null termination cause type indicates that no termination reason was provided by the subscriber and the RADIUS Acct-Terminate-Cause attribute (49) was not included in the Acct-Stop request	All levels
Code	Specific termination cause.	brief detail

Sample Output

show network-access aaa terminate-code

```

user@host> show network-access aaa terminate-code
Terminate-code:
Custom Mapping-Count Usage-Count Type
no      1             0      null
no      5             0      aaa
no      5             0      dhcp
no     364            0      l2tp
no     202            0      ppp

```

show network-access aaa terminate-code reverse

```

user@host> show network-access aaa terminate-code reverse
Terminate-code:
RADIUS Custom Mapping-Count Usage-Count Type
0      no      1             0      null
1      no      1             0      dhcp
1      no      5             0      l2tp
1      no      8             0      ppp
2      no      1             0      dhcp
2      no      3             0      ppp
4      no      1             0      dhcp
4      no      1             0      l2tp
4      no      1             0      ppp
5      no      1             0      l2tp
5      no      1             0      ppp
6      no      1             0      aaa

```

6	no	13	0	l2tp
6	no	3	0	ppp
8	no	3	0	l2tp
8	no	5	0	ppp
9	no	13	0	l2tp
9	no	12	0	ppp
10	no	2	0	aaa
10	no	1	0	dhcp
10	no	128	0	l2tp
10	no	163	0	ppp
15	no	1	0	dhcp
15	no	190	0	l2tp
17	no	2	0	aaa
17	no	10	0	l2tp
17	no	6	0	ppp

show network-access aaa terminate-code dhcp

```
user@host> show network-access aaa terminate-code dhcp
Terminate-code:
Custom Mapping-Count Usage-Count Type
no 5 0 dhcp
```

show network-access aaa terminate-code detail

```
user@host> show network-access aaa terminate-code aaa detail
Terminate-code:
RADIUS Custom Usage-Count Type Code
17 no 0 aaa deny-authentication-denied
10 no 0 aaa deny-no-resources
17 no 0 aaa deny-server-request-timeout
6 no 0 aaa shutdown-administrative-reset
10 no 0 aaa shutdown-remote-reset
```

show network-access aaa terminate-code brief

```
user@host> show network-access aaa terminate-code brief
Terminate-code:
RADIUS Custom Usage-Count Type Code
17 no 1 aaa deny-authentication-denied
15 no 7 dhcp nak
10 no 1 l2tp session-receive-cdn-avp-missing-secret
10 no 1 ppp bundle-fail-create
1 no 1 ppp lcp-peer-terminate-term-req
10 no 1 ppp lcp-tunnel-disconnected
```

show network-access aaa terminate-code summary

```
user@host> show network-access aaa terminate-code summary
Terminate-code:
Custom Mapping-Count Usage-Count Type
no 1 0 null
no 5 0 aaa
no 4 0 dhcp
yes 1 0 dhcp
no 364 0 l2tp
no 202 0 ppp
```

show network-access address-assignment pool

Syntax	<code>show network-access address-assignment pool <i>pool-name</i></code> <code><logical-system <i>logical-system-name</i>></code> <code><routing-instance <i>routing-instance-name</i>></code>
Release Information	Command introduced in Junos OS Release 9.0.
Description	Display state information for each address-assignment pool.
Options	<p>none—Display information about clients that have obtained addresses from the address-assignment pool.</p> <p>pool <i>pool-name</i>—Display information about the specified address-assignment pool.</p> <p>logical-system <i>logical-system-name</i>—(Optional) Perform this operation on the specified logical system.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Perform this operation on the specified routing instance.</p>
Required Privilege Level	view and system
List of Sample Output	show network-access address-assignment pool on page 1186
Output Fields	Table 99 on page 1186 lists the output fields for the show address-assignment pool command. Output fields are listed in the approximate order in which they appear.

Table 99: show network-access address-assignment pool Output Fields

Field Name	Field Description
IP address	IP address of the client.
Hardware address	MAC address of the client.
Type	Type of client.

Sample Output

show network-access address-assignment pool

```

user@host> show network-access address-assignment pool sunnywest logical-system ls1
routing-instance routinst2
IP address      Hardware address  Type
192.168.2.1     00:05:1b:00:b9:01 DHCP
192.168.2.2     00:05:1b:00:b9:02 DHCP
192.168.2.3     00:05:1b:00:b9:03 DHCP
192.168.2.4     00:05:1b:00:b9:04 DHCP

```

show network-access domain-map

Syntax	show network-access domain-map <statistics>
Release Information	Command introduced in Junos OS Release 10.4.
Description	Display domain map information.
Options	statistics —(Optional) Display domain map statistics.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Verifying and Managing Domain Map Configuration on page 183
List of Sample Output	show network-access domain-map statistics on page 1187
Output Fields	Table 100 on page 1187 lists the output fields for the show network-access domain-map statistics command. Output fields are listed in the approximate order in which they appear.

Table 100: show network-access domain-map Output Fields

Field Name	Field Description
Matched domains	Number of usernames with domain names that are matched.
Unmatched domains	Number of usernames with domain names that are not matched.
Missing domain names	Number of usernames without a domain name.
Stripped username	Number of usernames from which the domain name has been stripped.
Default used	Number of times the default domain map is used.

Sample Output

show network-access domain-map statistics

```

user@host> show network-access domain-map statistics
General domain mapping statistics
  Matched domains: 7
  Unmatched domains: 1
  Missing domain names: 0
  Stripped username: 7
Domain statistics for domain-name: default
  Default used: 1

```

show network-access gx-plus

Syntax	show network-access gx-plus <state statistics sync-state>
Release Information	Command introduced in Junos OS Release 11.2.
Description	Display Gx-Plus provisioning state, synchronization state, and statistics information.
Options	state —(Optional) Display Gx-Plus provisioning state. statistics —(Optional) Display Gx-Plus statistics. sync-state —(Optional) Display Gx-Plus synchronization state.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear network-access gx-plus replay on page 1030 • clear network-access gx-plus statistics on page 1031
List of Sample Output	show network-access gx-plus state on page 1189 show network-access gx-plus statistics on page 1189 show network-access gx-plus sync-state on page 1189
Output Fields	Table 101 on page 1188 lists the output fields for the show network-access gx-plus command. Output fields are listed in the approximate order in which they appear.

Table 101: show network-access gx-plus Output Fields

Field Name	Field Description
Gx-plus state	State of the Gx-Plus application, including the following: <ul style="list-style-type: none"> • Engine created • Partition configured • Configuration active • Diameter interface configured • Total number of entries—Number of provisioned, pending, and terminating subscribers. • Number of pending entries—Number of pending subscribers. • Number of pending logouts—Number of subscribers logging out.
Sync-Event	Type of synchronization event.
Timeout	Number of times notification sent without response.
Gx-plus general counters	Number and state of general events.
Gx-plus sync-event counters	Number and state of synchronization events.

Sample Output

show network-access gx-plus state

```
user@host> show network-access gx-plus state
Gx-plus state:
  Engine created           : yes
  Partition configured    : yes
  Configuration active     : yes
  Diameter interface configured : yes
  Total number of entries  : 0
  Number of pending entries : 0
  Number of pending logouts : 0
```

show network-access gx-plus statistics

```
user@host> show network-access gx-plus statistics
Gx-plus general counters:
  Counter                                     Value
  engine created                             1
  initial config: active                     1
  recovery: process restart                  1
  diameter-app initial config: success       1

Gx-plus sync-event counters:
  Category      Counter      Value
  warm-boot     activated    1

  warm-boot     posted       1

  warm-boot     response     1

  awd           posted       12

  awd           response     12
```

show network-access gx-plus sync-state

```
user@host> show network-access gx-plus sync-state
Gx-plus sync-events:
  Sync-Event      Timeout
  cold-boot       6100
```

show route extensive

List of Syntax	Syntax on page 1190 Syntax (EX Series Switches) on page 1190
Syntax	show route extensive <destination-prefix> <logical-system (all logical-system-name)>
Syntax (EX Series Switches)	show route extensive <destination-prefix>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Display extensive information about the active entries in the routing tables.
Options	<p>none—Display all active entries in the routing table.</p> <p>destination-prefix—(Optional) Display active entries for the specified address or range of addresses.</p> <p>logical-system (all logical-system-name)—(Optional) Perform this operation on all logical systems or on a particular logical system.</p>
Required Privilege Level	view
List of Sample Output	show route extensive on page 1197 show route extensive (Access Route) on page 1203 show route extensive (BGP PIC Edge) on page 1204 show route extensive (FRR and LFA) on page 1204 show route extensive (Route Reflector) on page 1205 show route label detail (Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs) on page 1205 show route label detail (Multipoint LDP with Multicast-Only Fast Reroute) on page 1206
Output Fields	Table 102 on page 1190 describes the output fields for the show route extensive command. Output fields are listed in the approximate order in which they appear.

Table 102: show route extensive Output Fields

Field Name	Field Description
<i>routing-table-name</i>	Name of the routing table (for example, inet.0).
<i>number destinations</i>	Number of destinations for which there are routes in the routing table.

Table 102: show route extensive Output Fields (*continued*)

Field Name	Field Description
<i>number routes</i>	<p>Number of routes in the routing table and total number of routes in the following states:</p> <ul style="list-style-type: none"> • active (routes that are active). • holddown (routes that are in the pending state before being declared inactive). • hidden (routes that are not used because of a routing policy).
<i>route-destination</i> (entry, announced)	<p>Route destination (for example: 10.0.0.1/24). The entry value is the number of route for this destination, and the announced value is the number of routes being announced for this destination. Sometimes the route destination is presented in another format, such as:</p> <ul style="list-style-type: none"> • MPLS-label (for example, 80001). • interface-name (for example, ge-1/0/2). • neighbor-address:control-word-status:encapsulation type:vc-id:source (Layer 2 circuit only; for example, 10.1.1.195:NoCtrlWord:1:1:Local/96). <ul style="list-style-type: none"> • neighbor-address—Address of the neighbor. • control-word-status—Whether the use of the control word has been negotiated for this virtual circuit: NoCtrlWord or CtrlWord. • encapsulation type—Type of encapsulation, represented by a number: (1) Frame Relay DLCI, (2) ATM AAL5 VCC transport, (3) ATM transparent cell transport, (4) Ethernet, (5) VLAN Ethernet, (6) HDLC, (7) PPP, (8) ATM VCC cell transport, (10) ATM VPC cell transport. • vc-id—Virtual circuit identifier. • source—Source of the advertisement: Local or Remote.
TSI	Protocol header information.
label stacking	<p>(Next-to-the-last-hop routing device for MPLS only) Depth of the MPLS label stack, where the label-popping operation is needed to remove one or more labels from the top of the stack. A pair of routes is displayed, because the pop operation is performed only when the stack depth is two or more labels.</p> <ul style="list-style-type: none"> • S=0 route indicates that a packet with an incoming label stack depth of two or more exits this router with one fewer label (the label-popping operation is performed). • If there is no S= information, the route is a normal MPLS route, which has a stack depth of 1 (the label-popping operation is not performed).
[protocol, preference]	<p>Protocol from which the route was learned and the preference value for the route.</p> <ul style="list-style-type: none"> • +—A plus sign indicates the active route, which is the route installed from the routing table into the forwarding table. • -—A hyphen indicates the last active route. • *—An asterisk indicates that the route is both the active and the last active route. An asterisk before a to line indicates the best subpath to the route. <p>In every routing metric except for the BGP LocalPref attribute, a lesser value is preferred. In order to use common comparison routines, Junos OS stores the 1's complement of the LocalPref value in the Preference2 field. For example, if the LocalPref value for Route 1 is 100, the Preference2 value is -101. If the LocalPref value for Route 2 is 155, the Preference2 value is -156. Route 2 is preferred because it has a higher LocalPref value and a lower Preference2 value.</p>

Table 102: show route extensive Output Fields (*continued*)

Field Name	Field Description
Level	(IS-IS only). In IS-IS, a single autonomous system (AS) can be divided into smaller groups called areas. Routing between areas is organized hierarchically, allowing a domain to be administratively divided into smaller areas. This organization is accomplished by configuring Level 1 and Level 2 intermediate systems. Level 1 systems route within an area. When the destination is outside an area, they route toward a Level 2 system. Level 2 intermediate systems route between areas and toward other ASs.
Route Distinguisher	IP subnet augmented with a 64-bit prefix.
PMSI	Provider multicast service interface (MVPN routing table).
Next-hop type	Type of next hop. For a description of possible values for this field, see the Output Field table in the <i>show route detail</i> command.
Next-hop reference count	Number of references made to the next hop.
Flood nexthop branches exceed maximum message	Indicates that the number of flood next-hop branches exceeded the system limit of 32 branches, and only a subset of the flood next-hop branches were installed in the kernel.
Source	IP address of the route source.
Next hop	Network layer address of the directly reachable neighboring system.
via	<p>Interface used to reach the next hop. If there is more than one interface available to the next hop, the name of the interface that is actually used is followed by the word Selected. This field can also contain the following information:</p> <ul style="list-style-type: none"> • Weight—Value used to distinguish primary, secondary, and fast reroute backup routes. Weight information is available when MPLS label-switched path (LSP) link protection, node-link protection, or fast reroute is enabled, or when the standby state is enabled for secondary paths. A lower weight value is preferred. Among routes with the same weight value, load balancing is possible. • Balance—Balance coefficient indicating how traffic of unequal cost is distributed among next hops when a routing device is performing unequal-cost load balancing. This information is available when you enable BGP multipath load balancing.
Label-switched-path lsp-path-name	Name of the LSP used to reach the next hop.
Label operation	MPLS label and operation occurring at this routing device. The operation can be pop (where a label is removed from the top of the stack), push (where another label is added to the label stack), or swap (where a label is replaced by another label).
Offset	Whether the metric has been increased or decreased by an offset value.
Interface	(Local only) Local interface name.
Protocol next hop	Network layer address of the remote routing device that advertised the prefix. This address is used to recursively derive a forwarding next hop.

Table 102: show route extensive Output Fields (*continued*)

Field Name	Field Description
<i>label-operation</i>	MPLS label and operation occurring at this routing device. The operation can be pop (where a label is removed from the top of the stack), push (where another label is added to the label stack), or swap (where a label is replaced by another label).
Indirect next hops	<p>When present, a list of nodes that are used to resolve the path to the next-hop destination, in the order that they are resolved.</p> <p>When BGP PIC Edge is enabled, the output lines that contain Indirect next hop: weight follow next hops that the software can use to repair paths where a link failure occurs. The next-hop weight has one of the following values:</p> <ul style="list-style-type: none"> • 0x1 indicates active next hops. • 0x4000 indicates passive next hops.
State	State of the route (a route can be in more than one state). See the Output Field table in the <i>show route detail</i> command.
Session ID	The BFD session ID number that represents the protection using MPLS fast reroute (FRR) and loop-free alternate (LFA).
Weight	<p>Weight for the backup path. If the weight of an indirect next hop is larger than zero, the weight value is shown.</p> <p>For sample output, see show route table.</p>

Table 102: show route extensive Output Fields (*continued*)

Field Name	Field Description
Inactive reason	<p>If the route is inactive, the reason for its current state is indicated. Typical reasons include:</p> <ul style="list-style-type: none"> • Active preferred—Currently active route was selected over this route. • Always compare MED—Path with a lower multiple exit discriminator (MED) is available. • AS path—Shorter AS path is available. • Cisco Non-deterministic MED selection—Cisco nondeterministic MED is enabled and a path with a lower MED is available. • Cluster list length—Path with a shorter cluster list length is available. • Forwarding use only—Path is only available for forwarding purposes. • IGP metric—Path through the next hop with a lower IGP metric is available. • IGP metric type—Path with a lower OSPF link-state advertisement type is available. • Interior > Exterior > Exterior via Interior—Direct, static, IGP, or EBGp path is available. • Local preference—Path with a higher local preference value is available. • Next hop address—Path with a lower metric next hop is available. • No difference—Path from a neighbor with a lower IP address is available. • Not Best in its group—Occurs when multiple peers of the same external AS advertise the same prefix and are grouped together in the selection process. When this reason is displayed, an additional reason is provided (typically one of the other reasons listed). • Number of gateways—Path with a higher number of next hops is available. • Origin—Path with a lower origin code is available. • OSPF version—Path does not support the indicated OSPF version. • RIB preference—Route from a higher-numbered routing table is available. • Route distinguisher—64-bit prefix added to IP subnets to make them unique. • Route metric or MED comparison—Route with a lower metric or MED is available. • Route preference—Route with a lower preference value is available. • Router ID—Path through a neighbor with a lower ID is available. • Unusable path—Path is not usable because of one of the following conditions: the route is damped, the route is rejected by an import policy, or the route is unresolved. • Update source—Last tiebreaker is the lowest IP address value.
Local AS	Autonomous system (AS) number of the local routing device.
Age	How long the route has been known.
AIGP	Accumulated interior gateway protocol (AIGP) BGP attribute.
Metric	Cost value of the indicated route. For routes within an AS, the cost is determined by IGP and the individual protocol metrics. For external routes, destinations, or routing domains, the cost is determined by a preference value.
MED-plus-IGP	Metric value for BGP path selection to which the IGP cost to the next-hop destination has been added.
TTL-Action	<p>For MPLS LSPs, state of the TTL propagation attribute. Can be enabled or disabled for all RSVP-signaled and LDP-signaled LSPs or for specific VRF routing instances.</p> <p>For sample output, see show route table.</p>

Table 102: show route extensive Output Fields (*continued*)

Field Name	Field Description
Task	Name of the protocol that has added the route.
Announcement bits	List of protocols that announce this route. n-Resolve inet indicates that the route is used for route resolution for next hops found in the routing table. n is an index used by Juniper Networks customer support only.
AS path	<p>AS path through which the route was learned. The letters at the end of the AS path indicate the path origin, providing an indication of the state of the route at the point at which the AS path originated:</p> <ul style="list-style-type: none"> • I—IGP. • E—EGP. • Recorded—The AS path is recorded by the sample process (sampled). • ?—Incomplete; typically, the AS path was aggregated. <p>When AS path numbers are included in the route, the format is as follows:</p> <ul style="list-style-type: none"> • []—Brackets enclose the local AS number associated with the AS path if more than one AS number is configured on the routing device, or if AS path prepending is configured. • { }—Braces enclose AS sets, which are groups of AS numbers in which the order does not matter. A set commonly results from route aggregation. The numbers in each AS set are displayed in ascending order. • ()—Parentheses enclose a confederation. • ([])—Parentheses and brackets enclose a confederation set. <p>NOTE: In Junos OS Release 10.3 and later, the AS path field displays an unrecognized attribute and associated hexadecimal value if BGP receives attribute 128 (attribute set) and you have not configured an independent domain in any routing instance.</p>
validation-state	<p>(BGP-learned routes) Validation status of the route:</p> <ul style="list-style-type: none"> • Invalid—Indicates that the prefix is found, but either the corresponding AS received from the EBGP peer is not the AS that appears in the database, or the prefix length in the BGP update message is longer than the maximum length permitted in the database. • Unknown—Indicates that the prefix is not among the prefixes or prefix ranges in the database. • Unverified—Indicates that origin validation is not enabled for the BGP peers. • Valid—Indicates that the prefix and autonomous system pair are found in the database.
FECs bound to route	Point-to-multipoint root address, multicast source address, and multicast group address when multipoint LDP (M-LDP) inband signaling is configured.
AS path: I <Originator>	(For route reflected output only) Originator ID attribute set by the route reflector.
Primary Upstream	When multipoint LDP with multicast-only fast reroute (MoFRR) is configured, the primary upstream path. MoFRR transmits a multicast join message from a receiver toward a source on a primary path, while also transmitting a secondary multicast join message from the receiver toward the source on a backup path.
RPF Nexthops	When multipoint LDP with MoFRR is configured, the reverse-path forwarding (RPF) next-hop information. Data packets are received from both the primary path and the secondary paths. The redundant packets are discarded at topology merge points due to the RPF checks.

Table 102: show route extensive Output Fields (*continued*)

Field Name	Field Description
Label	Multiple MPLS labels are used to control MoFRR stream selection. Each label represents a separate route, but each references the same interface list check. Only the primary label is forwarded while all others are dropped. Multiple interfaces can receive packets using the same label.
weight	Value used to distinguish MoFRR primary and backup routes. A lower weight value is preferred. Among routes with the same weight value, load balancing is possible.
VC Label	MPLS label assigned to the Layer 2 circuit virtual connection.
MTU	Maximum transmission unit (MTU) of the Layer 2 circuit.
VLAN ID	VLAN identifier of the Layer 2 circuit.
Cluster list	(For route reflected output only) Cluster ID sent by the route reflector.
Originator ID	(For route reflected output only) Address of router that originally sent the route to the route reflector.
Prefixes bound to route	Forwarding equivalent class (FEC) bound to this route. Applicable only to routes installed by LDP.
Communities	Community path attribute for the route. See the Output Field table in the <i>show route detail</i> command for all possible values for this field.
Layer2-info: encaps	Layer 2 encapsulation (for example, VPLS).
control flags	Control flags: none or Site Down.
mtu	Maximum transmission unit (MTU) information.
Label-Base, range	First label in a block of labels and label block size. A remote PE routing device uses this first label when sending traffic toward the advertising PE routing device.
status vector	Layer 2 VPN and VPLS network layer reachability information (NLRI).
Localpref	Local preference value included in the route.
Router ID	BGP router ID as advertised by the neighbor in the open message.
Primary Routing Table	In a routing table group, the name of the primary routing table in which the route resides.
Secondary Tables	In a routing table group, the name of one or more secondary tables in which the route resides.
Originating RIB	Name of the routing table whose active route was used to determine the forwarding next-hop entry in the resolution database. For example, in the case of inet.0 resolving through inet.0 and inet.3, this field indicates which routing table, inet.0 or inet.3, provided the best path for a particular prefix.
Node path count	Number of nodes in the path.

Table 102: show route extensive Output Fields (*continued*)

Field Name	Field Description
Forwarding nexthops	Number of forwarding next hops. The forwarding next hop is the network layer address of the directly reachable neighboring system (if applicable) and the interface used to reach it.

Sample Output

show route extensive

```

user@host> show route extensive
inet.0: 22 destinations, 23 routes (21 active, 0 holddown, 1 hidden)
10.10.0.0/16 (1 entry, 1 announced)
TSI:
KRT in-kernel 10.10.0.0/16 -> {192.168.71.254}
    *Static Preference: 5
        Next-hop reference count: 29
        Next hop: 192.168.71.254 via fxp0.0, selected
        State: <Active NoReadvrt Int Ext>
        Local AS: 69
        Age: 1:34:06
        Task: RT
        Announcement bits (2): 0-KRT 3-Resolve tree 2
        AS path: I

10.31.1.0/30 (2 entries, 1 announced)
    *Direct Preference: 0
        Next hop type: Interface
        Next-hop reference count: 2
        Next hop: via so-0/3/0.0, selected
        State: <Active Int>
        Local AS: 69
        Age: 1:32:40
        Task: IF
        Announcement bits (1): 3-Resolve tree 2
        AS path: I
    OSPF Preference: 10
        Next-hop reference count: 1
        Next hop: via so-0/3/0.0, selected
        State: <Int>
        Inactive reason: Route Preference
        Local AS: 69
        Age: 1:32:40 Metric: 1
        Area: 0.0.0.0
        Task: OSPF
        AS path: I

10.31.1.1/32 (1 entry, 1 announced)
    *Local Preference: 0
        Next hop type: Local
        Next-hop reference count: 7
        Interface: so-0/3/0.0
        State: <Active NoReadvrt Int>
        Local AS: 69
        Age: 1:32:43
        Task: IF
        Announcement bits (1): 3-Resolve tree 2
        AS path: I

```

```

...

10.31.2.0/30 (1 entry, 1 announced)
TSI:
KRT in-kerne1 10.31.2.0/30 -> {10.31.1.6}
    *OSPF    Preference: 10
             Next-hop reference count: 9
             Next hop: via so-0/3/0.0
             Next hop: 10.31.1.6 via ge-3/1/0.0, selected
             State: <Active Int>
             Local AS:    69
             Age: 1:32:19    Metric: 2
             Area: 0.0.0.0
             Task: OSPF
             Announcement bits (2): 0-KRT 3-Resolve tree 2
             AS path: I

...

224.0.0.2/32 (1 entry, 1 announced)
TSI:
KRT in-kerne1 224.0.0.2/32 -> {}
    *PIM     Preference: 0
             Next-hop reference count: 18
             State: <Active NoReadvrt Int>
             Local AS:    69
             Age: 1:34:08
             Task: PIM Recv
             Announcement bits (2): 0-KRT 3-Resolve tree 2
             AS path: I

...

224.0.0.22/32 (1 entry, 1 announced)
TSI:
KRT in-kerne1 224.0.0.22/32 -> {}
    *IGMP    Preference: 0
             Next-hop reference count: 18
             State: <Active NoReadvrt Int>
             Local AS:    69
             Age: 1:34:06
             Task: IGMP
             Announcement bits (2): 0-KRT 3-Resolve tree 2
             AS path: I

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

10.255.70.103/32 (1 entry, 1 announced)
State: <FlashAll>
    *RSVP    Preference: 7
             Next-hop reference count: 6
             Next hop: 10.31.1.6 via ge-3/1/0.0 weight 0x1, selected
             Label-switched-path green-r1-r3
             Label operation: Push 100096
             State: <Active Int>
             Local AS:    69
             Age: 1:28:12    Metric: 2
             Task: RSVP
             Announcement bits (2): 1-Resolve tree 1 2-Resolve tree 2
             AS path: I

```

```

10.255.71.238/32 (1 entry, 1 announced)
  State: <FlashAll>
  *RSVP   Preference: 7
          Next-hop reference count: 6
          Next hop: via so-0/3/0.0 weight 0x1, selected
          Label-switched-path green-r1-r2
          State: <Active Int>
          Local AS: 69
          Age: 1:28:12    Metric: 1
          Task: RSVP
          Announcement bits (2): 1-Resolve tree 1 2-Resolve tree 2
          AS path: I

private1___.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)

...

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

47.0005.80ff.f800.0000.0108.0001.0102.5507.1052/152 (1 entry, 0 announced)
  *Direct Preference: 0
          Next hop type: Interface
          Next-hop reference count: 1
          Next hop: via lo0.0, selected
          State: <Active Int>
          Local AS: 69
          Age: 1:34:07
          Task: IF
          AS path: I

mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)

0 (1 entry, 1 announced)
TSI:
KRT in-kernel 0 /36 -> {}
  *MPLS   Preference: 0
          Next hop type: Receive
          Next-hop reference count: 6
          State: <Active Int>
          Local AS: 69
          Age: 1:34:08    Metric: 1
          Task: MPLS
          Announcement bits (1): 0-KRT
          AS path: I

...

mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
299840 (1 entry, 1 announced)
TSI:
KRT in-kernel 299840 /52 -> {indirect(1048575)}
  *RSVP   Preference: 7/2
          Next hop type: Flood
          Address: 0x9174a30
          Next-hop reference count: 4
          Next hop type: Router, Next hop index: 798
          Address: 0x9174c28
          Next-hop reference count: 2
          Next hop: 8.0.0.2 via lt-1/2/0.9 weight 0x1
          Label-switched-path R2-to-R4-2p2mp

```

```

Label operation: Pop
Next hop type: Router, Next hop index: 1048574
Address: 0x92544f0
Next-hop reference count: 2
Next hop: 7.0.0.2 via lt-1/2/0.7 weight 0x1
Label-switched-path R2-to-R200-p2mp
Label operation: Pop
Next hop: 6.0.0.2 via lt-1/2/0.5 weight 0x8001
Label operation: Pop
State: <Active Int>
Age: 1:29      Metric: 1
Task: RSVP
Announcement bits (1): 0-KRT
AS path: I...

```

800010 (1 entry, 1 announced)

TSI:

```

KRT in-kernel 800010 /36 -> {vt-3/2/0.32769}
  *VPLS Preference: 7
    Next-hop reference count: 2
    Next hop: via vt-3/2/0.32769, selected
    Label operation: Pop
    State: <Active Int>
    Age: 1:31:53
    Task: Common L2 VC
    Announcement bits (1): 0-KRT
    AS path: I

```

vt-3/2/0.32769 (1 entry, 1 announced)

TSI:

```

KRT in-kernel vt-3/2/0.32769.0      /16 -> {indirect(1048574)}
  *VPLS Preference: 7
    Next-hop reference count: 2
    Next hop: 10.31.1.6 via ge-3/1/0.0 weight 0x1, selected
    Label-switched-path green-r1-r3
    Label operation: Push 800012, Push 100096(top)
    Protocol next hop: 10.255.70.103
    Push 800012
    Indirect next hop: 87272e4 1048574
    State: <Active Int>
    Age: 1:31:53      Metric2: 2
    Task: Common L2 VC
    Announcement bits (2): 0-KRT 1-Common L2 VC
    AS path: I
    Communities: target:11111:1 Layer2-info: encaps:VPLS,
    control flags:, mtu: 0
    Indirect next hops: 1
      Protocol next hop: 10.255.70.103 Metric: 2
      Push 800012
      Indirect next hop: 87272e4 1048574
      Indirect path forwarding next hops: 1
        Next hop: 10.31.1.6 via ge-3/1/0.0 weight 0x1
        10.255.70.103/32 Originating RIB: inet.3
        Metric: 2                      Node path count: 1
        Forwarding nexthops: 1
        Nexthop: 10.31.1.6 via ge-3/1/0.0

```

inet6.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)

abcd::10:255:71:52/128 (1 entry, 0 announced)

```

*Direct Preference: 0
  Next hop type: Interface
  Next-hop reference count: 1
  Next hop: via lo0.0, selected
  State: <Active Int>
  Local AS: 69
  Age: 1:34:07
  Task: IF
  AS path: I

fe80::280:42ff:fe10:f179/128 (1 entry, 0 announced)
*Direct Preference: 0
  Next hop type: Interface
  Next-hop reference count: 1
  Next hop: via lo0.0, selected
  State: <Active NoReadvrt Int>
  Local AS: 69
  Age: 1:34:07
  Task: IF
  AS path: I

ff02::2/128 (1 entry, 1 announced)
TSI:
KRT in-kernel ff02::2/128 -> {}
  *PIM Preference: 0
    Next-hop reference count: 18
    State: <Active NoReadvrt Int>
    Local AS: 69
    Age: 1:34:08
    Task: PIM Recv6
    Announcement bits (1): 0-KRT
    AS path: I

ff02::d/128 (1 entry, 1 announced)
TSI:
KRT in-kernel ff02::d/128 -> {}
  *PIM Preference: 0
    Next-hop reference count: 18
    State: <Active NoReadvrt Int>
    Local AS: 69
    Age: 1:34:08
    Task: PIM Recv6
    Announcement bits (1): 0-KRT
    AS path: I

ff02::16/128 (1 entry, 1 announced)
TSI:
KRT in-kernel ff02::16/128 -> {}
  *MLD Preference: 0
    Next-hop reference count: 18
    State: <Active NoReadvrt Int>
    Local AS: 69
    Age: 1:34:06
    Task: MLD
    Announcement bits (1): 0-KRT
    AS path: I

private.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

fe80::280:42ff:fe10:f179/128 (1 entry, 0 announced)
*Direct Preference: 0

```

```

    Next hop type: Interface
    Next-hop reference count: 1
    Next hop: via lo0.16385, selected
    State: <Active NoReadvrt Int>
    Age: 1:34:07
    Task: IF
    AS path: I

green.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)

10.255.70.103:1:3:1/96 (1 entry, 1 announced)
  *BGP   Preference: 170/-101
        Route Distinguisher: 10.255.70.103:1
        Next-hop reference count: 7
        Source: 10.255.70.103
        Protocol next hop: 10.255.70.103
        Indirect next hop: 2 no-forward
        State: <Secondary Active Int Ext>
        Local AS: 69 Peer AS: 69
        Age: 1:28:12 Metric2: 1
        Task: BGP_69.10.255.70.103+179
        Announcement bits (1): 0-green-l2vpn
        AS path: I
        Communities: target:11111:1 Layer2-info: encaps:VPLS,
        control flags:, mtu: 0
        Label-base: 800008, range: 8
        Localpref: 100
        Router ID: 10.255.70.103
        Primary Routing Table bgp.l2vpn.0

10.255.71.52:1:1:1/96 (1 entry, 1 announced)
TSI:
Page 0 idx 0 Type 1 val 8699540
  *L2VPN Preference: 170/-1
        Next-hop reference count: 5
        Protocol next hop: 10.255.71.52
        Indirect next hop: 0 -
        State: <Active Int Ext>
        Age: 1:34:03 Metric2: 1
        Task: green-l2vpn
        Announcement bits (1): 1-BGP.0.0.0.0+179
        AS path: I
        Communities: Layer2-info: encaps:VPLS, control flags:Site-Down,
        mtu: 0
        Label-base: 800016, range: 8, status-vector: 0x9F

10.255.71.52:1:5:1/96 (1 entry, 1 announced)
TSI:
Page 0 idx 0 Type 1 val 8699528
  *L2VPN Preference: 170/-101
        Next-hop reference count: 5
        Protocol next hop: 10.255.71.52
        Indirect next hop: 0 -
        State: <Active Int Ext>
        Age: 1:34:03 Metric2: 1
        Task: green-l2vpn
        Announcement bits (1): 1-BGP.0.0.0.0+179
        AS path: I
        Communities: Layer2-info: encaps:VPLS, control flags:, mtu: 0
        Label-base: 800008, range: 8, status-vector: 0x9F
```

```

...

l2circuit.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

TSI:

10.245.255.63:CtrlWord:4:3:Local/96 (1 entry, 1 announced)
  *L2CKT Preference: 7
    Next hop: via so-1/1/2.0 weight 1, selected
    Label-switched-path my-lsp
    Label operation: Push 100000[0]
    Protocol next hop: 10.245.255.63 Indirect next hop: 86af000 296
    State: <Active Int>
    Local AS: 99
    Age: 10:21
    Task: l2 circuit
    Announcement bits (1): 0-LDP
    AS path: I
    VC Label 100000, MTU 1500, VLAN ID 512

55.0.0.0/24 (1 entry, 1 announced)
TSI:
KRT queued (pending) add
  55.0.0.0/24 -> {Push 300112}
    *BGP Preference: 170/-101
      Next hop type: Router
      Address: 0x925c208
      Next-hop reference count: 2
      Source: 10.0.0.9
      Next hop: 10.0.0.9 via ge-1/2/0.15, selected
      Label operation: Push 300112
      Label TTL action: prop-ttl
      State: <Active Ext>
      Local AS: 7019 Peer AS: 13979
      Age: 1w0d 23:06:56
      AIGP: 25
      Task: BGP_13979.10.0.0.9+56732
      Announcement bits (1): 0-KRT
      AS path: 13979 7018 I
      Accepted
      Route Label: 300112
      Localpref: 100
      Router ID: 10.9.9.1

```

show route extensive (Access Route)

```

user@host> show route 13.160.0.102 extensive
inet.0: 39256 destinations, 39258 routes (39255 active, 0 holddown, 1 hidden)
13.160.0.102/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 13.160.0.102/32 -> {13.160.0.2}
OSPF area : 0.0.0.0, LSA ID : 13.160.0.102, LSA type : Extern
  *Access Preference: 13
    Next-hop reference count: 78472
    Next hop: 13.160.0.2 via fe-0/0/0.0, selected
    State: <Active Int>
  Age: 12
    Task: RPD Unix Domain Server./var/run/rpd_serv.local
    Announcement bits (2): 0-KRT 1-OSPFv2
    AS path: I

```

show route extensive (BGP PIC Edge)

```

user@host> show route 1.1.1.6 extensive
ed.inet.0: 6 destinations, 9 routes (6 active, 0 holddown, 0 hidden)
  1.1.1.6/32 (3 entries, 2 announced)
    State: <CalcForwarding>
TSI:
KRT in-kernel 1.1.1.6/32 -> {indirect(1048574), indirect(1048577)}
Page 0 idx 0 Type 1 val 9219e30
  Nexthop: Self
  AS path: [2] 3 I
  Communities: target:2:1
  Path 1.1.1.6 from 1.1.1.4 Vector len 4. Val: 0
..
    #Multipath Preference: 255
      Next hop type: Indirect
      Address: 0x93f4010
      Next-hop reference count: 2
..
      Protocol next hop: 1.1.1.4
      Push 299824
      Indirect next hop: 944c000 1048574 INH Session ID: 0x3
      Indirect next hop: weight 0x1
      Protocol next hop: 1.1.1.5
      Push 299824
      Indirect next hop: 944c1d8 1048577 INH Session ID: 0x4
      Indirect next hop: weight 0x4000
      State: <ForwardingOnly Int Ext>
      Inactive reason: Forwarding use only
      Age: 25      Metric2: 15
      Validation State: unverified
      Task: RT
      Announcement bits (1): 0-KRT
      AS path: 3 I
      Communities: target:2:1

```

show route extensive (FRR and LFA)

```

user@host> show route 20.31.2.0 extensive
inet.0: 46 destinations, 49 routes (45 active, 0 holddown, 1 hidden)
  20.31.2.0/24 (2 entries, 1 announced)
    State: FlashAll
TSI:
KRT in-kernel 20.31.2.0/24 -> {Push 299776, Push 299792}
  *RSVP Preference: 7/1
    Next hop type: Router, Next hop index: 1048574
    Address: 0xbbbc010
    Next-hop reference count: 5
    Next hop: 10.31.1.2 via ge-2/1/8.0 weight 0x1, selected
    Label-switched-path europa-d-to-europa-e
    Label operation: Push 299776
    Label TTL action: prop-ttl
    Session Id: 0x201
    Next hop: 10.31.2.2 via ge-2/1/4.0 weight 0x4001
    Label-switched-path europa-d-to-europa-e
    Label operation: Push 299792
    Label TTL action: prop-ttl
    Session Id: 0x202
    State: Active Int
    Local AS: 100
    Age: 5:31 Metric: 2

```



```

Task: RSVP
Announcement bits (1): 0-KRT
AS path: I
OSPF Preference: 10
Next hop type: Router, Next hop index: 615
Address: 0xb9d78c4
Next-hop reference count: 7
Next hop: 10.31.1.2 via ge-2/1/8.0, selected
Session Id: 0x201
State: Int
Inactive reason: Route Preference
Local AS: 100
Age: 5:35 Metric: 3
Area: 0.0.0.0
Task: OSPF
AS path: I

```

show route extensive (Route Reflector)

```

user@host> show route extensive
1.0.0.0/8 (1 entry, 1 announced)

TSI:
KRT in-kernel 1.0.0.0/8 -> {indirect(40)}
*BGP Preference: 170/-101
Source: 192.168.4.214
Protocol next hop: 207.17.136.192 Indirect next hop: 84ac908 40
State: <Active Int Ext>
Local AS: 10458 Peer AS: 10458
Age: 3:09 Metric: 0 Metric2: 0
Task: BGP_10458.192.168.4.214+1033
Announcement bits (2): 0-KRT 4-Resolve inet.0
AS path: 3944 7777 I <Originator>
Cluster list: 1.1.1.1
Originator ID: 10.255.245.88
Communities: 7777:7777
Localpref: 100
Router ID: 4.4.4.4
Indirect next hops: 1
    Protocol next hop: 207.17.136.192 Metric: 0
    Indirect next hop: 84ac908 40
    Indirect path forwarding next hops: 0
    Next hop type: Discard

```

show route label detail (Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs)

```

user@host> show route label 299872 detail
mpls.0: 13 destinations, 13 routes (13 active, 0 holddown, 0 hidden)
299872 (1 entry, 1 announced)
*LDP Preference: 9
Next hop type: Flood
Next-hop reference count: 3
Address: 0x9097d90
Next hop: via vt-0/1/0.1
Next-hop index: 661
Label operation: Pop
Address: 0x9172130
Next hop: via so-0/0/3.0
Next-hop index: 654
Label operation: Swap 299872
State: **Active Int>

```

```

Local AS: 1001
Age: 8:20      Metric: 1
Task: LDP
Announcement bits (1): 0-KRT
AS path: I
FECs bound to route: P2MP root-addr 10.255.72.166, grp 232.1.1.1,
src 192.168.142.2

```

show route label detail (Multipoint LDP with Multicast-Only Fast Reroute)

```

user@host> show route label 301568 detail

mpls.0: 18 destinations, 18 routes (18 active, 0 holddown, 0 hidden)
301568 (1 entry, 1 announced)
  *LDP    Preference: 9
    Next hop type: Flood
    Address: 0x2735208
    Next-hop reference count: 3
    Next hop type: Router, Next hop index: 1397
    Address: 0x2735d2c
    Next-hop reference count: 3
    Next hop: 1.3.8.2 via ge-1/2/22.0
    Label operation: Pop
    Load balance label: None;
    Next hop type: Router, Next hop index: 1395
    Address: 0x2736290
    Next-hop reference count: 3
    Next hop: 1.3.4.2 via ge-1/2/18.0
    Label operation: Pop
    Load balance label: None;
    State: <Active Int AckRequest MulticastRPF>
    Local AS: 10
    Age: 54:05      Metric: 1
    Validation State: unverified
    Task: LDP
    Announcement bits (1): 0-KRT
    AS path: I
    FECs bound to route: P2MP root-addr 1.1.1.1, grp: 232.1.1.1, src:
192.168.219.11
      Primary Upstream : 1.1.1.3:0--1.1.1.2:0
        RPF Nexthops :
          ge-1/2/15.0, 1.2.94.1, Label: 301568, weight: 0x1
          ge-1/2/14.0, 1.2.3.1, Label: 301568, weight: 0x1
      Backup Upstream : 1.1.1.3:0--1.1.1.6:0
        RPF Nexthops :
          ge-1/2/20.0, 1.2.96.1, Label: 301584, weight: 0xffffe
          ge-1/2/19.0, 1.3.6.1, Label: 301584, weight: 0xffffe

```

show services subscriber bandwidth

Syntax	<pre>show services subscriber bandwidth <client-id <i>client-id</i>> <interface <i>interface-name</i>> <top-talkers <i>top-talkers</i>> <ip-address <i>ip-address</i>> <service-interface <i>interface-name</i>> <top-talkers <i>top-talkers</i>></pre>
Release Information	Command introduced in Junos OS Release 10.2.
Description	Display bandwidth information about subscribers with the specified criteria. The bandwidth is computed at fixed intervals on the MS-DPC and only the last interval is used for comparison.
Options	<p>client-id <i>client-id</i>—(Optional) Displays bandwidth information for the subscriber with this client ID. The client ID is a generated identifier assigned to each packet-triggered subscriber known to the router.</p> <p>interface <i>interface-name</i>—(Optional) Displays bandwidth information for the subscriber with this underlying interface name.</p> <p>ip-address <i>ip-address</i>—(Optional) Displays bandwidth information for the subscriber with this IPv4 address.</p> <p>service-interface <i>interface-name</i>—(Optional) Displays bandwidth information for the subscriber with this service interface name.</p> <p>top-talkers <i>number-top-talkers</i>—(Optional) Displays bandwidth information for the specified number of subscribers using the most bandwidth based on the input-bps or output-bps values for the interface or service interface.</p>
Required Privilege Level	view
List of Sample Output	show services subscriber bandwidth client-id on page 1208
Output Fields	Table 103 on page 1207 lists the output fields for the show services subscriber bandwidth command. Output fields are listed in the approximate order in which they appear.

Table 103: show services subscriber bandwidth Output Fields

Field Name	Field Description
client-id	Client identifier.
input-bps	Ingress bandwidth in bytes per second.
output-bps	Egress bandwidth in bytes per second.
input-pps	Ingress bandwidth in packets per second.
output-pps	Egress bandwidth in packets per second.

Sample Output

show services

subscriber bandwidth client-id

```
user@host> show services subscriber bandwidth client-id 1
client-id  input-bps  output-bps  input-pps  output-pps
1           20          20          1000       1000
```

show services subscriber dynamic-policies

Syntax	show services subscriber dynamic-policies client-id <i>client-id</i>
Release Information	Command introduced in Junos OS Release 10.2.
Description	Display information about the active dynamic policies applied to the specified subscriber.
Options	client-id <i>client-id</i> —Displays information about the active dynamic policies applied to the subscriber with this client ID. The client ID is a generated identifier assigned to each packet-triggered subscriber known to the router.
Required Privilege Level	view
List of Sample Output	show services subscriber dynamic-policies client-id on page 1210
Output Fields	Table 104 on page 1209 lists the output fields for the show services subscriber dynamic-policies command. Output fields are listed in the approximate order in which they appear.

Table 104: show services subscriber dynamic-policies Output Fields

Field Name	Field Description
Subscriber session	Client identifier.
Policy name	Dynamic policy identifier.
rpr	Rule precedence for the dynamic policy.
d	Direction of the dynamic policy.
Template	Service rule associated with the dynamic policy.
tpr	Term precedence.
ra	Remote address.
rm	Remote address mask.
lpl	Lower boundary for the local port range.
lph	Upper boundary for the local port range.
rpl	Lower boundary for the remote port range.
rph	Upper boundary for the remote port range.
p	Protocol.

Table 104: show services subscriber dynamic-policies Output Fields (*continued*)

Field Name	Field Description
a-f	Action.
a-s	Type of statistics collection and aggregation.
a-fc	Forwarding class.
a-p-l	Policer instance.
a-p-bw	Policer bandwidth.
a-p-mbs	Policer maximum burst size.
a-fu	Unit number for forwarding instance.
anl	Application names.
agl	Application group name.

Sample Output

show services

subscriber dynamic-policies client-id

```

user@host> show services subscriber dynamic-policies client-id 1
Subscriber session 1 policy
  Policy name: 1311465998724890695
  rpr: 200
  d: input-output
    Template: __svc_rule__
    tpr: 100
    ra: 0.0.0.0
    rm: 0
    lpl: 0
    lph: 65535
    rpl: 0
    rph: 65535
    p: 0
    a-f: accept forwarding-class
    a-s:
    a-fc: assured-forwarding
    a-p-i: 0
    a-p-bw: 0
    a-p-mbs: 0
    a-fu: 0
    anl: junos:http
    agl: junos:web
    Template: __svc_rule__
    tpr: 100
    ra: 10.10.10.0
    rm: 0
    lpl: 0

```

```
lph: 65535  
rpl: 0  
rph: 65535  
p: 0  
a-f: accept  
a-s:  
a-fc:  
a-p-i: 0  
a-p-bw: 0  
a-p-mbs: 0  
a-fu: 0  
anl:  
agl:
```

show services subscriber flows

Syntax	show services subscriber flows client-id <i>client-id</i>
Release Information	Command introduced in Junos OS Release 10.2. Offload status for flows using Juniper Forwarding Mechanism (JFM) added in Junos OS Release 12.1.
Description	Display information about the data flows associated with the specified subscriber. Offloading using JFM is supported only on MX Series routers with Modular Port Concentrators (MPCs) for the packet-triggered subscribers and policy control (PTSP) plug-in.
Options	client-id <i>client-id</i> —Displays information about the data flows associated with the subscriber identified by this client ID. The client ID is a generated identifier assigned to each packet-triggered subscriber known to the router.
Required Privilege Level	view
List of Sample Output	show services subscriber flows client-id on page 1213 show services subscriber flows client-id for offloading using JFM on page 1213
Output Fields	Table 105 on page 1212 lists the output fields for the show services subscriber flows command. Output fields are listed in the approximate order in which they appear.

Table 105: show services subscriber flows Output Fields

Field Name	Field Description
Subscriber session	Client identifier.
Number of data flows	Number of data sessions associated with this subscriber.
Data flow high-water-mark	High water mark number of concurrent data sessions for this subscriber. This value is never reset during the login session.
5-tuple	5 tuple information for each flow.
Application-ID	Application ID for each flow.
Policy-name	Service rule name for each flow.
Dir	Direction of each flow.
Packets	Information about counter statistics for each flow.
Bytes	Information about counter statistics for each flow.

Table 105: show services subscriber flows Output Fields (*continued*)

Field Name	Field Description
Off	The status of offload to Packet Forwarding Engine using JFM. The various options are: <ul style="list-style-type: none"> • Not Offloaded (-) • Offload requested but not completed (R) • Offload requested and completed (O)
Action	Action of the service rule for each flow.

Sample Output

show services
subscriber flows client-id

```

user@host> show services subscriber flows client-id 1
Subscriber session 1
Number of data flows: 1
Data flows high-water-mark: 8180
5-tuple
80.1.1.2:45287->90.2.255.2:80,6      Application-ID      Policy-name      Dir
junos:http      ptsp-appl/23      I
Packets      Bytes      Action
6      511      C-T

```

show services subscriber flows client-id for offloading using JFM

```

user@host> show services subscriber flows client-id 1
5-tuple      Application-ID      Policy-name      Dir      Packets
Bytes Off Action
80.1.1.2:45288->90.2.255.2:80,6      junos:http      ptsp-appl/23      I      12
1511      -      C-T
80.1.1.2:45287->90.2.255.2:80,6      junos:http      ptsp-appl/23      I      6
511      R      C-T
80.1.1.2:45287->91.4.2.200:80,6      junos:http      ptsp-appl/23      I      645
5329      0      C-T

```

show services subscriber sessions

Syntax	show services subscriber sessions <brief detail summary> <client-id <i>client-id</i>> <interface <i>interface-name</i>> <ip-address <i>ip-address</i>> <routing-instance <i>routing-instance-name</i>> <service-interface <i>interface-name</i>> <user-id <i>user-id</i>>
Release Information	Command introduced in Junos OS Release 10.2.
Description	Display information about the active packet-triggered subscriber sessions on the router.
Options	<p>brief detail summary—(Optional) Display the specified level of output. The default level is brief.</p> <p>client-id <i>client-id</i>—(Optional) Displays information about the active packet-triggered subscriber sessions for this client ID. The client ID is a generated identifier assigned to each packet-triggered subscriber known to the router.</p> <p>interface <i>interface-name</i>—(Optional) Displays information about the active packet-triggered subscriber sessions for the subscriber with this underlying interface name.</p> <p>ip-address <i>ip-address</i>—(Optional) Displays information about the active packet-triggered subscriber sessions for the subscriber with this IP address.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Displays information about the active packet-triggered subscriber sessions for the subscriber on this routing instance.</p> <p>service-interface <i>interface-name</i>—(Optional) Displays information about the active packet-triggered subscriber sessions for the subscriber with this service interface name.</p> <p>user-id <i>user-id</i>—(Optional) Displays information about the active packet-triggered subscriber sessions with this user ID.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• clear services subscriber sessions on page 1033
List of Sample Output	show services subscriber sessions client-id summary on page 1215 show services subscriber sessions client-id on page 1215 show services subscriber sessions client-id detail on page 1215 show services subscriber sessions detail on page 1215
Output Fields	Table 106 on page 1215 lists the output fields for the show services subscriber sessions command. Output fields are listed in the approximate order in which they appear.

Table 106: show services subscriber sessions Output Fields

Field Name	Field Description
Client-ID	Client identifier.
IP-address	IPv4 address.
Underlying-interface	Interface where services are applied.
User-name	Subscriber identifier.
Service interface name	Location of the MS-DPC on which the subscriber is instantiated.
Routing instance	Routing instance on which the subscriber is instantiated.
State	State of the subscriber.

Sample Output

show services
subscriber sessions client-id summary

```
user@host> show services subscriber sessions client-id 1 summary
1
```

show services
subscriber sessions client-id

```
user@host> show services subscriber sessions client-id 1
Client-ID      IP-address      Underlying-interface  User-name
1              80.1.1.2        ge-1/3/2.1           ip80.1.1.2@default
```

show services
subscriber sessions
client-id detail

```
user@host> show services subscriber sessions client-id 1 detail
Subscriber session 1
  User name: ip80.1.1.2@default
  Interface name: ge-1/3/2.1
  User IP address: 80.1.1.2
  Service interface name: ms-2/0/0
  Routing instance: default
  State: logged in
  Login time: Tue Dec 29 19:56:07 2009
  1 service session(s) instantiated:
  Service session 1323423760868442114 => State: activated
```

show services subscriber sessions detail

```
user@host> show services subscriber sessions detail
Subscriber session 4503599627370515
  User name: 00a0.c9b2.551e@kanlab.jnpr.net<6.6.0.11>:glacier:ge-1/0/6.0[:0-0]
  Interface name: ge-1/0/3.8
  User IP address: 6.6.0.11
```

```
Service interface name: ms-4/0/0
Partition name: radius-p1
State: logged in
Subscriber profile: enable_HCM_only
Login time: Mon Oct  4 14:32:51 2010
1 service session(s) instantiated:
Service session radius => State: activated
```

show services subscriber statistics

Syntax	show services subscriber statistics client-id <i>client-id</i>
Release Information	Command introduced in Junos OS Release 10.2.
Description	Display information about the data traffic statistics for the specified packet-triggered subscriber and for each service rule attached to that subscriber.
Options	client-id <i>client-id</i> —Displays information about the data traffic statistics associated with the subscriber identified by this client ID. The client ID is a generated identifier assigned to each packet-triggered subscriber known to the router.
Required Privilege Level	view
List of Sample Output	show services subscriber statistics client-id by rule on page 1217 show services subscriber statistics client-id by application on page 1217
Output Fields	Table 107 on page 1217 lists the output fields for the show services subscriber statistics command. Output fields are listed in the approximate order in which they appear.

Table 107: show services subscriber statistics Output Fields

Field Name	Field Description
Aggregation-level	Type of statistics collected — subscriber and service rule or application.
Name/Id	Identifier for Aggregation-level field.
Packets-in	Number of ingress packets.
Packets-out	Number of egress packets.
Bytes-in	Number of ingress bytes.
Bytes-out	Number of egress bytes.

Sample Output

show services
subscriber statistics client-id by rule

```
user@host> show services subscriber statistics client-id 1
Aggregation-level Name/Id   Packets-in Packets-out Bytes-in Bytes-out
subscriber        1             5           5       1000    1000
dynamic rule      ptsp-rule     5           5       1000    1000
```

Sample Output

show services

subscriber statistics client-id by application

```
user@host> show services subscriber statistics client-id 1
```

Aggregation-level	Name/Id	Packets-in	Packets-out	Bytes-in	Bytes-out
subscriber	1	4358118	3630087	371167451	3301658453
application group	any	4358118	3631768	371167451	3304179953

show static-subscribers sessions

Syntax	show static-subscribers sessions <code><group group-name></code> <code><interface interface-name></code>
Release Information	Command introduced in Junos OS Release 9.6.
Description	Display information about the subscriber sessions for all static subscribers, all static subscribers on an interface group, or a single subscriber on an interface.
Options	<p>group-name—(Optional) Display session information for static subscribers on all interfaces in the specified group.</p> <p>interface-name—(Optional) Display session information for the static subscriber on the specified in the specified group.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Subscribers on Static Interfaces Overview on page 463
List of Sample Output	show static-subscribers sessions on page 1220 show static-subscribers sessions group on page 1220 show static-subscribers sessions interface on page 1220
Output Fields	Table 108 on page 1219 lists the output fields for the show static-subscribers sessions command. Output fields are listed in the approximate order in which they appear.

Table 108: show static-subscribers sessions Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the interface.	None specified
State	State of the static subscriber session: <ul style="list-style-type: none"> • authenticating—Subscriber is being authenticated. • activating client—Client is being activated. • activating services—Subscriber services are being activated. • deactivating client—Client is being deactivated. • deactivating services—Subscriber services are being deactivated. • initializing—Process is initializing. • logged in—Subscriber is logged in to the interface. • logged out—Subscriber is logged out of the interface. • processing statistics—Session statistics are being processed. • terminating session—Subscriber session is being terminated. 	None specified
Group	Name of the interface group to which the interface belongs.	None specified

Table 108: show static-subscribers sessions Output Fields (*continued*)

Field Name	Field Description	Level of Output
User Name	Username used for the static subscriber. Can be the interface name.	None specified

Sample Output

show static-subscribers sessions

```
user@host> show static-subscribers sessions
```

Static subscriber information:

Interface	State	Group	User Name
ge-9/1/0.1	logged out	SS1	ge-9-1-0.1
ge-9/1/0.10	logged out	SS1	ge-9-1-0.10
ge-9/1/0.100	logged out	SS1	ge-9-1-0.100
ge-9/1/0.11	logged out	SS1	ge-9-1-0.11
ge-9/1/0.12	logged out	SS1	ge-9-1-0.12
ge-9/1/0.13	logged out	SS1	ge-9-1-0.13
ge-9/1/0.14	logged out	SS1	ge-9-1-0.14
ge-9/1/0.15	logged out	SS1	ge-9-1-0.15
ge-9/1/0.16	logged out	SS1	ge-9-1-0.16
ge-9/1/0.17	logged out	SS1	ge-9-1-0.17
ge-9/1/0.18	logged out	SS1	ge-9-1-0.18
ge-9/1/0.19	logged out	SS1	ge-9-1-0.19
ge-9/1/0.2	logged out	SS1	ge-9-1-0.2
ge-9/1/0.20	logged out	SS1	ge-9-1-0.20
ge-9/1/0.21	logged out	SS1	ge-9-1-0.21

show static-subscribers sessions group

```
user@host> show static-subscribers sessions group boston
```

Interface	State	Group	User Name
ge-0/0/1.1	logged in	boston	ge-0/0/1.1
ge-0/0/1.2	logged in	boston	ge-0/0/1.2

show static-subscribers sessions interface

```
user@host> show static-subscribers sessions interface ge-0/0/1.1
```

Interface	State	Group	User Name
ge-0/0/1.1	logged in	foo	ge-0/0/1.1

show subscribers

Syntax show subscribers
 <detail | extensive | terse>
 <aci-interface-set-name *aci-interface-set-name*>
 <address *address*>
 <agent-circuit-identifier *agent-circuit-identifier-substring*>
 <client-type *client-type*>
 <count>
 <id>
 <interface *interface*>
 <logical-system *logical-system*>
 <mac-address *mac-address*>
 <physical-interface *physical-interface-name*>
 <profile-name *profile-name*>
 <routing-instance *routing-instance*>
 <stacked-vlan-id *stacked-vlan-id*>
 <subscriber-state *subscriber-state*>
 <user-name *user-name*>
 <vci *vci-identifier*>
 <vpi *vpi-identifier*>
 <vlan-id *vlan-id*>

Release Information Command introduced in Junos OS Release 9.3.
 Command introduced in Junos OS Release 9.3 for EX Series switches.
client-type, **mac-address**, **subscriber-state**, and **extensive** options introduced in Junos OS Release 10.2.
count option usage with other options introduced in Junos OS Release 10.2.
 Command introduced in Junos OS Release 11.1 for the QFX Series.
 Options **aci-interface-set-name** and **agent-circuit-identifier** introduced in Junos OS Release 12.2.
 The **physical-interface** and **user-name** options introduced in Junos OS Release 12.3.
 Options **vci** and **vpi** introduced in Junos OS Release 12.3R3 and supported in later 12.3Rx releases.
 Options **vci** and **vpi** supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)
 Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Display information for active subscribers.

Options **detail | extensive | terse**—(Optional) Display the specified level of output.

aci-interface-set-name—(Optional) Display all dynamic subscriber sessions that use the specified agent circuit identifier (ACI) interface set. Use the ACI interface set name generated by the router, such as aci-1003-ge-1/0/0.4001, and not the actual ACI value found in the DHCP or PPPoE control packets.

address—(Optional) Display subscribers whose IP address matches the specified address. You must specify the IPv4 or IPv6 address prefix without a netmask (for example, 192.168.17.1). If you specify the IP address as a prefix with a netmask (for example,

192.168.17.1/32), the router displays a message that the IP address is invalid, and rejects the command.

agent-circuit-identifier-substring—(Optional) Display all dynamic subscriber sessions whose ACI value matches the specified substring.

client-type—(Optional) Display subscribers whose client type matches the specified client type (DHCP, L2TP, PPP, PPPOE, VLAN, or static).

count—(Optional) Display the count of total subscribers and active subscribers for any specified option. You can use the ***count*** option alone or with the ***address***, ***client-type***, ***interface***, ***logical-system***, ***mac-address***, ***profile-name***, ***routing-instance***, ***stacked-vlan-id***, ***subscriber-state***, or ***vlan-id*** options.

id—(Optional) Display a specific subscriber session whose session id matches the specified subscriber ID. You can display subscriber IDs by using the ***show subscribers extensive*** or the ***show subscribers interface extensive*** commands.

interface—(Optional) Display subscribers whose interface matches the specified interface.

logical-system—(Optional) Display subscribers whose logical system matches the specified logical system.

mac-address—(Optional) Display subscribers whose MAC address matches the specified MAC address.

physical-interface-name—(M120, M320, and MX Series routers only) (Optional) Display subscribers whose physical interface matches the specified physical interface.

profile-name—(Optional) Display subscribers whose dynamic profile matches the specified profile name.

routing-instance—(Optional) Display subscribers whose routing instance matches the specified routing instance.

stacked-vlan-id—(Optional) Display subscribers whose stacked VLAN ID matches the specified stacked VLAN ID.

subscriber-state—(Optional) Display subscribers whose subscriber state matches the specified subscriber state (ACTIVE, CONFIGURED, INIT, TERMINATED, or TERMINATING).

user-name—(M120, M320, and MX Series routers only) (Optional) Display subscribers whose username matches the specified subscriber name.

vci-identifier—(MX Series routers with MPCs and ATM MICs with SFP only) (Optional) Display active ATM subscribers whose ATM virtual circuit identifier (VCI) matches the specified VCI identifier. The range of values is **0** through **255**.

vpi-identifier—(MX Series routers with MPCs and ATM MICs with SFP only) (Optional) Display active ATM subscribers whose ATM virtual path identifier (VPI) matches the specified VPI identifier. The range of values is **0** through **65535**.

vlan-id—(Optional) Display subscribers whose VLAN ID matches the specified VLAN ID, regardless of whether the subscriber uses a single-tagged or double-tagged VLAN. For subscribers using a double-tagged VLAN, this option displays subscribers where the inner VLAN tag matches the specified VLAN ID. To display only subscribers where the specified value matches only double-tagged VLANs, use the **stacked-vlan-id** option to match the outer VLAN tag.



NOTE: Due to display limitations, logical system and routing instance output values are truncated when necessary.

Required Privilege Level view

Related Documentation

- [show subscribers summary on page 1239](#)
- *Verifying and Managing Agent Circuit Identifier-Based Dynamic VLAN Configuration*

List of Sample Output

- [show subscribers \(IPv4\) on page 1227](#)
- [show subscribers \(IPv6\) on page 1227](#)
- [show subscribers \(IPv4 and IPv6 Dual Stack\) on page 1227](#)
- [show subscribers \(LNS on MX Series Routers\) on page 1228](#)
- [show subscribers \(L2TP Switched Tunnels\) on page 1228](#)
- [show subscribers client-type dhcp detail on page 1228](#)
- [show subscribers count on page 1228](#)
- [show subscribers address detail \(IPv6\) on page 1229](#)
- [show subscribers detail \(IPv4\) on page 1229](#)
- [show subscribers detail \(IPv6\) on page 1229](#)
- [show subscribers detail \(IPv6 Static Demux Interface\) on page 1230](#)
- [show subscribers detail \(L2TP LNS Subscribers on MX Series Routers\) on page 1230](#)
- [show subscribers detail \(L2TP Switched Tunnels\) on page 1230](#)
- [show subscribers detail \(Tunneled Subscriber\) on page 1231](#)
- [show subscribers detail \(IPv4 and IPv6 Dual Stack\) on page 1231](#)
- [show subscribers detail \(ACI Interface Set Session\) on page 1232](#)
- [show subscribers detail \(PPPoE Subscriber Session with ACI Interface Set\) on page 1232](#)
- [show subscribers extensive on page 1232](#)
- [show subscribers extensive \(RPF Check Fail Filter\) on page 1233](#)
- [show subscribers extensive \(L2TP LNS Subscribers on MX Series Routers\) on page 1233](#)
- [show subscribers extensive \(IPv4 and IPv6 Dual Stack\) on page 1233](#)
- [show subscribers extensive \(Effective Shaping-Rate\) on page 1234](#)
- [show subscribers aci-interface-set-name detail \(Subscriber Sessions Using Specified ACI Interface Set\) on page 1235](#)
- [show subscribers agent-circuit-identifier detail \(Subscriber Sessions Using Specified ACI Substring\) on page 1235](#)
- [show subscribers interface extensive on page 1236](#)
- [show subscribers logical-system terse on page 1236](#)
- [show subscribers physical-interface count on page 1237](#)
- [show subscribers routing-instance inst1 count on page 1237](#)

[show subscribers stacked-vlan-id detail on page 1237](#)

[show subscribers stacked-vlan-id vlan-id detail \(Combined Output\) on page 1237](#)

[show subscribers stacked-vlan-id vlan-id interface detail \(Combined Output for a Specific Interface\) on page 1237](#)

[show subscribers user-name detail on page 1237](#)

[show subscribers vlan-id on page 1238](#)

[show subscribers vlan-id detail on page 1238](#)

[show subscribers vpi vci extensive \(PPPoE-over-ATM Subscriber Session\) on page 1238](#)

Output Fields [Table 109 on page 1224](#) lists the output fields for the **show subscribers** command. Output fields are listed in the approximate order in which they appear.

Table 109: show subscribers Output Fields

Field Name	Field Description
Interface	Interface associated with the subscriber. The router or switch displays subscribers whose interface matches or begins with the specified interface. The * character indicates a continuation of addresses for the same session.
IP Address/VLAN ID	Subscriber IP address or VLAN ID associated with the subscriber in the form <i>tpid.vlan-id</i> No IP address or VLAN ID is assigned to an L2TP tunnel-switched session. For these subscriber sessions the value is Tunnel-switched .
User Name	Name of subscriber.
LS:RI	Logical system and routing instance associated with the subscriber.
Type	Subscriber client type (DHCP, L2TP, PPP, PPPoE, STATIC-INTERFACE, VLAN).
IP Address	Subscriber IPv4 address.
IP Netmask	Subscriber IP netmask.
Primary DNS Address	IP address of primary DNS server.
Secondary DNS Address	IP address of secondary DNS server.
Primary WINS Address	IP address of primary WINS server.
Secondary WINS Address	IP address of secondary WINS server.
IPv6 Address	Subscriber IPv6 address, or multiple addresses.
IPv6 Prefix	Subscriber IPv6 prefix. If you are using DHCPv6 prefix delegation, this is the delegated prefix.
IPv6 User Prefix	IPv6 prefix obtained through ND/RA.
IPv6 Address Pool	Subscriber IPv6 address pool. The IPv6 address pool is used to allocate IPv6 prefixes to the DHCPv6 clients.

Table 109: show subscribers Output Fields (*continued*)

Field Name	Field Description
IPv6 Network Prefix Length	Length of the network portion of the IPv6 address.
IPv6 Prefix Length	Length of the subscriber IPv6 prefix.
Logical System	Logical system associated with the subscriber.
Routing Instance	Routing instance associated with the subscriber.
Interface Type	Whether the subscriber interface is Static or Dynamic .
Interface Set	Internally generated name of the dynamic ACI interface set used by the subscriber session.
Interface Set Type	Interface type of the ACI interface set: Dynamic . This is the only ACI interface set type currently supported.
Interface Set Session ID	Identifier of the dynamic ACI interface set entry in the session database.
Underlying Interface	Name of the underlying interface for the subscriber session.
Dynamic Profile Name	Dynamic profile used for the subscriber.
Dynamic Profile Version	Version number of the dynamic profile used for the subscriber.
MAC Address	MAC address associated with the subscriber.
State	Current state of the subscriber session (Init , Configured , Active , Terminating , Tunneled).
L2TP State	Current state of the L2TP session, Tunneled or Tunnel-switched . When the value is Tunnel-switched , two entries are displayed for the subscriber; the first entry is at the LNS interface on the LTS and the second entry is at the LAC interface on the LTS.
Tunnel switch Profile Name	Name of the L2TP tunnel switch profile that initiates tunnel switching.
Local IP Address	IP address of the local gateway (LAC).
Remote IP Address	IP address of the remote peer (LNS).
VLAN Id	VLAN ID associated with the subscriber in the form <i>tpid.vlan-id</i> .
Stacked VLAN Id	Stacked VLAN ID associated with the subscriber in the form <i>tpid.vlan-id</i> .
RADIUS Accounting ID	RADIUS accounting ID associated with the subscriber.
Agent Circuit ID	Option 82 agent circuit ID associated with the subscriber. The ID is displayed as an ASCII string unless the value has nonprintable characters, in which case it is displayed in hexadecimal format.

Table 109: show subscribers Output Fields (*continued*)

Field Name	Field Description
Agent Remote ID	Option 82 agent remote ID associated with the subscriber. The ID is displayed as an ASCII string unless the value has nonprintable characters, in which case it is displayed in hexadecimal format.
DHCP Relay IP Address	IP address used by the DHCP relay agent.
ATM VPI	(MX Series routers with MPCs and ATM MICs with SFP only) ATM virtual path identifier (VPI) on the subscriber's physical interface.
ATM VCI	(MX Series routers with MPCs and ATM MICs with SFP only) ATM virtual circuit identifier (VCI) for each VPI configured on the subscriber interface.
Login Time	Date and time at which the subscriber logged in.
Effective shaping-rate	Actual downstream traffic shaping rate for the subscriber, in kilobits per second.
IPv4 rpf-check Fail Filter Name	Name of the filter applied by the dynamic profile to IPv4 packets that fail the RPF check.
IPv6 rpf-check Fail Filter Name	Name of the filter applied by the dynamic profile to IPv6 packets that fail the RPF check.
DHCP Options	len = number of hex values in the message. The hex values specify the type, length, value (TLV) for DHCP options, as defined in RFC 2132.
Session ID	ID number for a subscriber service session.
Underlying Session ID	For DHCPv6 subscribers on a PPPoE network, displays the session ID of the underlying PPPoE interface.
Service Sessions	Number of service sessions (that is, a service activated using RADIUS CoA) associated with the subscribers.
Service Session Name	Service session profile name.
Session Timeout (seconds)	Number of seconds of access provided to the subscriber before the session is automatically terminated.
Idle Timeout (seconds)	Number of seconds subscriber can be idle before the session is automatically terminated.
IPv6 Delegated Address Pool	Name of the pool used for DHCPv6 prefix delegation.
IPv6 Delegated Network Prefix Length	Length of the prefix configured for the IPv6 delegated address pool.
IPv6 Interface Address	Address assigned by the Framed-lpv6-Prefix AAA attribute.
IPv6 Framed Interface Id	Interface ID assigned by the Framed-Interface-Id AAA attribute.

Table 109: show subscribers Output Fields (*continued*)

Field Name	Field Description
ADF IPv4 Input Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv4 input filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
ADF IPv4 Output Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv4 output filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
ADF IPv6 Input Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv6 input filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
ADF IPv6 Output Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv6 output filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
IPv4 Input Filter Name	Name assigned to the IPv4 input filter (client or service session).
IPv4 Output Filter Name	Name assigned to the IPv4 output filter (client or service session).
IPv6 Input Filter Name	Name assigned to the IPv6 input filter (client or service session).
IPv6 Output Filter Name	Name assigned to the IPv6 output filter (client or service session).
IFL Input Filter Name	Name assigned to the logical interface input filter (client or service session).
IFL Output Filter Name	Name assigned to the logical interface output filter (client or service session).

Sample Output

show subscribers (IPv4)

```

user@host> show subscribers
Interface      IP Address/VLAN ID  User Name      LS:RI
ge-1/3/0.1073741824  100                WHOLESALE-CLIENT default:default
demux0.1073741824    10.0.0.10          RETAILER1-CLIENT test1:retailer1
demux0.1073741825    11.0.0.3            RETAILER2-CLIENT test1:retailer2
demux0.1073741826    12.0.0.3

```

show subscribers (IPv6)

```

user@host> show subscribers
Interface      IP Address/VLAN ID  User Name      LS:RI
ge-1/0/0.0     2001:db8::c0:0:0:0/74 WHOLESALE-CLIENT default:default
*              2001:db8::1/128     subscriber-25   default:default

```

show subscribers (IPv4 and IPv6 Dual Stack)

```

user@host> show subscribers
Interface      IP Address/VLAN ID  User Name
LS:RI
demux0.1073741834  0x8100.1002 0x8100.1

```

```
default:default
demux0.1073741835 0x8100.1001 0x8100.1
default:default
pp0.1073741836 61.1.1.1 dualstackuser1@EXAMPLE1.com
default:ASP-1
* 2041:1:1::/48
* 2061:1:1:1::/64
pp0.1073741837 23.1.1.3 dualstackuser2@EXAMPLE1.com
default:ASP-1
* 2001:db8:1:2:5::/64
```

show subscribers (LNS on MX Series Routers)

```
user@host> show subscribers
Interface      IP Address/VLAN ID  User Name      LS:RI
si-4/0/0.1     192.168.4.1        xyz@example.com default:default
```

show subscribers (L2TP Switched Tunnels)

```
user@host> show subscribers
Interface      IP Address/VLAN ID  User Name      LS:RI
si-2/1/0.1073741842 Tunnel-switched    ap@example.com  default:default
si-2/1/0.1073741843 Tunnel-switched    ap@example.com  default:default
```

show subscribers client-type dhcp detail

```
user@host> show subscribers client-type dhcp detail
Type: DHCP
IP Address: 10.20.9.7
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:10:95:00:00:98
State: Active
Radius Accounting ID: jnpr :2304
Login Time: 2009-08-25 14:43:52 PDT

Type: DHCP
IP Address: 10.20.10.7
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073744383
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:10:94:00:01:f3
State: Active
Radius Accounting ID: jnpr :2560
Login Time: 2009-08-25 14:43:56 PDT
```

show subscribers count

```
user@host> show subscribers count
Total Subscribers: 188, Active Subscribers: 188
```


show subscribers address detail (IPv6)

```

user@host> show subscribers address 10.16.12.137 detail
Type: PPPoE
User Name: pppoeTerV6User1Svc
IP Address: 10.16.12.137
IP Netmask: 255.0.0.0
IPv6 User Prefix: 1016:0:0:c88::/64
Logical System: default
Routing Instance: default
Interface: pp0.1073745151
Interface type: Dynamic
Underlying Interface: demux0.8201
Dynamic Profile Name: pppoe-client-profile
MAC Address: 00:0d:02:01:00:01
Session Timeout (seconds): 31622400
Idle Timeout (seconds): 86400
State: Active
Radius Accounting ID: jnpr demux0.8201:6544
Session ID: 6544
Agent Circuit ID: if13720
Agent Remote ID: if13720
Login Time: 2012-05-21 13:37:27 PDT
Service Sessions: 1

```

show subscribers detail (IPv4)

```

user@host> show subscribers detail
Type: DHCP
IP Address: 10.20.9.7
IP Netmask: 255.255.0.0
Primary DNS Address: 192.168.17.1
Secondary DNS Address: 192.168.17.2
Primary WINS Address: 192.168.22.1
Secondary WINS Address: 192.168.22.2
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:10:95:00:00:98
State: Active
Radius Accounting ID: jnpr :2304
Idle Timeout (seconds): 600
Login Time: 2009-08-25 14:43:52 PDT
DHCP Options: len 52
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 08 33 04 00 00
00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 36 2f
33 2d 37 2d 30 37 05 01 06 0f 21 2c
Service Sessions: 2

```

show subscribers detail (IPv6)

```

user@host> show subscribers detail
Type: DHCP
User Name: pd-user1
IPv6 Prefix: 2001:db8:db2:ffff:1::/64
Logical System: default
Routing Instance: default
Interface: ge-3/1/3.2
Interface type: Static

```

```
MAC Address: 00:51:ff:ff:00:03
State: Active
Radius Accounting ID: 1
Session ID: 1
Login Time: 2011-08-25 12:12:26 PDT
DHCP Options: len 42
00 08 00 02 00 00 00 01 00 0a 00 03 00 01 00 51 ff ff 00 03
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00
00 00
```

show subscribers detail (IPv6 Static Demux Interface)

```
user@host> show subscribers detail
Type: STATIC-INTERFACE
User Name: demux0.1@example.net
IPv6 Prefix: 1:2:3:4:5:6:7:aa/128
Logical System: default
Routing Instance: default
Interface: demux0.1
Interface type: Static
Dynamic Profile Name: junos-default-profile
State: Active
Radius Accounting ID: 185
Login Time: 2010-05-18 14:33:56 EDT
```

show subscribers detail (L2TP LNS Subscribers on MX Series Routers)

```
user@host> show subscribers detail
Type: L2TP
User Name: user1@example.net
IP Address: 10.1.32.58
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: si-5/2/0.1073749824
Interface type: Dynamic
Dynamic Profile Name: dyn-lns-profile2
Dynamic Profile Version: 1
State: Active
Radius Accounting ID: 8001
Session ID: 8001
Login Time: 2011-04-25 20:27:50 IST
```

show subscribers detail (L2TP Switched Tunnels)

```
user@host> show subscribers detail
Type: L2TP
User Name: ap@example.com
Logical System: default
Routing Instance: default
Interface: si-2/1/0.1073741842
Interface type: Dynamic
Dynamic Profile Name: dyn-lts-profile
State: Active
L2TP State: Tunnel-switched
Tunnel switch Profile Name: ce-lts-profile
Local IP Address: 10.50.1.1
Remote IP Address: 192.168.20.3
Radius Accounting ID: 21
Session ID: 21
Login Time: 2013-01-18 03:01:11 PST
```

```

Type: L2TP
User Name: ap@example.com
Logical System: default
Routing Instance: default
Interface: si-2/1/0.1073741843
Interface type: Dynamic
Dynamic Profile Name: dyn-lts-profile
State: Active
L2TP State: Tunnel-switched
Tunnel switch Profile Name: ce-lts-profile
Local IP Address: 10.30.1.1
Remote IP Address: 172.20.1.10
Session ID: 22
Login Time: 2013-01-18 03:01:14 PST

```

show subscribers detail (Tunneled Subscriber)

```

user@host> show subscribers detail
Type: PPPoE
User Name: user1@example.com
Logical System: default
Routing Instance: default
Interface: pp0.1
State: Active, Tunneled
Radius Accounting ID: 512

```

show subscribers detail (IPv4 and IPv6 Dual Stack)

```

user@host> show subscribers detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlanProfile
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.1001
VLAN Id: 0x8100.1
Login Time: 2011-11-30 00:18:04 PST

Type: PPPoE
User Name: dualstackuser1@EXAMPLE1.com
IP Address: 61.1.1.1
IPv6 Prefix: 2041:1:1::/48
IPv6 User Prefix: 2061:1:1:1::/64
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: dualStack-Profile1
MAC Address: 00:00:64:03:01:02
State: Active
Radius Accounting ID: 2
Session ID: 2
Login Time: 2011-11-30 00:18:05 PST

Type: DHCP
IPv6 Prefix: 2041:1:1::/48
Logical System: default
Routing Instance: ASP-1

```

```
Interface: pp0.1073741825
Interface type: Static
MAC Address: 00:00:64:03:01:02
State: Active
Radius Accounting ID: jnpr :3
Session ID: 3
Underlying Session ID: 2
Login Time: 2011-11-30 00:18:35 PST
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 00 64 03 01 02
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
```

show subscribers detail (ACI Interface Set Session)

```
user@host> show subscribers detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0
Interface Set: aci-1001-ge-1/0/0.2800
Interface Set Session ID: 0
Underlying Interface: ge-1/0/0.2800
Dynamic Profile Name: aci-vlan-set-profile-2
Dynamic Profile Version: 1
State: Active
Session ID: 1
Agent Circuit ID: aci-ppp-dhcp-20
Login Time: 2012-05-26 01:54:08 PDT
```

show subscribers detail (PPPoE Subscriber Session with ACI Interface Set)

```
user@host> show subscribers detail
Type: PPPoE
User Name: ppphint2
IP Address: 10.10.1.5
Logical System: default
Routing Instance: default
Interface: pp0.1073741825
Interface type: Dynamic
Interface Set: aci-1001-demux0.1073741824
Interface Set Type: Dynamic
Interface Set Session ID: 2
Underlying Interface: demux0.1073741824
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:64:39:01:02
State: Active
Radius Accounting ID: 3
Session ID: 3
Agent Circuit ID: aci-ppp-dhcp-dvlan-50
Login Time: 2012-03-07 13:46:53 PST
```

show subscribers extensive

```
user@host> show subscribers extensive
Type: DHCP
User Name: pd-user1
IPv6 Prefix: 2001:db8:db2:ffff:1::/64
Logical System: default
Routing Instance: default
```

```

Interface: ge-3/1/3.2
Interface type: Static
MAC Address: 00:51:ff:ff:00:03
State: Active
Radius Accounting ID: 1
Session ID: 1
Login Time: 2011-08-25 12:12:26 PDT
DHCP Options: len 42
00 08 00 02 00 00 00 01 00 0a 00 03 00 01 00 51 ff ff 00 03
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00
00 00
IPv6 Address Pool: pd_pool
IPv6 Network Prefix Length: 48

```

show subscribers extensive (RPF Check Fail Filter)

```

user@host> show subscribers extensive
...
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ae0.1073741824
Interface type: Dynamic
Dynamic Profile Name: vlan-prof
State: Active
Session ID: 9
VLAN Id: 100
Login Time: 2011-08-26 08:17:00 PDT
IPv4 rpf-check Fail Filter Name: rpf-allow-dhcp
IPv6 rpf-check Fail Filter Name: rpf-allow-dhcpv6
...

```

show subscribers extensive (L2TP LNS Subscribers on MX Series Routers)

```

user@host> show subscribers extensive
Type: L2TP
User Name: user1@example.net
IP Address: 10.1.32.58
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: si-5/2/0.1073749824
Interface type: Dynamic
Dynamic Profile Name: dyn-lns-profile2
Dynamic Profile Version: 1
State: Active
Radius Accounting ID: 8001
Session ID: 8001
Login Time: 2011-04-25 20:27:50 IST
IPv4 Input Filter Name: classify-si-5/2/0.1073749824-in
IPv4 Output Filter Name: classify-si-5/2/0.1073749824-out

```

show subscribers extensive (IPv4 and IPv6 Dual Stack)

```

user@host> show subscribers extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlanProfile
State: Active

```

```
Session ID: 1
Stacked VLAN Id: 0x8100.1001
VLAN Id: 0x8100.1
Login Time: 2011-11-30 00:18:04 PST

Type: PPPoE
User Name: dualstackuser1@EXAMPLE1.com
IP Address: 61.1.1.1
IPv6 Prefix: 2041:1:1::/48
IPv6 User Prefix: 2061:1:1:1::/64
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: dualStack-Profile1
MAC Address: 00:00:64:03:01:02
State: Active
Radius Accounting ID: 2
Session ID: 2
Login Time: 2011-11-30 00:18:05 PST
IPv6 Delegated Network Prefix Length: 48
IPv6 Interface Address: 2061:1:1:1::1/64
IPv6 Framed Interface Id: 1:1:2:2
IPv4 Input Filter Name: FILTER-IN-pp0.1073741825-in
IPv4 Output Filter Name: FILTER-OUT-pp0.1073741825-out
IPv6 Input Filter Name: FILTER-IN6-pp0.1073741825-in
IPv6 Output Filter Name: FILTER-OUT6-pp0.1073741825-out

Type: DHCP
IPv6 Prefix: 2041:1:1::/48
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Static
MAC Address: 00:00:64:03:01:02
State: Active
Radius Accounting ID: jnpr :3
Session ID: 3
Underlying Session ID: 2
Login Time: 2011-11-30 00:18:35 PST
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 00 64 03 01 02
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
IPv6 Delegated Network Prefix Length: 48
```

show subscribers extensive (Effective Shaping-Rate)

```
user@host> show subscribers extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741837
Interface type: Dynamic
Interface Set: ifset-1
Underlying Interface: ae1
Dynamic Profile Name: svlan-dhcp-test
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.201
```

```
VLAN Id: 0x8100.201
Login Time: 2011-11-30 00:18:04 PST
Effective shaping-rate: 31000000k
...
```

show subscribers aci-interface-set-name detail (Subscriber Sessions Using Specified ACI Interface Set)

```
user@host> show subscribers aci-interface-set-name aci-1003-ge-1/0/0.4001 detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-set-profile
Dynamic Profile Version: 1
State: Active
Session ID: 13
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:56 PDT

Type: PPPoE
User Name: ppphint2
IP Address: 10.10.1.7
Logical System: default
Routing Instance: default
Interface: pp0.1073741834
Interface type: Dynamic
Interface Set: aci-1003-ge-1/0/0.4001
Interface Set Type: Dynamic
Interface Set Session ID: 13
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:65:26:01:02
State: Active
Radius Accounting ID: 14
Session ID: 14
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:57 PDT
```

show subscribers agent-circuit-identifier detail (Subscriber Sessions Using Specified ACI Substring)

```
user@host> show subscribers agent-circuit-identifier aci-ppp-vlan detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-set-profile
Dynamic Profile Version: 1
State: Active
Session ID: 13
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:56 PDT

Type: PPPoE
User Name: ppphint2
IP Address: 10.10.1.7
Logical System: default
Routing Instance: default
Interface: pp0.1073741834
```

```
Interface type: Dynamic
Interface Set: aci-1003-ge-1/0/0.4001
Interface Set Type: Dynamic
Interface Set Session ID: 13
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:65:26:01:02
State: Active
Radius Accounting ID: 14
Session ID: 14
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:57 PDT
```

show subscribers interface extensive

```
user@host> show subscribers interface demux0.1073741826 extensive
Type: VLAN
User Name: test1@test.com
Logical System: default
Routing Instance: testnet
Interface: demux0.1073741826
Interface type: Dynamic
Dynamic Profile Name: profile-vdemux-relay-23qos
MAC Address: 00:00:6e:56:01:04
State: Active
Radius Accounting ID: 12
Session ID: 12
Stacked VLAN Id: 0x8100.1500
VLAN Id: 0x8100.2902
Login Time: 2011-10-20 16:21:59 EST

Type: DHCP
User Name: test1@test.com
IP Address: 172.16.200.6
IP Netmask: 255.255.255.0
Logical System: default
Routing Instance: testnet
Interface: demux0.1073741826
Interface type: Static
MAC Address: 00:00:6e:56:01:04
State: Active
Radius Accounting ID: 21
Session ID: 21
Login Time: 2011-10-20 16:24:33 EST
Service Sessions: 2

Service Session ID: 25
Service Session Name: SUB-QOS
State: Active

Service Session ID: 26
Service Session Name: service-cb-content
State: Active
IPv4 Input Filter Name: content-cb-in-demux0.1073741826-in
IPv4 Output Filter Name: content-cb-out-demux0.1073741826-out
```

show subscribers logical-system terse

```
user@host> show subscribers logical-system test1 terse
```


Interface	IP Address/VLAN ID	User Name	LS:RI
demux0.1073741825	11.0.0.3	RETAILER1-CLIENT	test1:retailer1
demux0.1073741826	12.0.0.3	RETAILER2-CLIENT	test1:retailer2

show subscribers physical-interface count

```
user@host> show subscribers physical-interface ge-1/0/0 count
Total subscribers: 3998, Active Subscribers: 3998
```

show subscribers routing-instance inst1 count

```
user@host> show subscribers routing-instance inst1 count
Total Subscribers: 188, Active Subscribers: 183
```

show subscribers stacked-vlan-id detail

```
user@host> show subscribers stacked-vlan-id 101 detail
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT
```

show subscribers stacked-vlan-id vlan-id detail (Combined Output)

```
user@host> show subscribers stacked-vlan-id 101 vlan-id 100 detail
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT
```

show subscribers stacked-vlan-id vlan-id interface detail (Combined Output for a Specific Interface)

```
user@host> show subscribers stacked-vlan-id 101 vlan-id 100 interface ge-1/2/0.* detail
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT
```

show subscribers user-name detail

```
user@host> show subscribers user-name larry1 detail
Type: DHCP
User Name: larry1
IP Address: 100.0.0.37
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.1
Interface type: Static
Dynamic Profile Name: foo
```

```
MAC Address: 00:10:94:00:00:01
State: Active
Radius Accounting ID: 1
Session ID: 1
Login Time: 2011-11-07 08:25:59 PST
DHCP Options: len 52
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 01 33 04 00 00
00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 32 2f
37 2d 30 2d 30 37 05 01 06 0f 21 2c
```

show subscribers vlan-id

```
user@host> show subscribers vlan-id 100
Interface          IP Address          User Name
ge-1/0/0.1073741824
ge-1/2/0.1073741825
```

show subscribers vlan-id detail


```
user@host> show subscribers vlan-id 100 detail
Type: VLAN
Interface: ge-1/0/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: vlan-prof-tpid
State: Active
VLAN Id: 100
Login Time: 2009-03-11 06:48:54 PDT

Type: VLAN
Interface: ge-1/2/0.1073741825
Interface type: Dynamic
Dynamic Profile Name: vlan-prof-tpid
State: Active
VLAN Id: 100
Login Time: 2009-03-11 06:48:54 PDT
```

show subscribers vpi vci extensive (PPPoE-over-ATM Subscriber Session)

```
user@host> show subscribers vpi 40 vci 50 extensive
Type: PPPoE
User Name: testuser
IP Address: 100.0.0.2
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: pp0.0
Interface type: Static
MAC Address: 00:00:65:23:01:02
State: Active
Radius Accounting ID: 2
Session ID: 2
ATM VPI: 40
ATM VCI: 50
Login Time: 2012-12-03 07:49:26 PST
IP Address Pool: pool_1
IPv6 Framed Interface Id: 200:65ff:fe23:102
```

show subscribers summary

Syntax	<pre>show subscribers summary <all> < detail extensive terse> <count> <physical-interface <i>physical-interface-name</i>> <logical-system <i>logical-system</i> pic port routing-instance <i>routing-instance</i> slot></pre>
Release Information	Command introduced in Junos OS Release 10.2.
Description	Display summary information for subscribers.
Options	<p>all—(Optional) Display full subscriber summary.</p> <p>detail extensive terse—(Optional) Display the specified level of output.</p> <p>count—(Optional) Display the count of total subscribers and active subscribers for any specified option.</p> <p>logical-system—(Optional) Display subscribers whose logical system matches the specified logical system.</p> <p>physical-interface-name—(M120, M320, and MX Series routers only) (Optional) Display a count of subscribers whose physical interface matches the specified physical interface, by subscriber state, client type and LS:RI.</p> <p>pic—(M120, M320, and MX Series routers only) (Optional) Display a count of subscribers by PIC number and the total number of subscribers.</p> <p>port—(M120, M320, and MX Series routers only) (Optional) Display a count of subscribers by port number and the total number of subscribers.</p> <p>routing-instance—(Optional) Display subscribers whose routing instance matches the specified routing instance.</p> <p>slot—(M120, M320, and MX Series routers only) (Optional) Display a count of subscribers by FPC slot number and the total number of subscribers.</p>
	<div>  <p>NOTE: Due to display limitations, logical system and routing instance output values are truncated when necessary.</p> </div>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> show subscribers on page 1221
List of Sample Output	show subscribers summary on page 1241

[show subscribers summary all on page 1241](#)
[show subscribers summary physical-interface on page 1241](#)
[show subscribers summary physical-interface pic on page 1242](#)
[show subscribers summary physical-interface port on page 1242](#)
[show subscribers summary physical-interface slot on page 1242](#)
[show subscribers summary pic on page 1242](#)
[show subscribers summary pic \(Aggregated Ethernet Interfaces\) on page 1243](#)
[show subscribers summary port on page 1243](#)
[show subscribers summary slot on page 1243](#)
[show subscribers summary terse on page 1243](#)

Output Fields Table 110 on page 1240 lists the output fields for the **show subscribers** command. Output fields are listed in the approximate order in which they appear.

Table 110: show subscribers summary Output Fields

Field Name	Field Description
Subscribers by State	<p>Number of subscribers summarized by state. The summary information includes the following:</p> <ul style="list-style-type: none"> • Init—Number of subscriber currently in the initialization state. • Configured—Number of configured subscribers. • Active—Number of active subscribers. • Terminating—Number of subscribers currently terminating. • Terminated—Number of terminated subscribers. • Total—Total number of subscribers for all states.
Subscribers by Client Type	<p>Number of subscribers summarized by client type. Client types can include DHCP, L2TP, PPP, PPPOE, STATIC-INTERFACE, and VLAN. Also displays the total number of subscribers for all client types (Total).</p>
Subscribers by LS:RI	<p>Number of subscribers summarized by logical system:routing instance (LS:RI) combination. Also displays the total number of subscribers for all LS:RI combinations (Total).</p>
Interface	<p>Interface associated with the subscriber. The router or switch displays subscribers whose interface matches or begins with the specified interface.</p> <p>The * character indicates a continuation of addresses for the same session.</p> <p>For aggregated Ethernet interfaces, the output of the summary (pic port slot) options prefixes the interface name with ae0:.</p>
Count	<p>Count of subscribers displayed for each PIC, port, or slot when those options are specified with the summary option. For an aggregated Ethernet configuration, the total subscriber count does not equal the sum of the individual PIC, port, or slot counts, because each subscriber can be in more than one aggregated Ethernet link.</p>
Total Subscribers	<p>Total number of subscribers for all physical interfaces, all PICS, all ports, or all LS:RI slots.</p>
IP Address/VLAN ID	<p>Subscriber IP address or VLAN ID associated with the subscriber in the form <i>tpid.vlan-id</i></p>
User Name	<p>Name of subscriber.</p>
LS:RI	<p>Logical system and routing instance associated with the subscriber.</p>

Sample Output

show subscribers summary

```
user@host> show subscribers summary
```

Subscribers by State

```
Init      3
Configured  2
Active    183
Terminating  2
Terminated  1
```

```
TOTAL      191
```

Subscribers by Client Type

```
DHCP      107
PPP        76
VLAN       8
```

```
TOTAL      191
```

show subscribers summary all

```
user@host> show subscribers summary all
```

Subscribers by State

```
Init      3
Configured  2
Active    183
Terminating  2
Terminated  1
```

```
TOTAL      191
```

Subscribers by Client Type

```
DHCP      107
PPP        76
VLAN       8
```

```
TOTAL      191
```

Subscribers by LS:RI

```
default:default  1
default:ri1      28
default:ri2      16
ls1:default      22
ls1:riA          38
ls1:riB          44
logsysX:routinstY 42
```

```
TOTAL      191
```

show subscribers summary physical-interface

```
user@host> show subscribers summary physical-interface ge-1/0/0
```

Subscribers by State

```
Active: 3998
Total: 3998
```

Subscribers by Client Type

```
DHCP: 3998
```

Total: 3998

Subscribers by LS:RI
default:default: 3998
Total: 3998

show subscribers summary physical-interface pic

```
user@host> show subscribers summary physical-interface ge-0/2/0 pic
Subscribers by State
Active: 4825
Total: 4825
```

Subscribers by Client Type
DHCP: 4825
Total: 4825

Subscribers by LS:RI
default:default: 4825
Total: 4825

show subscribers summary physical-interface port

```
user@host> show subscribers summary physical-interface ge-0/3/0 port
Subscribers by State
Active: 4825
Total: 4825
```

Subscribers by Client Type
DHCP: 4825
Total: 4825

Subscribers by LS:RI
default:default: 4825
Total: 4825

show subscribers summary physical-interface slot

```
user@host> show subscribers summary physical-interface ge-2/0/0 slot
Subscribers by State
Active: 4825
Total: 4825
```

Subscribers by Client Type
DHCP: 4825
Total: 4825

Subscribers by LS:RI
default:default: 4825
Total: 4825

show subscribers summary pic

```
user@host> show subscribers summary pic
Interface      Count
ge-1/0         1000
ge-1/3         1000

Total Subscribers: 2000
```

show subscribers summary pic (Aggregated Ethernet Interfaces)

```

user@host> show subscribers summary pic
Interface          Count
ae0: ge-1/0        801
ae0: ge-1/3        801

Total Subscribers: 801

```

show subscribers summary port

```

user@host> show subscribers summary port
Interface          Count
ge-1               2000

Total Subscribers: 2000

```

show subscribers summary slot

```

user@host> show subscribers summary slot
Interface          Count
ge-1               2000

Total Subscribers: 2000

```

show subscribers summary terse

```

user@host> show subscribers summary terse
Interface          IP Address/VLAN ID  User Name          LS:RI
ge-1/3/0.1073741824 100                 WHOLESALE-CLIENT default:default
demux0.1073741824   100.0.0.10          RETAILER1-CLIENT test1:retailer1
demux0.1073741825   101.0.0.3           RETAILER2-CLIENT test1:retailer2
demux0.1073741826   102.0.0.3

```

show system subscriber-management summary

Syntax	show system subscriber-management summary
Release Information	Command introduced in Junos OS Release 11.1.
Description	Display complete subscriber management database summary information.
Options	none—This command has no options.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show database-replication statistics on page 1081• show database-replication summary on page 1083
List of Sample Output	show system subscriber-management summary on page 1245
Output Fields	Table 111 on page 1244 lists the output fields for the show system subscriber-management summary command. Output fields are listed in the approximate order in which they appear.

Table 111: show system subscriber-management summary Output Fields

Field Name	Field Description
Graceful Restart	State of graceful Routing Engine switchover (GRES): <ul style="list-style-type: none">• Enabled• Disabled
Mastership	State of the Routing Engine: <ul style="list-style-type: none">• Master• Standby
Database	State of the subscriber management database: <ul style="list-style-type: none">• Available• Init• Not-available

Table 111: show system subscriber-management summary Output Fields (*continued*)

Field Name	Field Description
Chassisd ISSU State	State of unified ISSU chassis daemon: <ul style="list-style-type: none"> • ABORT • DAEMON_ISSU_PREPARE • DAEMON_ISSU_PREPARE_DONE • DAEMON_SWITCHOVER_PREPARE • DAEMON_SWITCHOVER_PREPARE_DONE • FRU_ISSU • FRU_ISSU_DONE • IDLE • UNKNOWN
ISSU State	State of unified ISSU aggregate daemon: <ul style="list-style-type: none"> • ABORT • IDLE • PREPARE • READY • SWITCHOVER_PREPARE • SWITCHOVER_READY • UNKNOWN
ISSU Wait	Amount of time, in seconds, requested by a daemon to perform cleanup. If multiple daemons request time, the displayed value is the highest wait time requested by a daemon.

Sample Output

show system subscriber-management summary

```

user@host> show system subscriber-management summary
General:
  Graceful Restart      Enabled
  Mastership            Master
  Database              Available
  Chassisd ISSU State   DAEMON_ISSU_PREPARE
  ISSU State            PREPARE
  ISSU Wait             198

```

test aaa authd-lite user

Syntax	<code>test aaa authd-lite user <i>username</i> password <i>password</i> profile <i>access-profile-name</i> <port <i>nas-port</i>> <zero-stats></code>
Release Information	Command introduced in Junos OS Release 11.2.
Description	Verify authd-lite subscriber access authentication, accounting, and address allocation configuration.
Options	<p><i>username</i>—Specify the subscriber username to test.</p> <p><i>password password</i>—Specify the password associated with the username.</p> <p><i>profile access-profile-name</i>—Specify the access profile associated with the subscriber.</p> <p><i>port nas-port</i>—(Optional) Specify the NAS port used for the test.</p> <p><i>zero-stats</i>—(Optional) Specify that no accounting statistics are set for this test.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• Testing a Subscriber AAA Configuration on page 515
List of Sample Output	test aaa authd-lite user on page 1246
Output Fields	<p>When you enter this command, you are provided feedback on the status of your request. For information about output fields related to authentication, accounting, and subscriber-specific information, see the show network-access aaa statistics, show network-access aaa statistics authentication, show network-access aaa subscribers, and show subscribers commands.</p> <p>The test command does not support volume-time accounting. If volume-time accounting is configured for the test subscriber, the test command replaces the statistics with time-only accounting statistics.</p>

Sample Output

test aaa authd-lite user

The following example tests the configuration for authd-lite subscriber brady-t with a password of a11pr0 and an access profile of employee12, and displays the resulting output:

```
user@host> test aaa authd-lite user brady-t password a11pr0 profile employee12
Authentication Grant
*****User Attributes*****
  User Name -                               brady-t
  Framed IPv6 Prefix -                       ::/0
  Framed IPv6 Pool -                         NULL
  Nas IPv6 Address -                         ::
  NDRA IPv6 Prefix -                        NULL
```

```

Login IPv6 Host - ::
Framed Interface Id - 0:0:0:0
Delegated IPv6 Prefix - ::/0
NDRA IPv6 Pool - NULL
User Password - allpr0
Nas Ip Address - 0.0.0.0
NAS Port - 0
Service Type- 0
Framed IP Address - 0.0.0.0
Framed IP Netmask - 0.0.0.0
Filter Id - NULL
Framed MTU - 0
Reply Message - NULL
Framed Route- not set
Framed MTU - 0
Class - SBR2CL
Virtual Router Name NULL
Primary DNS IP Address - 0.0.0.0
Secondary DNS IP Address - 0.0.0.0
Primary WINS IP Address - 0.0.0.0
Secondary WINS IP Address - 0.0.0.0
Ingress Statistics - disabled
Egress Statistics - disabled
Ingress Policy Name not set
Egress Policy Name not set
IGMP disabled
Redirect VR Name not set
Service Bundle not set
Framed Ip Route Tag not set
LI Action 0
LI Interception Identifier 0
LI Mediation Device IP Address 0.0.0.0
LI_Mediation_Device_Port_Number 0
Activate Service NULL
Deactivate Service NULL
Service Statistics 0
Ignore_DF_Bit - disabled
IGMP Access Group Name not set
IGMP Access Source Group_Name - not set
MLD Access Group Name not set
MLD Access Source Group Name not set
MLD Version - MLD Version not set
IGMP Version IGMP Version not set
IGMP Immediate Leave - disabled
MLD Immediate Leave - disabled
IPv6_Ingress_Policy_Name - not set
IPv6_Egress_Policy_Name - not set
Cos_Parameter_Type - not set
Service Interim Acct Interval 0
Max Clients Per Interface 0
Cos_Scheduler_Pmt_Type not set
Session Timeout 599999940
NAS Port Type 0
Framed Pool NULL
Idle Timeout 0
Acct-start sent
Acct-start succeeded
Pausing 10 seconds
Interim-Acct sent
Acct-interim succeeded
Pausing 10 seconds

```

```
Acct-stop sent
Acct-stop succeeded
Logging out subscriber
Test complete. Exiting
```

test aaa dhcp user

Syntax	<pre>test aaa dhcp user <i>username</i> <agent-remote-id <i>ari</i>> <logical-system <i>logical-system-name</i>> <mac-address <i>mac-address</i>> <option-82 <i>option-82</i>> <password <i>password</i>> <profile <i>access-profile-name</i>> <routing-instance <i>routing-instance-name</i>> <source-address <i>source-address</i>> <terminate-code <i>code-value</i>></pre>
Release Information	<p>Command introduced in Junos OS Release 11.2.</p> <p>Option terminate-code introduced in Junos OS Release 11.4.</p> <p>Option agent-remote-id introduced in Junos OS Release 14.1.</p>
Description	Verify Dynamic Host Configuration Protocol (DHCP) subscriber access authentication, accounting, and address allocation configuration.
Options	<p><i>username</i>—Subscriber username to test.</p> <p>agent-remote-id <i>ari</i>—(Optional) Value of the DSL Forum Agent-Remote-Id (VSA 26–2).</p> <p>logical-system <i>logical-system-name</i>—(Optional) Logical system in which the subscriber is authenticated.</p> <p>mac-address <i>mac-address</i>—(Optional) MAC address of the DHCP client.</p> <p>option-82 <i>option-82</i>—(Optional) DHCP relay agent information option (option-82) value.</p> <p>password <i>password</i>—(Optional) Password associated with the username.</p> <p>profile <i>access-profile-name</i>—(Optional) Access profile associated with the subscriber.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Routing instance in which the subscriber is authenticated.</p> <p>source-address <i>source-address</i>—(Optional) IP address of the outgoing interface.</p> <p>terminate-code <i>code-value</i>—(Optional) Code associated with the subscriber termination.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Testing a Subscriber AAA Configuration on page 515
List of Sample Output	test aaa dhcp user on page 1250
Output Fields	<p>When you enter this command, you are provided feedback on the status of your request. For information about output fields related to authentication, accounting, and subscriber-specific information, see the show network-access aaa statistics, show</p>

`network-access aaa statistics authentication`, `show network-access aaa subscribers`, and `show subscribers` commands.

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

Sample Output

test aaa dhcp user

The following example tests the configuration for DHCP subscriber esmeralda and password rch4Astar, and displays the resulting output:

```
user@host> test aaa dhcp user esmeralda@xyz.net password rch4Astar
Authentication Grant
*****User Attributes*****
  User Name - esmeralda@xyz.net
  Client IP Address - 192.168.1.1
  Client IP Netmask - 255.255.0.0
  Virtual Router Name - default
  Agent Remote Id - NULL
  Reply Message - NULL
  Primary DNS IP Address - 0.0.0.0
  Secondary DNS IP Address - 0.0.0.0
  Primary WINS IP Address - 0.0.0.0
  Secondary WINS IP Address - 0.0.0.0
  Primary DNS IPv6 Address - ::
  Secondary DNS IPv6 Address - ::
  Framed Pool - not set
  Service Type - 0
  DHCP Guided Relay Server - 0
  Class Attribute - TEST
  Client IPv6 Address - ::
  Client IPv6 Mask - null
  Framed IPv6 Prefix - ::/0
  Framed IPv6 Pool - not-set
  NDRA IPv6 Prefix - not-set
  Login IPv6 Host - ::
  Framed Interface Id - 0:0:0:0
  Delegated IPv6 Prefix - ::/0
  Delegated IPv6 Pool - not-set
  User Password - rch4Astar
  CHAP Password - NULL
  Mac Address - AB:CD:00:00:00:01
  Idle Timeout - 600
  Session Timeout - 6000
  Service Name (1) - cos-service(video_sch, nc_sch)

  Service Statistics (1) - 1
  Service Acct Interim (1) - 600
  Service Activation Type (1) - 1
  Service Name (2) - filter-service(in_filter,
out_filter)
  Service Statistics (2) - 2
  Service Acct Interim (2) - 900
  Service Activation Type (2) - 1
  Cos shaping rate - 100m
  Filter Id - not set
```

```

Framed MTU - (null)
Framed Route - not set
Ingress Policy Name - not set
Egress Policy Name - not set
IGMP - disabled
Redirect VR Name - default
Service Bundle - Null
Framed Ip Route Tag - not set
Ignore DF Bit - disabled
IGMP Access Group Name - not set
IGMP Access Source Group Name - not set
MLD Access Group Name - not set
MLD Access Source Group Name - not set
IGMP Version - not set
MLD Version - not set
IGMP Immediate Leave - disabled
MLD Immediate Leave - disabled
IPv6 Ingress Policy Name - not set
IPv6 Egress Policy Name - not set
Acct Session ID - 1
Acct Interim Interval - 750
Acct Type - 1
Ingress Statistics - disabled
Egress Statistics - disabled
Chargeable user identity - 0
NAS Port Id - -0/0/0.0
NAS Port - 4095
NAS Port Type - 15
Framed Protocol - 1
IPv4 ADF Rule - 010100
IPv4 ADF Rule - 010101
IPv6 ADF Rule - 030100
IPv6 ADF Rule - 030101
****Pausing 10 seconds before disconnecting the test user*****
Logging out subscriber
  Terminate Id - not set
Test complete. Exiting

```

test aaa ppp user

Syntax	<code>test aaa ppp user <i>username</i></code> <code><agent-remote-id <i>ari</i>></code> <code><logical-system <i>logical-system-name</i>></code> <code><password <i>password</i>></code> <code><profile <i>access-profile-name</i>></code> <code><routing-instance <i>routing-instance-name</i>></code> <code><terminate-code <i>code-value</i>></code>
Release Information	Command introduced in Junos OS Release 11.2. Option terminate-code introduced in Junos OS Release 11.4. Option agent-remote-id introduced in Junos OS Release 14.1.
Description	Verify Point-to-Point Protocol (PPP) subscriber access authentication, accounting, and address allocation configuration.
Options	<p><i>username</i>—Subscriber username to test.</p> <p>agent-remote-id <i>ari</i>—(Optional) Value of the DSL Forum Agent-Remote-Id (VSA 26–2).</p> <p>logical-system <i>logical-system-name</i>—(Optional) Logical system in which the subscriber is authenticated.</p> <p>password <i>password</i>—(Optional) Password associated with the username.</p> <p>profile <i>access-profile-name</i>—(Optional) Access profile associated with the subscriber.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Routing instance in which the subscriber is authenticated.</p> <p>terminate-code <i>code-value</i>—(Optional) Code associated with the subscriber termination.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• Testing a Subscriber AAA Configuration on page 515
List of Sample Output	test aaa ppp user on page 1253 test aaa ppp user (tunneled user) on page 1254 test aaa ppp user (authentication failure) on page 1254
Output Fields	<p>When you enter this command, you are provided feedback on the status of your request. For information about output fields related to authentication, accounting, and subscriber-specific information, see the show network-access aaa statistics, show network-access aaa statistics authentication, show network-access aaa subscribers, and show subscribers commands.</p> <p>The test command does not support volume-time accounting. If volume-time accounting is configured for the test subscriber, the test command replaces the statistics with time-only accounting statistics.</p>

Sample Output

test aaa ppp user

The following example tests the configuration for PPP subscriber jilldoe and password 92&tDcb, and displays the resulting output:

```
user@host> test aaa ppp user jilldoe@xyz.net password 92&tDcb
Authentication Grant
*****User Attributes*****
    User Name - jilldoe@xyz.net
    Client IP Address - 192.168.1.1
    Client IP Netmask - 255.255.0.0
    Virtual Router Name - default
    Agent Remote Id - NULL
    Reply Message - NULL
    Primary DNS IP Address - 0.0.0.0
    Secondary DNS IP Address - 0.0.0.0
    Primary WINS IP Address - 0.0.0.0
    Secondary WINS IP Address - 0.0.0.0
    Primary DNS IPv6 Address - ::
    Secondary DNS IPv6 Address - ::
    Framed Pool - not set
    Class Attribute - TEST
    Service Type - 0
    Client IPv6 Address - ::
    Client IPv6 Mask - null
    Framed IPv6 Prefix - ::/0
    Framed IPv6 Pool - not-set
    NDRA IPv6 Prefix - not-set
    Login IPv6 Host - ::
    Framed Interface Id - 0:0:0:0
    Delegated IPv6 Prefix - ::/0
    Delegated IPv6 Pool - not-set
    User Password - 92&tDcb
    CHAP Password - NULL
    Mac Address - AB:CD:00:00:00:01
    Idle Timeout - 600
    Session Timeout - 6000
    Service Name (1) - cos-service(video_sch, nc_sch)

    Service Statistics (1) - 1
    Service Acct Interim (1) - 600
    Service Activation Type (1) - 1
    Service Name (2) - filter-service(in_filter,
out_filter)
    Service Statistics (2) - 2
    Service Acct Interim (2) - 900
    Service Activation Type (2) - 1
    Cos shaping rate - 100m
    Filter Id - not set
    Framed MTU - (null)
    Framed Route - not set
    Ingress Policy Name - not set
    Egress Policy Name - not set
    IGMP - disabled
    Redirect VR Name - default
    Service Bundle - Null
    Framed Ip Route Tag - not set
    Ignore DF Bit - disabled
```

```

IGMP Access Group Name -          not set
IGMP Access Source Group Name -    not set
MLD Access Group Name -           not set
MLD Access Source Group Name -     not set
IGMP Version -                    not set
MLD Version -                     not set
IGMP Immediate Leave -            disabled
MLD Immediate Leave -             disabled
IPv6 Ingress Policy Name -         not set
IPv6 Egress Policy Name -          not set
Acct Session ID -                  1
Acct Interim Interval -            750
Acct Type -                        1
Ingress Statistics -               disabled
Egress Statistics -                disabled
Chargeable user identity -         0
NAS Port Id -                     -0/0/0.0
NAS Port -                         4095
NAS Port Type -                    15
Framed Protocol -                  1
IPv4 ADF Rule -                    010100
IPv4 ADF Rule -                    010101
IPv6 ADF Rule -                    030100
IPv6 ADF Rule -                    030101
****Pausing 10 seconds before disconnecting the test user*****
Logging out subscriber
  Terminate Id -                    not set
Test complete. Exiting

```

test aaa ppp user (tunneled user)

The following example tests the configuration for PPP tunneled subscriber accounting14, with password bncntr14 and access profile finance-b, and displays the resulting output:

```

user@host> test aaa ppp user accounting14 password bncntr14 profile finance-b
Authentication Grant with Tunnel Attributes
*****Tunnel Attributes*****
  ****Tunnel Definiton -          1
    Tunnel Medium -                1
    Tunnel Type -                  3
    Tunnel Max Sessions -          100
    Tunnel Server Endpoint -       1.2.3.4
    Tunnel Client Endpoint -       2.3.4.5
    Tunnel Server AuthId -         rt1
    Tunnel Client AuthId -         ts1
    Tunnel Password -              radius
    Tunnel Assignment Id -         til
    Tunnel Logical System -
    Tunnel Routing Instance -
  ****Pausing 10 seconds before disconnecting the test user*****
Logging out subscriber
  Terminate Id -                  12tp
session-receive-cdn-avp-bad-hidden
Test complete. Exiting

```

test aaa ppp user (authentication failure)

The following example shows sample output when the authentication grant fails due to an invalid password:

```
user@host>test aaa ppp user thomastank@xyz.net password 55N333%%56
```

```
Authentication Deny
```

```
Reason : Access Denied
```

```
Received Attributes :
```

```

User Name - thomastank@xyz.net
Client IP Address - 0.0.0.0
Client IP Netmask - 0.0.0.0
Virtual Router Name - default
Agent Remote Id - NULL
Reply Message - NULL
Primary DNS IP Address - 0.0.0.0
Secondary DNS IP Address - 0.0.0.0
Primary WINS IP Address - 0.0.0.0
Secondary WINS IP Address - 0.0.0.0
Primary DNS IPv6 Address - ::
Secondary DNS IPv6 Address - ::
Framed Pool - not set
Class Attribute - not set
Service Type - 0
Client IPv6 Address - ::
Client IPv6 Mask - null
Framed IPv6 Prefix - ::/0
Framed IPv6 Pool - not-set
NDRA IPv6 Prefix - not-set
Login IPv6 Host - ::
Framed Interface Id - 0:0:0:0
Delegated IPv6 Prefix - ::/0
Delegated IPv6 Pool - not-set
User Password - 55N333%%56
CHAP Password - NULL
Mac Address - AB:CD:00:00:00:01
Filter Id - not set
Framed MTU - (null)
Framed Route - not set
Ingress Policy Name - not set
Egress Policy Name - not set
IGMP - disabled
Redirect VR Name - default
Service Bundle - Null
Framed Ip Route Tag - not set
Ignore DF Bit - disabled
IGMP Access Group Name - not set
IGMP Access Source Group Name - not set
MLD Access Group Name - not set
MLD Access Source Group Name - not set
IGMP Version - not set
MLD Version - not set
IGMP Immediate Leave - disabled
MLD Immediate Leave - disabled
IPv6 Ingress Policy Name - not set
IPv6 Egress Policy Name - not set
Acct Session ID - 12
Acct Interim Interval - 0
Acct Type - 0
Ingress Statistics - disabled
Egress Statistics - disabled
Chargeable user identity - 0
NAS Port Id - -0/0/0.0
NAS Port - 4095
NAS Port Type - 15

```

Framed Protocol - Test complete. Exiting	0
---	---

PART 11

Index

- [Index on page 1259](#)

Index

Symbols

#, comments in configuration statements.....	xxxviii
\$junos-subscriber-ipv6-multi-address predefined variable.....	289
(), in syntax descriptions.....	xxxviii
3GPP Gx	
Gx-Plus and.....	439
< >, in syntax descriptions.....	xxxviii
[], in configuration statements.....	xxxviii
{ }, in configuration statements.....	xxxviii
(pipe), in syntax descriptions.....	xxxviii

A

AAA	
ANCP interactions.....	403
configuration testing.....	515
RADIUS accounting	
Acct-On reponse state.....	1085, 1158
radius servers	
displaying.....	1159
subscriber sessions	
displaying.....	1178
subscriber statistics	
clearing.....	1027, 1029
displaying.....	1164, 1169, 1173
subscriber termination codes	
displaying.....	1183
subscribers	
displaying.....	1175
logging out.....	1029
with Diameter base protocol.....	419
AAA access messages	
supported attributes.....	31
AAA accounting messages	
supported attributes.....	37
AAA directed logout	
DHCP authentication services.....	217
AAA logical system/routing instance	
domain map.....	134

AAA Service Framework.....	3
dynamic service activation	
during login.....	144
aaa-logical-system statement	
domain map.....	623
aaa-routing-instance statement	
domain map.....	624
abated-utilization statement	
address-assignment pools.....	625
abated-utilization-v6 statement	
address-assignment pools.....	625
access loop circuit identifier	
ANCP.....	353
configuring ANCP	370
access profile	
configuring global static subscriber.....	471
configuring static subscriber group.....	476
domain map.....	132
session options.....	109
access profile statements	
access-profile-name.....	629
accounting-backup-options.....	631
ancp-speed-change-immediate-update.....	646
duplication-vrf.....	716
max-pending-accounting-stops.....	798
max-withhold-time.....	799
session-options.....	928
update-interval.....	975
vrf-name.....	995
access profiles	
attaching.....	108
configuring.....	107
access-identifier statement	
ANCP.....	626
access-loop-id-local statement.....	626
access-profile statement	
domain map.....	627
static subscribers.....	628
access-profile statements	
accounting.....	630
access-profile-name statement	
duplicate accounting.....	629
accounting	
configuring RADIUS.....	80
duplicate reports.....	87
opaque DHCP options.....	117
accounting methods.....	80
accounting statement	
access profile.....	630

accounting statistics.....	85
per-service accounting.....	85
subscriber service session.....	94, 95
subscriber session.....	92
accounting-backup-options statement	
RADIUS accounting.....	631
accounting-order statement	
service accounting.....	631
accounting-port statement.....	632
accounting-retry statement.....	633
accounting-server statement.....	633
accounting-session-id-format statement.....	634
accounting-stop-on-access-deny statement.....	634
accounting-stop-on-failure statement.....	635
accounting-timeout statement.....	635
Acct-Off messages.....	91
Acct-On messages.....	91
ACI	
ANCP.....	353
activating subscriber services.....	903
CLI-based.....	332
active server groups	
DHCP relay.....	259
active-server-group statement	
DHCP relay agent.....	636
address assignment pools	
displaying.....	1186
address assignment precedence.....	207
address pool	
domain map.....	133
address statement	
Diameter base protocol	
peer.....	637
transport.....	637
address-assignment pools	
abated-utilization.....	625
abated-utilization-v6.....	625
client attributes.....	205
configuring.....	316
DHCP attributes.....	201
mapping option 82.....	201
setting the grace period.....	201
setting the maximum lease time.....	201
setting the name server address.....	201
specifying NetBIOS node type.....	201
specifying router addresses.....	201
specifying the boot file	201
specifying the boot server	201
specifying the DNS server IPv6	
address.....	201
specifying the domain name to	
search.....	201
specifying the SIP server domain	
name.....	201
specifying the SIP server IPv6	
address.....	201
specifying the source address.....	201
specifying the TFTP server.....	201
specifying the WINS server.....	201
specifying user-defined options.....	201
DHCP local server.....	192
DHCPv6 attributes.....	201
specifying the	
preferred-lifetime.....	201, 683
specifying the t1-percentage.....	201, 683
specifying the t2-percentage.....	201, 683
specifying the valid-lifetime.....	201, 683
high-utilization.....	748
high-utilization-v6.....	748
license requirements.....	316
linking.....	320
name.....	318
named range.....	319
network address.....	318
router advertisement.....	815
static address.....	321
threshold traps.....	320
tracing operations.....	559
address-assignment statement	
address-assignment pools.....	638
address-pool statement	
domain map.....	639
adjacency timer	
ANCP global configuration.....	371
ANCP neighbor configuration.....	369, 371
adjacency-timer statement	
ANCP.....	639
advisory-options statement	
ANCP.....	640
L2TP.....	640
Agent Circuit ID suboption	
DHCP relay.....	267
Agent Remote ID suboption	
DHCP relay.....	267
aggregate-clients statement	
DHCP relay agent.....	641
static subscribers.....	642

always-write-giaddr statement		neighbor configuration	
DHCP relay agent.....	643	adjacency timer.....	369
always-write-option-82 statement		discovery table entries.....	369
DHCP relay agent.....	644	ietf mode.....	369
ANCP		IP address.....	369
AAA interactions.....	403	pre-ietf mode.....	369
access loop circuit identifier.....	353	neighbor information	
access loop circuit identifier		clearing.....	412
configuration.....	370	verifying.....	412
ACI.....	353	neighbor summary	
adjacency timer global configuration.....	371	displaying.....	1078
adjacency timer neighbor configuration.....	371	neighbors	
adjusting subscriber line traffic		displaying.....	1058
rates.....	400, 402, 407	operations in different access models.....	358
adjusting subscriber traffic with.....	395	overview.....	351
associating subscriber VLANs with access		partition ID learning.....	373
nodes.....	370	pre-ietf mode global configuration.....	372
backwards compatibility global		pre-ietf mode neighbor	
configuration.....	372	configuration.....	369, 372
backwards compatibility neighbor		regular expressions for tracing	
configuration.....	369, 372	operations.....	550
clearing statistics.....	1002	reporting traffic to CoS.....	399
configuration overview.....	368	request OAM per interface.....	1034
CoS information		request OAM per neighbor.....	1035
verifying.....	414	restart time global configuration.....	373
CoS shaping across restarts.....	398	statistics	
CoS shaping rate adjustment for subscriber		displaying.....	1066
local loops.....	395	statistics information	
CoS state		clearing.....	414
displaying ANCP.....	1055	subscriber	
discovery table global configuration.....	371	clearing.....	1004
discovery table neighbor		subscriber information	
configuration.....	369, 371	clearing.....	413
event logging.....	553	verifying.....	413
flags for tracing operations.....	554	subscriber summary	
immediate interim-accounting		displaying.....	1080
messages.....	408	subscribers	
local access loop		displaying.....	1071
displaying.....	1071	summary	
log file access for tracing operations.....	550	displaying.....	1076
log file size and number.....	549	tracing operations.....	553
log filenames for tracing operations.....	554	triggering OAM	
message severity levels for tracing		local loop.....	411
operations.....	550	ANCP agent See ANCP	
monitoring subscriber traffic with.....	351	ancp statement	
neighbor		ANCP.....	645
clearing.....	1000	ANCP statements	
		access-identifier.....	626
		adjacency-timer.....	639

advisory-options.....	640	authentication statement	
ancp.....	645	DHCP local server.....	650
ancp-speed-change-immediate-update.....	646	DHCP relay agent.....	651
downstream-rate.....	714	static subscribers.....	652
gsmpp-syn-timeout.....	745	authentication-order statement	
gsmpp-syn-wait.....	746	access.....	653
ietf-mode.....	750	authentication-server statement.....	654
interface-set.....	769	authorization, subscriber	
interfaces.....	772	JSRC.....	457
juniper-dsl-attributes.....	775	authorization-order statement	
maximum-discovery-table-entries.....	799	JSRC.....	654
maximum-helper-restart-time.....	800	auto logout	
neighbor		DHCP.....	249
for all neighbors.....	814	DHCP relay agent option 82.....	252
overhead-accounting.....	833	autonomous statement	
pre-ietf-mode.....	851	dynamic router advertisement.....	655
qos-adjust.....	868	AVPs	
qos-adjust-adsl.....	868	Diameter.....	426
qos-adjust-adsl2.....	869	Juniper Networks	
qos-adjust-adsl2-plus.....	869	Diameter and Diameter applications.....	426
qos-adjust-sdsl.....	870	B	
qos-adjust-vdsl.....	870	backup-options, RADIUS accounting	
qos-adjust-vdsl2.....	871	configuring.....	97, 101
traceoptions.....	954	overview.....	88, 182
underlying-interface.....	974	backwards compatibility	
upstream-rate.....	976	ANCP global configuration.....	372
ancp-speed-change-immediate-update statement		ANCP neighbor configuration.....	369, 372
ANCP.....	646	binding state of DHCP client	
application-group-any statement		clearing.....	1006, 1016
PTSP.....	646	displaying.....	1086, 1094
application-groups statement		binding state of DHCPv6 client	
PTSP.....	647	clearing.....	1011, 1021
applications statement		displaying.....	1102, 1111
PTSP.....	647	bindingst	
attempts statement		clearing DHCP.....	308
DHCP local server.....	648	boot-file statement.....	655
attributes statement.....	649	boot-server statement.....	656
authentication		braces, in configuration statements.....	xxxviii
configuring RADIUS.....	80	brackets	
authentication and accounting information		angle, in syntax descriptions.....	xxxviii
retaining.....	79	square, in configuration statements.....	xxxviii
authentication methods.....	80	C	
authentication password		Calling-Station-ID	
configuring global static subscriber.....	473	configuring.....	58
configuring group static subscriber.....	477	calling-station-id-delimiter statement.....	656
authentication services		calling-station-id-format statement.....	657
with DHCP.....	217	change of authorization <i>See</i> CoA	

circuit-id statement	
address-assignment pools.....	658
circuit-type statement	
DHCP local server.....	659
DHCP relay agent.....	660
clear ancp neighbor command.....	1000
clear ancp statistics command.....	1002
clear ancp subscriber command.....	1004
clear dhcp relay binding command.....	1006
clear dhcp relay statistics command.....	1008
clear dhcp server binding command.....	1016
clear dhcp server statistics command.....	1019
clear dhcpv6 relay binding command.....	1011
clear dhcpv6 relay statistics command.....	1014
clear dhcpv6 server binding command.....	1021
clear dhcpv6 server statistics command.....	1023
clear diameter function statistics command.....	1024
clear diameter peer command.....	1025
clear ipv6 router-advertisement command.....	1026
clear network-access aaa statistics	
command.....	1027
clear network-access aaa subscriber	
command.....	1029
clear network-access gx-plus replay	
command.....	1030
clear network-access gx-plus statistics	
command.....	1031
clear services subscriber sessions command.....	1033
clear-on-abort statement	
DHCP local server.....	661
client attributes	
address-assignment pools.....	205
client configuration information	
DHCP.....	190
client usernames	
DHCP	
unique.....	218
client-accounting-algorithm statement	
RADIUS.....	662
client-authentication-algorithm statement	
RADIUS.....	662
client-discover-match statement	
DHCP local server.....	663
DHCP relay agent.....	664
client-id statement.....	665
DHCP relay agent.....	666
client-idle-timeout statement	
access profile session options.....	666
client-session-timeout statement	
access profile session options.....	667
CoA	
messages.....	145
RADIUS.....	145
coa-dynamic-variable-validation.....	668
coa-immediate-update statement	
accounting.....	668
comments, in configuration statements.....	xxxviii
concurrent-data-sessions statement.....	669
connect-actively statement	
Diameter base protocol.....	670
conventions	
text and syntax.....	xxxvii
CoS	
shaping preserved across ANCP restarts.....	398
subscriber access	
modifying.....	335
traffic-control profiles.....	335
CoS traffic shaping	
with ANCP.....	400, 407
count-type statement	
PTSP.....	671
curly braces, in configuration statements.....	xxxviii
current-hop-limit statement	
dynamic router advertisement.....	672
customer support.....	xxxix
contacting JTAC.....	xxxix
D	
database-replication statement	
subscriber session database replication.....	672
deactivating subscriber services.....	905
CLI-based.....	332
CLI-based for services with multiple	
instances.....	341, 343
default subscriber service.....	199
configuring.....	200
default-action statement	
DHCP relay agent.....	673
default-lifetime statement	
dynamic router advertisement.....	674
delay-authentication statement	
DHCP relay agent.....	674
delegated-pool statement	
DHCP local server.....	675

delimiter statement		relay binding	
DHCP local server.....	676	clearing.....	1006
DHCP relay agent.....	678	relay binding state	
domain map.....	677	displaying.....	1086
delimiters		relay statistics	
domain and realm names.....	136	clearing.....	1008
demux statement		displaying.....	1091
PTSP.....	679	unique client usernames.....	218
destination statement		user passwords.....	221
Diameter base protocol.....	679	DHCP client	
destination-host statement		binding state	
Gx-Plus.....	680	clearing.....	1006, 1016
JSRC.....	680	displaying.....	1086, 1094
PTSP.....	681	statistics	
destination-realm statement		clearing.....	1008, 1019
Gx-Plus.....	682	displaying.....	1099
JSRC.....	681	DHCP lease thresholds	
PTSP.....	682	configuring.....	209
DHCP		DHCP lease time thresholds	
allowing one client per interface.....	234	DHCP.....	210
authentication services.....	217	DHCP lease-time validation.....	210
AAA directed logout.....	217	DHCP local server	
auto logout.....	249	address-assignment pool selection.....	203
centrally-configured DHCP options.....	114, 118	address-assignment pools.....	192
clearing bindings.....	308	allowing one client per interface.....	234
client configuration information.....	190	client auto logout.....	251
extended server binding		delegated IPv6 pool.....	290
clearing.....	1016	DHCPv6.....	287
displaying.....	1094	DHCPv6 rapid commit.....	291
extended server statistics		dynamic client reconfiguration	
clearing.....	1019	authentication token configuration.....	283
displaying.....	1099	behavior on failure configuration.....	247
firewall filters on routers using the jdhcpd		configuration overview.....	244
process.....	305	number of attempts configuration.....	246
example.....	301	preventing binding of nonsupporting	
grouping interfaces.....	223	clients.....	292
configuration guidelines.....	224	RADIUS-initiated disconnect	
information request processing		configuration.....	247
overriding.....	214	requesting.....	307
maximum clients per interface		grouping interfaces	
overriding.....	233	options.....	225
message severity levels for tracing		information request message processing.....	213
operations.....	525	information request processing	
override settings		overriding.....	214
deleting.....	258	interaction	
rapid commit.....	291	address-assignment pools.....	190
regular expressions for tracing		DHCP clients.....	190
operations.....	524	lease time thresholds.....	210
		lease timers.....	800

maximum clients per interface	
overriding.....	233
minimal configuration	
default settings.....	192
option 50.....	204
override settings	
deleting.....	258
overriding default configuration.....	255
overriding third-party leases.....	209
overview.....	188
per-interface tracing operations.....	526, 527
processing client information requests.....	213
reconfigure client bindings.....	1036
specific address.....	204
subnet for client addresses.....	206
tracing operations.....	521
verifying configuration.....	311
DHCP local server statements	
attempts.....	648
boot-file.....	655
boot-server.....	656
circuit-type.....	659
clear-on-abort.....	661
client-discover-match.....	663
client-id.....	665
delegated-pool	675
delimiter.....	676
dhcp-local-server.....	684
dhcpv6.....	695
dns-server.....	704
domain-name.....	706
dynamic-profile.....	717
group.....	738
interface.....	755
interface-client-limit.....	762
interface-name.....	767
interface-traceoptions.....	770
ip-address-first.....	773
lease-time-threshold.....	777
lease-time-validation.....	778
logical-system-name.....	787
mac-address.....	790
option-60.....	823
option-82.....	826, 827
overrides.....	834
password.....	844
pool.....	848
pool-match-order.....	849
process-inform.....	862
rapid-commit.....	879
relay-agent-interface-id.....	883
relay-agent-remote-id.....	886
relay-agent-subscriber-id.....	889
requested-ip-network-match.....	909
routing-instance-name.....	917
service-profile.....	926
strict.....	935
timeout.....	951
trace.....	953
traceoptions.....	958
trigger.....	972
username-include.....	988
violation-action.....	992
DHCP option information	
DHCP relay.....	273
DHCP option strings	
DHCP relay agent.....	227, 275
DHCPv6 relay agent.....	227, 275
DHCP options	
accounting.....	117
configuring on RADIUS.....	114
opaque.....	114
RADIUS-sourced.....	114
renewing.....	117
verifying.....	118
DHCP relay	
active server groups.....	259
Agent Circuit ID suboption.....	267
Agent Remote ID suboption.....	267
allowing one client per interface.....	234
automatic binding of stray requests.....	265
client auto logout.....	251
configuration examples	
minimum configuration.....	274
multiple clients and servers	
configuration.....	279
DHCP option information.....	273
DHCP relay proxy.....	197, 281
DHCPv6 Interface-ID option.....	297
DHCPv6 Remote-ID option.....	298
disabling.....	280
discarded packets	
counting.....	310
grouping interfaces	
options.....	226
how components interact.....	195
Layer 2 unicast transmission.....	263
lease time thresholds.....	210

liveness detection.....	196	interface-traceoptions.....	770
maximum clients per interface		layer2-unicast-replies.....	776
overriding.....	233	lease-time-threshold.....	777
monitoring DHCP server responsiveness.....	310	lease-time-validation.....	778
option 82		local-server-group.....	783
auto logout.....	252	logical-system-name.....	788
option 82 information.....	266	mac-address.....	791
option 82 prefix.....	269	no-bind-on-request.....	818
option 82 textual description.....	271	no-vlan-interface-name.....	820
override settings		option-60.....	824
deleting.....	258	option-number.....	829
overriding broadcast bit.....	263	overrides.....	836
overriding default configuration.....	256	password.....	845
overriding third-party leases.....	209	prefix.....	855
overview.....	194	proxy-mode.....	867
overwrite giaddr.....	261	relay-agent-interface-id.....	884
per-interface tracing operations.....	526, 527	username.....	885
replacing IP source address.....	261	relay-agent-remote-id.....	887, 888
selective traffic processing.....	227, 273, 275	relay-agent-subscriber-id.....	890
sending release messages.....	264	relay-option.....	891
server groups.....	259	relay-option-82.....	892
tracing operations.....	521	relay-server-group.....	893
trusting option 82.....	264	remote-id.....	896
verifying configuration.....	312	replace-ip-source-with.....	900
DHCP relay agent		routing-instance-name.....	916
DHCP option strings.....	227, 275	send-release-on-delete.....	922
DHCP relay agent statements		server-group.....	923
active-server-group.....	636	server-response-time.....	924
always-write-giaddr.....	643	service-profile.....	927
always-write-option-82.....	644	starts-with.....	932
circuit-type.....	660	traceoptions.....	958
client-discover-match.....	664	trust-option-82.....	973
client-id.....	666	use-interface-description.....	977
default-action.....	673	use-option-82.....	979
delay-authentication.....	674	use-primary.....	980
delimiter.....	678	user-prefix.....	984, 986
dhcp-relay.....	689	username-include.....	651, 989
dhcpv6.....	698	violation-action.....	992
disable-relay.....	704	DHCP relay proxy.....	867
domain-name.....	708	enabling.....	281
drop.....	715	how components interact.....	197
dynamic-profile.....	718	overview.....	197
equals.....	722	DHCP server responsiveness	
forward-only.....	730	monitoring.....	310
group.....	741	DHCP stray requests	
include-irb-and-l2.....	753	disabling automatic binding.....	265
interface.....	757	enabling automatic binding.....	265
interface-client-limit.....	764	DHCP subscriber	
interface-name.....	768	auto logout.....	251

- dhcp-attributes statement
 - address-assignment pools.....683
- dhcp-local-server statement.....684
- dhcp-relay statement.....689
- DHCPv6
 - DNS address
 - multiple addresses.....290, 326
 - extended server binding
 - clearing.....1021
 - displaying.....1111
 - extended server statistics
 - clearing.....1023
 - displaying.....1117
 - multiple address assignment.....289
 - relay binding
 - clearing.....1011
 - relay binding state
 - displaying.....1102
 - relay statistics
 - clearing.....1014
 - displaying.....1108
- DHCPv6 client
 - binding state
 - clearing.....1021
 - displaying.....1102, 1111
 - statistics
 - clearing.....1014, 1023
 - displaying.....1117
- DHCPv6 Interface-ID option
 - DHCP relay.....297
- DHCPv6 local server
 - IA_NA.....204
 - lease timers.....800, 853, 941, 991
 - overview.....287
 - reconfigure client bindings.....1038
 - specific address.....204
 - verifying configuration.....311
- DHCPv6 local server statements
 - multi-address-embedded-option-response...803
 - preferred-lifetime.....853
 - t1-percentage.....941
 - t2-percentage.....942
 - valid-lifetime.....991
- DHCPv6 Option-18
 - DHCP relay.....297
- DHCPv6 Option-37
 - DHCP relay.....298
- DHCPv6 relay
 - monitoring DHCP server responsiveness.....310
 - options.....295
 - options prefix.....269, 271
 - Relay Agent Interface ID option 18.....296
 - Relay Agent Remote ID option 37.....296
 - verifying configuration.....312
- DHCPv6 relay agent
 - DHCP option strings.....227, 275
- DHCPv6 Remote-ID option
 - DHCP relay.....298
- dhcpv6 statement.....695, 698
- DHCPv6client
 - binding state
 - clearing.....1011
- Diameter
 - AVPs.....426
 - message sequences for Gx-Plus.....441
 - message sequences for JSRC.....453
 - message sequences for PTSP.....481
 - messages used by Diameter applications.....421
- Diameter base protocol.....419
 - clearing function statistics.....1024
 - clearing peers.....1025
 - configuration overview.....434
 - event log access.....540
 - event logging.....543
 - filtering trace operation output.....540
 - flags for tracing operations.....544
 - function information
 - verifying.....502
 - function statistics
 - displaying.....1130
 - function status
 - displaying.....1126
 - instance information
 - displaying.....1133
 - verifying.....501
 - log file size.....539
 - log filenames.....544
 - network element configuration.....437
 - network element information
 - displaying.....1135
 - verifying.....504
 - network element map information
 - displaying.....1138
 - node information
 - verifying.....501

node status		traceoptions.....	956
displaying.....	1120	transport	
origin attribute configuration.....	435	local.....	970
peer configuration.....	435	peer.....	971
peer information		diameter statement	
verifying.....	503	Diameter base protocol.....	701
peer map		diameter-instance statement	
displaying.....	1146	Gx-Plus.....	702
peer statistics		JSRC.....	702
displaying.....	1149	PTSP.....	703
peer status		directed logout	
displaying.....	1141	AAA.....	217
route information		disable statement.....	703
displaying.....	1153	disable-relay statement.....	704
verifying.....	501	discovery table	
tracing operations.....	543	ANCP global configuration.....	371
transport configuration.....	436	ANCP neighbor configuration.....	369, 371
troubleshooting configuration.....	547	DNS (Domain Name System)	
troubleshooting connectivity.....	547	name server address	
Diameter Base Protocol		configuring.....	325
message severity levels for tracing		DNS address assignment	
operations.....	540	DHCPv6 multiple addresses.....	290, 326
Diameter base protocol statements		DNS statements	
address		domain-name-server.....	711
peer.....	637	domain-name-server-inet.....	712
transport.....	637	domain-name-server-inet6.....	713
connect-actively.....	670	dns-server statement.....	704
destination.....	679	documentation	
diameter.....	701	comments on.....	xxxix
forwarding.....	732	domain map.....	128
function		AAA logical system/routing instance.....	134
network element.....	735	access profile.....	132
route.....	736	address pool.....	133
host.....	749	configuring.....	131
logical-system.....	784	default.....	129
transport.....	785	domain name.....	136
metric.....	801	dynamic profile.....	133, 140
network-element.....	817	L2TP tunnel profile.....	139
origin.....	832	L2TP tunnel switch profile.....	140
peer		logical system/routing instance contexts.....	130
network element.....	846	none.....	129
remote.....	846	target logical system/routing instance.....	135
port.....	850	usernames with no domain name.....	129
priority.....	857	verifying configuration.....	183
realm.....	880	domain map statements	
route.....	912	aaa-logical-system.....	623
routing-instance		aaa-routing-instance.....	624
peer.....	914	access-profile.....	627
transport.....	914	address-pool.....	639

- delimiter.....677
- domain.....705
- dynamic-profile.....719
- map.....794
- mask.....795
- metric.....801
- padn.....838
- parse-direction.....839
- parse-order.....840
- realm-delimiter.....881
- realm-parse-direction881
- strip-domain.....936
- target-logical-system.....943
- target-routing-instance.....944
- tunnel-profile.....974
- domain mapping See domain map
- domain maps
 - displaying.....1187
- domain names
 - delimiters.....136
 - domain map.....136
 - parse order.....137
 - parsing direction.....138
 - stripping from username.....139
- domain statement
 - domain map.....705
- domain-name statement
 - address-assignment pools.....709
 - DHCP local server.....706
 - DHCP relay agent.....708
 - static subscribers.....710
- domain-name-server statement
 - DNS.....711
- domain-name-server-inet statement
 - DNS.....712
- domain-name-server-inet6 statement
 - DNS.....713
- downstream-rate statement
 - ANCP.....714
 - L2TP.....714
- drop statement
 - DHCP relay agent.....715
- DSL Forum VSAs.....51
 - ANCP.....405
 - supported RADIUS messages.....53
- duplicate accounting reports.....87
- duplicate accounting statements
 - access-profile-name.....629
 - duplication-vrf.....716
 - vrf-name.....995
- duplication statement.....715
- duplication-vrf statement
 - duplicate accounting.....716
- dynamic client reconfiguration
 - DHCP local server
 - attempts configuration.....246
 - authentication token configuration.....283
 - behavior on failure configuration.....247
 - configuration overview.....244
 - preventing binding of nonsupporting
 - clients.....292
 - RADIUS-initiated disconnect
 - configuration.....247
 - requesting.....307
- Dynamic Host Control Protocol See DHCP
- dynamic profiles
 - configuring global static
 - subscriber.....471, 472, 477
 - configuring static subscriber group.....476
 - domain map.....133, 140
- dynamic profiles statements
 - protocols.....864
 - router-advertisement.....913
- dynamic requests
 - RADIUS.....143, 144
- dynamic Router Advertisement protocol
 - overview.....511
- dynamic router advertisement statements
 - autonomous.....655
 - current-hop-limit.....672
 - default-lifetime.....674
 - interface.....759
 - managed-configuration.....793
 - max-advertisement-interval.....796
 - min-advertisement-interval.....802
 - no-managed-configuration.....793
 - no-other-stateful-configuration.....832
 - on-link.....819
 - other-stateful-configuration.....832
 - preferred-lifetime.....854
 - prefix.....856
 - reachable-time.....880
 - retransmit-timer.....910
 - router-advertisement.....913
 - valid-lifetime.....990

dynamic service activation	
during login.....	144
dynamic-profile statement	
DHCP local server.....	717
DHCP relay agent.....	718
domain map.....	719
static subscribers.....	720

E

enable statement.....	721
equals statement	
DHCP relay agent.....	722
ethernet-port-type-virtual statement.....	723
exceed-action statement.....	723
exclude statement.....	724
extended DHCP local server	
overview.....	188
external-authority statement	
DHCP local server pool matching.....	728

F

family statement	
address-assignment pools.....	729
firewall filter	
DHCP on routers using the jdhcpd	
process.....	305
example	
DHCP on routers using the jdhcpd	
process.....	301
font conventions.....	xxxvii
forward-only statement	
DHCP relay agent.....	730
forward-rule statement	
PTSP.....	732
forwarding instance.....	731
forwarding options	
DHCP relay agent.....	1006, 1008, 1086, 1091
DHCPv6 relay agent.....	1011, 1014, 1102, 1108
forwarding statement	
Diameter base protocol.....	732
from statement	
PTSP.....	734
PTSP forward rule.....	733
function statement	
Diameter base protocol	
network element.....	735
route.....	736
function statistics	
clearing Diameter base protocol.....	1024

G

general authentication service	
subscriber filtering for tracing	
operations.....	561, 564
tracing operations.....	559
global attributes	
Gx-Plus, configuring.....	448
global statement	
Gx-Plus.....	736
grace-period statement.....	737
group	
configuring static subscriber.....	475
group statement	
DHCP local server.....	738
DHCP relay agent.....	741
static subscribers.....	744
gsmpp-syn-timeout statement	
ANCP.....	745
gsmpp-syn-wait statement	
ANCP.....	746
Gx-Plus	
configuration overview.....	446
Diameter AVPs.....	426
Diameter message sequences.....	441
Diameter messages.....	421
disabling PCRF policy control.....	581
displaying.....	1188
global attributes	
configuring.....	448
inclusion of IPv6 subscribers	
configuring.....	448
interactions with the PCRF.....	441
number of outstanding requests	
configuring.....	448
overview.....	439
partition	
configuring.....	447
pending requests	
clearing.....	1030
provisioning subscribers.....	449
statistics	
clearing.....	1031
tracing operations.....	559
verifying.....	501, 502
Gx-plus commands	
request network-access aaa subscriber set	
session-id.....	1040
gx-plus statement	
Gx-Plus.....	747

-
- Gx-Plus statements
 - destination-host.....680
 - destination-realm.....682
 - diameter-instance.....702
 - global.....736
 - gx-plus.....747
 - include-ipv6.....752
 - max-outstanding-requests.....798
 - partition.....841
 - provisioning-order.....866
 - H**
 - hardware-address statement.....747
 - high-utilization statement
 - address-assignment pools.....748
 - high-utilization-v6 statement
 - address-assignment pools.....748
 - host statement
 - address-assignment pools.....749
 - Diameter base protocol.....749
 - I**
 - IA_NA
 - DHCPv6 local server.....204
 - idle timeout
 - subscriber access.....109
 - ietf-mode statement
 - ANCP.....750
 - IGMP
 - enabling.....865
 - ignore statement.....751
 - immediate-update statement
 - accounting.....752
 - inactive VLANs
 - removing.....112
 - include-ipv6 statement
 - Gx-Plus.....752
 - include-irb-and-l2 statement.....753
 - interface delete events
 - maintaining subscribers.....237, 238
 - interface groups
 - DHCP local server
 - configuration guidelines.....224
 - options.....225
 - DHCP relay
 - configuration guidelines.....224
 - options.....226
 - enabling static subscribers to log in.....506
 - forcing static subscribers to log out.....506
 - interface ranges
 - DHCP configuration guidelines.....224
 - interface statement
 - DHCP local server.....755
 - DHCP relay agent.....757
 - dynamic router advertisement.....759
 - static subscribers
 - group.....760
 - username.....761
 - interface-client-limit statement
 - DHCP local server.....762
 - DHCP relay agent.....764
 - interface-delete statement
 - subscriber management.....765, 766
 - interface-description-format statement.....766
 - interface-name statement
 - DHCP local server.....767
 - DHCP relay agent.....768
 - interface-set statement
 - ANCP.....769
 - interface-traceoptions statement
 - DHCP local server.....770
 - DHCP relay agent.....770
 - interfaces
 - enabling static subscribers to log in.....505
 - forcing static subscribers to log out.....505
 - interfaces statement
 - ANCP.....772
 - interim accounting
 - ANCP immediate updates.....408
 - ip-address statement.....772
 - ip-address-first statement.....773
 - IPv6
 - router advertisements
 - clearing.....1026
 - displaying.....1155
 - J**
 - JSRC
 - authorizing subscribers.....457
 - configuration overview.....455, 466
 - Diameter AVPs.....426
 - Diameter message sequences.....453
 - Diameter messages.....421
 - interactions with the SAE.....453
 - managing subscribers.....451
 - partition
 - assigning.....457
 - configuring.....456

provisioning services.....	451
provisioning static subscribers.....	463
provisioning subscribers.....	458
service accounting.....	459
tracing operations.....	559
verifying.....	501, 502
jsrc statement	
JSRC.....	774
JSRC statements	
accounting-order.....	631
authorization-order.....	654
destination-host.....	680
destination-realm.....	681
diameter-instance.....	702
jsrc.....	774
jsrc-partition.....	774
partition.....	841
provisioning-order.....	866
service.....	925
jsrc-partition statement	
JSRC.....	774
Juniper Networks VSAs.....	13
corresponding predefined variables.....	46
supported.....	21
juniper-dsl-attributes statement	
RADIUS.....	775
Junos OS	
rebooting.....	1045
L	
L2TP (Layer 2 Tunneling Protocol)	
tunnel profile	
domain map configuration.....	139
tunnel switch profile	
domain map configuration.....	140
L2TP statements	
LAC	
advisory-options.....	640
downstream-rate.....	714
upstream-rate.....	976
layer2-unicast-replies statement.....	776
lease-time-threshold	
DHCP local server.....	777
DHCP relay agent.....	777
lease-time-validation	
DHCP local server.....	778
DHCP relay agent.....	778
license requirements	
address-assignment pools.....	316
link statement	
address-assignment pools.....	779
liveness detection	
DHCP relay.....	196
LLID	
preauthentication.....	121, 122
preauthentication server.....	124
verifying configuration.....	184
local-address statement	
PTSP.....	780
local-address-range statement	
PTSP.....	781
local-port-range statement	
PTSP.....	781
local-ports statement	
PTSP.....	782
local-prefix-list statement	
PTSP.....	782
local-server-group statement	
DHCP relay agent.....	783
log files	
access to Diameter base protocol.....	540
collecting for Juniper Networks Technical Support.....	583
configuring ANCP trace.....	553
configuring Diameter base protocol trace.....	543
configuring static subscribers trace.....	571
filenames for Diameter base protocol.....	544
filenames for subscriber management	
database.....	532
filenames for subscriber management session	
database replication.....	536
number of ANCP.....	549
number of Diameter base protocol.....	539
number of static subscribers.....	567
number of subscriber management	
database.....	529
number of subscriber management session	
database replication.....	533
profile properties.....	578
size of ANCP.....	549
size of Diameter base protocol.....	539
size of packet-triggered subscribers.....	576
size of PTSP.....	577
size of static subscribers.....	567
size of subscriber management	
database.....	529
size of subscriber management session	
database replication.....	533

-
- Logical Line ID See LLID
 - logical system/routing instance contexts
 - domain map.....130
 - logical-system statement
 - Diameter base protocol.....784
 - transport.....785
 - logical-system-name statement
 - DHCP local server.....787
 - DHCP relay agent.....788
 - static subscribers.....786
 - ltv-syslog-interval statement
 - DHCP server process interval.....789
 - M**
 - mac-address statement
 - DHCP local server.....790
 - DHCP relay agent.....791
 - maintain-subscriber statement
 - subscriber management.....792
 - maintaining subscribers
 - interface delete events.....237, 238
 - verifying configuration.....238
 - managed-configuration statement
 - dynamic router advertisement.....793
 - manuals
 - comments on.....xxxix
 - map statement
 - domain map.....794
 - mask statement
 - domain map.....795
 - match-direction statement
 - PTSP.....795
 - max-advertisement-interval statement
 - dynamic router advertisement.....796
 - max-data-sessions-per-subscriber
 - statement.....778, 796
 - max-outstanding-requests statement
 - access.....797
 - Gx-Plus.....798
 - max-pending-accounting-stops statement
 - RADIUS accounting.....798
 - max-withhold-time statement
 - RADIUS accounting.....799
 - maximum-discovery-table-entries statement
 - ANCP.....799
 - maximum-helper-restart-time statement
 - ANCP.....800
 - maximum-lease-time statement.....800
 - metric statement
 - Diameter base protocol.....801
 - domain map.....801
 - min-advertisement-interval statement
 - dynamic router advertisement.....802
 - Mobile IP statements
 - statistics.....934
 - modifying subscriber services.....907
 - multi-address-embedded-option-responsestatement
 - DHCPv6 local server.....803
 - multiple address assignment
 - DHCPv6.....289
 - multiple DHCPv6 addresses
 - predefined variable.....289
 - Multiservices DPC
 - configuring PTSP.....493
 - N**
 - name-server statement.....803
 - nas-identifier statement.....804
 - NAS-Port attribute extended format
 - configuring for ATM interfaces.....76
 - configuring per physical interface.....71
 - configuring per stacked VLAN.....74
 - configuring per VLAN.....72
 - nas-port-extended-format statement
 - access profiles.....805
 - interfaces.....807
 - NAS-Port-ID
 - configuring.....56
 - NAS-Port-ID attribute
 - manual configuration.....55
 - nas-port-id-delimiter statement.....808
 - nas-port-id-format statement.....809
 - nas-port-options statement
 - RADIUS options.....810
 - NAS-Port-Type attribute
 - configuring per physical interface.....66
 - configuring per stacked VLAN.....69
 - configuring per VLAN.....68
 - manual configuration.....64
 - nas-port-type statement.....811
 - RADIUS options.....813
 - neighbor
 - ANCP.....1000
 - parameters for ANCP.....369
 - neighbor statement
 - ANCP
 - for all neighbors.....814

neighbor-discovery-router-advertisement	
statement	
address-assignment pools.....	815
netbios-node-type statement.....	815
network element	
configuring Diameter.....	437
network statement.....	816
network-element statement	
Diameter base protocol.....	817
no-bind-on-request statement	
DHCP relay agent.....	818
no-managed-configuration statement	
dynamic router advertisement.....	793
no-other-stateful-configuration statement	
dynamic router advertisement.....	832
no-vlan-interface-name statement.....	820
O	
OAM	
triggering ANCP.....	411
on-link statement	
dynamic router advertisement.....	819
opaque DHCP options.....	114
option 37 information	
DHCPv6 relay.....	295
option 38 information	
DHCPv6 relay.....	295
option 50	
DHCP local server.....	204
option 82	
DHCP relay	
auto logout.....	252
option 82 information	
DHCP relay.....	266
option 82 prefix	
DHCP relay.....	269
option 82 textual description	
DHCP relay.....	271
option statement.....	822
option-60 statement	
DHCP local server.....	823
DHCP relay agent.....	824
option-82 statement	
address-assignment pools.....	828
DHCP local server authentication.....	826
DHCP local server pool matching.....	827
DHCP relay agent.....	825
option-match statement.....	828
option-number statement	
DHCP relay agent.....	829
options	
RADIUS.....	7, 105
RADIUS server.....	4, 55, 56, 58, 64, 102
options per interface, VLAN, or S-VLAN	
NAS-Port-Type.....	66
options per interface, VLAN, or stacked VLAN	
configuration guidelines.....	62
NAS-Port extended format.....	71, 72, 74
NAS-Port-Type.....	68, 69
RADIUS server.....	60, 63
options prefix	
DHCPv6 relay.....	269, 271
options statement	
RADIUS.....	830
order statement	
accounting.....	831
origin attributes	
configuring Diameter endpoint.....	435
origin statement	
Diameter base protocol.....	832
other-stateful-configuration statement	
dynamic router advertisement.....	832
outstanding requests	
Gx-Plus, configuring.....	448
overhead-accounting statement	
ANCP.....	833
overrides statement	
DHCP local server.....	834
DHCP relay agent.....	836
P	
packet-triggered subscribers.....	482
flags for tracing operations.....	576, 579
log file size.....	576
log filenames for tracing operations.....	576
monitoring.....	507
profile properties.....	578
record type.....	578
tracing operations.....	575, 577
packet-triggered subscribers and policy control See	
PTSP	
packet-triggered-subscribers statement.....	837
packet-triggered-subscribers-partition	
statement.....	838
padn statement	
domain map.....	838
parentheses, in syntax descriptions.....	xxxviii

-
- parse order
 - domain and realm names.....137
 - parse-direction statement
 - domain map.....839
 - parse-order statement
 - domain map.....840
 - partition
 - Gx-Plus, configuring.....447
 - JSRC, assigning.....457
 - JSRC, configuring.....456
 - partition ID
 - learning ANCP.....373
 - partition statement
 - Gx-Plus.....841
 - JSRC.....841
 - PTSP.....842
 - password
 - configuring global static subscriber authentication.....473
 - configuring static subscriber group authentication.....477
 - password statement
 - DHCP local server.....844
 - DHCP relay agent.....845
 - static subscribers.....843
 - passwords
 - DHCP users.....221
 - PCRF
 - interactions with Gx-Plus.....441
 - peer
 - configuring Diameter.....435
 - peer statement
 - Diameter base protocol
 - network element.....846
 - remote peer.....846
 - peers
 - clearing Diameter base protocol.....1025
 - per-interface tracing operations
 - DHCP local server.....526, 527
 - DHCP relay.....526, 527
 - pool statement
 - address-assignment pools.....847
 - DHCP local server.....848
 - pool-match-order statement.....849
 - port statement
 - Diameter base protocol.....850
 - RADIUS servers.....850
 - pre-ietf mode
 - ANCP global configuration.....372
 - ANCP neighbor configuration.....369, 372
 - pre-ietf-mode statement
 - ANCP.....851
 - preauthentication
 - LLID.....121, 122
 - verifying configuration.....184
 - preauthentication server
 - LLID.....124
 - preauthentication-order statement
 - access profiles.....851
 - preauthentication-server statement
 - access profiles.....852
 - precedence
 - address assignment207
 - predefined variables
 - corresponding RADIUS attributes and VSAs.....46
 - preferred-lifetime statement.....853
 - dynamic router advertisement.....854
 - prefix statement
 - address-assignment pools.....856
 - DHCP relay agent.....855
 - DHCPv6 relay agent.....855
 - dynamic router advertisement.....856
 - priority statement
 - Diameter base protocol.....857
 - process-inform statement
 - DHCP local server.....862
 - profile statement
 - subscriber access.....858
 - protocol statement
 - PTSP.....863
 - protocols statement
 - dynamic profiles.....864
 - provisioning-order statement
 - subscriber services.....866
 - proxy-mode statement.....867
 - PTSP
 - configuration overview.....486
 - configuring forward rules.....498
 - configuring forwarding instance.....498
 - configuring rules.....494
 - configuring service sets.....497
 - configuring services interface.....494
 - configuring static policies.....495
 - configuring static rule sets.....497
 - configuring static rules.....495

Diameter AVPs.....	426	remote-ports.....	898
Diameter message sequences.....	481	remote-prefix-list.....	899
Diameter messages.....	421	rule-set.....	919
flags for tracing operations.....	579	services.....	928
interactions with the SAE.....	481	term	
log file size.....	577	forward rule.....	945
log filenames for tracing operations.....	577	rule.....	946
managing subscribers.....	480	then	
monitoring.....	507	forward rule.....	948
overview.....	479	rule.....	949
profile properties.....	578		
provisioning packet-triggered			
subscribers.....	482	Q	
provisioning services.....	480	qos-adjust statement	
record type.....	578	ANCP.....	868
subscriber bandwidth, displaying.....	1207	qos-adjust-adsl statement	
subscriber dynamic policies, displaying.....	1209	ANCP.....	868
subscriber flows, displaying.....	1212	qos-adjust-adsl2 statement	
subscriber sessions		ANCP.....	869
clearing.....	1033	qos-adjust-adsl2-plus statement	
displaying.....	1214	ANCP.....	869
subscriber statistics, displaying.....	1217	qos-adjust-sdsl statement	
tracing operations.....	575, 577	ANCP.....	870
verifying.....	501, 502	qos-adjust-vdsl statement	
		ANCP.....	870
PTSP statements		qos-adjust-vdsl2 statement	
application-group-any.....	646	ANCP.....	871
application-groups.....	647		
applications.....	647	R	
count-type.....	671	RADIUS	
demux.....	679	Acct-Off messages.....	91
destination-host.....	681	Acct-On messages.....	91
destination-realm.....	682	changing default idle-timeout mapping to	
diameter-instance.....	703	RADIUS code.....	153
forward-rule		changing default session-timeout mapping to	
.....	732	RADIUS code.....	153
forwarding instance.....	731	CoA.....	145
local-address.....	780	dynamic requests.....	143, 144
local-address-range.....	781	mapping terminate causes to RADIUS	
local-port-range.....	781	codes.....	151, 153
local-ports.....	782	options.....	7, 105
local-prefix-list.....	782		
match-direction.....	795	RADIUS accounting	
packet-triggered-subscribers.....	837	back-up options, configuring.....	97
packet-triggered-subscribers-partition.....	838	backing up accounting stop	
partition.....	842	requests.....	1051, 1172
protocol.....	863	backing up during an outage.....	88
remote-address.....	894	duplicating in a nondefault LS:RI.....	87
remote-address-range.....	895	forcing contact with offline server.....	101
remote-port-range.....	898		

- monitoring backup.....182
- releasing pending accounting stop requests.....902
- RADIUS accounting statements
 - access-profile-name.....629
 - accounting-backup-options.....631
 - accounting-retry.....633
 - accounting-timeout.....635
 - duplication-vrf.....716
 - max-pending-accounting-stops.....798
 - max-withhold-time.....799
 - vrf-name.....995
- RADIUS attribute 31
 - configuring.....58
- RADIUS attribute 5
 - configuring extended format per physical interface.....71
 - configuring extended format per stacked VLAN.....74
 - configuring extended format per VLAN.....72
 - configuring for ATM interfaces.....76
- RADIUS attribute 61
 - configuring per physical interface.....66
 - configuring per VLAN.....68, 69
 - manual configuration.....64
- RADIUS attribute 87
 - configuring.....56
 - manual configuration.....55
- RADIUS attributes.....13
 - configuring for ATM interfaces.....76
 - configuring per physical interface.....66, 71
 - configuring per stacked VLAN.....69, 74
 - configuring per VLAN.....68, 72
 - corresponding predefined variables.....46
 - ignoring and excluding.....40
 - preauthentication.....122
 - supported.....14
- RADIUS dynamic request information
 - verifying.....183
- RADIUS messages
 - supported DSL Forum VSAs.....53
- RADIUS preauthentication server
 - specifying.....124
- RADIUS server
 - Calling-Station-ID attribute.....58
 - configuring interaction with.....99
 - configuring parameters.....102
 - NAS-Port-ID attribute.....55, 56
 - NAS-Port-Type attribute.....64
 - options.....4, 55, 56, 58, 64, 102
 - options per interface, VLAN, or stacked VLAN.....60, 63
 - configuration guidelines.....62
- RADIUS servers
 - configuration example.....82
 - specifying.....81, 124
- radius statement
 - subscriber access.....872
- RADIUS statements
 - accounting-order.....631
 - juniper-dsl-attributes.....775
 - terminate-code.....947
- RADIUS terminate codes.....151
- radius-disconnect statement
 - DHCP local server.....874
- RADIUS-initiated disconnect.....148
 - messages.....148
- radius-options statement875, 876
- radius-server statement.....877
- RADIUS-sourced DHCP options.....114
- range statement
 - address-assignment pools.....878
- rapid commit
 - DHCP.....291
- rapid-commit statement
 - DHCP local server.....879
- reachable-time statement
 - dynamic router advertisement.....880
- realm names
 - delimiters.....136
 - parse order.....137
- realm statement
 - Diameter base protocol.....880
- realm-delimiter statement
 - domain map.....881
- realm-parse-direction statement
 - domain map.....881
- rebooting router software
 - requesting a system reboot.....1045
- reconfigure statement
 - DHCP local server.....882
- Relay Agent Interface ID option 18
 - DHCPv6 relay.....296
- Relay Agent Remote ID option 37
 - DHCPv6 relay.....296

relay-agent-interface-id statement	
DHCP local server.....	883
DHCP relay agent.....	884
username.....	885
relay-agent-remote-id statement	
DHCP local server statements.....	886
DHCP relay agent.....	887, 888
relay-agent-subscriber-id statement	
DHCP local server.....	889
DHCP relay agent.....	890
relay-option statement.....	891
relay-option-82 statement	
deleting.....	266, 892
relay-server-group statement	
DHCP relay agent.....	893
remote-address statement	
PTSP.....	894
remote-address-range statement	
PTSP.....	895
remote-id statement.....	895
DHCP relay agent.....	896
remote-port-range statement	
PTSP.....	898
remote-ports statement	
PTSP.....	898
remote-prefix-list statement	
PTSP.....	899
replace-ip-source-with statement.....	900
report-interface-descriptions statement	901
request ancp oam interface command.....	1034
request ancp oam neighbor command.....	1035
request dhcp server reconfigure command.....	1036
request dhcpv6 server reconfigure	
command.....	1038
request network-access aaa replay	
pending-accounting-stops command.....	902
request network-access aaa subscriber add	
session-id command.....	903
request network-access aaa subscriber delete	
session-id command.....	905
request network-access aaa subscriber modify	
session-id command.....	907
request network-access aaa subscriber set	
session-id command.....	1040
request services static-subscribers login group	
command.....	1041
request services static-subscribers login interface	
command.....	1043
request services static-subscribers logout group	
command.....	1042
request services static-subscribers logout interface	
command.....	1044
request system reboot command.....	1045
request-rate statement	
access.....	908
requested-ip-network-match statement	
DHCP local server.....	909
restart time	
ANCP global configuration.....	373
retransmit-timer statement	
dynamic router advertisement.....	910
retry statement.....	910
revert-interval statement.....	911
route statement	
Diameter base protocol.....	912
router advertisements	
IPv6	
clearing.....	1026
displaying.....	1155
router statement	
address-assignment pools.....	912
router-advertisement statement	
dynamic profiles.....	913
routes, displaying	
extensive information.....	1190
routing-instance statement	
Diameter base protocol	
transport.....	914
Diameter base protocol peer	
peer.....	914
RADIUS.....	913
routing-instance-name statement	
DHCP local server.....	917
DHCP relay agent.....	916
static subscribers.....	915
rule statement	
PTSP.....	918, 919
rule-set statement	
PTSP.....	919
S	
SAE	
interactions with JSRC.....	453
interactions with PTSP.....	481
service accounting with JSRC.....	459
secret statement	
access.....	920

- selective traffic processing
 - DHCP relay.....227, 273, 275
- send-acct-status-on-config-change statement
 - accounting.....921
- send-release-on-delete statement
 - DHCP relay agent.....922
- server groups
 - DHCP relay.....259
- server-group statement
 - DHCP relay agent.....923
- server-identifier statement
 - address-assignment pools.....924
- server-response-time statement
 - DHCP relay agent.....924
- service accounting
 - JSRC.....459
- service provisioning
 - packet-triggered subscribers with PTSP.....482
 - static subscribers with JSRC.....463
 - with JSRC.....451
 - with PTSP.....480
- service statement
 - service accounting.....925
- service thresholds.....147
- service-profile statement
 - DHCP local server.....926
 - DHCP relay agent.....927
- services statement
 - PTSP.....928
- services with multiple instances
 - deactivating all instances with CLI.....343
 - deactivating single instance with CLI.....341
 - overview.....339
- session options
 - subscriber access.....109
- session options statements
 - client-idle-timeout.....666
 - client-session-timeout.....667
- session startup
 - authentication and accounting
 - information.....79
- session timeout
 - subscriber access.....109
- session-options statement
 - access profile.....928
- set request services subscribers
 - command.....1032, 1050
- shaping-rate adjustments
 - for subscriber local loops.....395
- show accounting pending-accounting-stops
 - command.....1051
- show ancp cos command.....1055
- show ancp neighbor command.....1058
- show ancp statistics command.....1066
- show ancp subscriber command.....1071
- show ancp summary command.....1076
- show ancp summary neighbor command.....1078
- show ancp summary subscriber command.....1080
- show database-replication statistics
 - command.....1081
- show database-replication summary
 - command.....1083
- show dhcp relay binding command.....1086
- show dhcp relay statistics command.....1091
- show dhcp server binding command.....1094
- show dhcp server statistics command.....1099
- show dhcpv6 relay binding command.....1102
- show dhcpv6 relay statistics command.....1108
- show dhcpv6 server binding command.....1111
- show dhcpv6 server statistics command.....1117
- show diameter command.....1120
- show diameter function command.....1126
- show diameter function statistics command.....1130
- show diameter instance command.....1133
- show diameter network-element command.....1135
- show diameter network-element map
 - command.....1138
- show diameter peer command.....1141
- show diameter peer map command.....1146
- show diameter peer statistics command.....1149
- show diameter route command.....1153
- show ipv6 router-advertisement command.....1155
- show network-access aaa accounting
 - command.....1085, 1158
- show network-access aaa radius-servers
 - command.....1159
- show network-access aaa statistics authentication
 - command.....1169
- show network-access aaa statistics
 - command.....1164
- show network-access aaa statistics
 - pending-accounting-stops command.....1172
- show network-access aaa statistics
 - preauthentication command.....1173
- show network-access aaa subscriber session-id
 - command.....1178
- show network-access aaa subscribers
 - command.....1175

show network-access aaa terminate-code command.....	1183	interface group.....	760
show network-access address-assignment pool command.....	1186	username.....	761
show network-access domain-map command.....	1187	logical-system-name.....	786
show network-access gx-plus command.....	1188	password.....	843
show route extensive command.....	1190	routing-instance.....	915
show services subscriber bandwidth command.....	1207	static-subscribers.....	933
show services subscriber dynamic-policies command.....	1209	traceoptions.....	965
show services subscriber flows command.....	1212	user-prefix.....	985
show services subscriber sessions command.....	1214	username-include.....	987
show services subscriber statistics command.....	1217	static subscribers.....	463
show static-subscribers sessions command.....	1219	configuring interface groups.....	475
show subscribers command.....	1221	event logging.....	571
show subscribers summary command.....	1239	flags for tracing operations.....	572
show system subscriber-management summary command.....	1244	forced group logout.....	1042
sip-server-address statement.....	929	forced logout.....	1044
sip-server-domain-name statement.....	929	forcing logout.....	505
source-address statement RADIUS.....	930	forcing logout for interface groups.....	506
SRC packet-triggered subscriber management with PTSP.....	482	global access profile.....	471
SAE interactions with JSRC.....	453	global authentication password.....	473
SAE interactions with PTSP.....	481	global dynamic profile.....	471, 472, 477
static subscriber management with JSRC.....	463	global username.....	473
subscriber management with JSRC.....	451	group.....	475
subscriber management with PTSP.....	480	group access profile.....	476
stacked VLANs configuration guidelines for RADIUS options.....	62	group authentication password.....	477
configuring RADIUS options for.....	63, 69	group dynamic profile.....	476
overview of configuring RADIUS options for.....	60	group username.....	478
stacked-vlan-ranges statement.....	931	interface group state reset.....	1041
starts-with statement DHCP relay agent.....	932	interface state reset.....	1043
static subscriber statements access-profile.....	628	log file access for tracing operations.....	568
aggregate-clients.....	642	log file size and number.....	567
authentication.....	652	log filenames for tracing operations.....	572
domain-name.....	710	message severity levels for tracing operations.....	568
dynamic-profile.....	720	regular expressions for tracing operations.....	568
group.....	744	resetting login state for an interface.....	505
		resetting login state for interface groups.....	506
		session status displaying.....	1219
		verifying.....	506
		tracing operations.....	571
		static-subscribers statement.....	933
		statistics statement access.....	934
		strict statement DHCP local server.....	935
		strip-domain statement domain map.....	936

subscriber	
ANCP.....	1004
subscriber AAA information	
verifying.....	181
subscriber access	
subscriber information, displaying.....	1221
subscriber summary information,	
displaying.....	1239
subscriber local loops	
CoS shaping-rate adjustments with	
ANCP.....	395
subscriber management	
packet-triggered.....	482
static.....	463
with JSRC.....	451
with PTSP.....	480
subscriber management database	
flags for tracing operations.....	532
log file access for tracing operations.....	530
log file size and number.....	529
log filenames.....	532
regular expressions for tracing	
operations.....	530
statistics information, displaying.....	1081
summary information, displaying.....	1083, 1244
tracing operations.....	531
subscriber management session database	
replication	
flags for tracing operations.....	536
log file access for tracing operations.....	534
log file size and number.....	533
log filenames.....	536
regular expressions for tracing	
operations.....	534
tracing operations.....	535
subscriber management statements	
interface-delete.....	765, 766
maintain-subscriber.....	792
subscriber-management.....	939
traceoptions.....	967
subscriber provisioning	
Gx-Plus.....	449
JSRC.....	458
subscriber service	
activating with CLI.....	331
deactivating with CLI.....	331
default.....	199, 200
subscriber service session	
accounting statistics.....	94, 95
subscriber services	
activating.....	903
activating with CLI.....	332
deactivating.....	905
deactivating with CLI.....	332
local activation and deactivation.....	332
modifying.....	907
removing PCRF control.....	581, 1040
subscriber services with multiple instances	
deactivating all instances with CLI.....	343
deactivating single instance with CLI.....	341
local deactivation with CLI.....	341, 343
overview.....	339
subscriber session	
accounting statistics.....	92
subscriber session database statements	
database-replication.....	672
traceoptions.....	969
subscriber session options	
configuration overview.....	111
removing inactive VLANs.....	112
subscriber-identification statement	
PTSP.....	937
subscriber-management statement	
subscriber management.....	939
subscriber-packet-idle-timeout statement.....	938
subscriber-profile statement.....	940
subscribers	
displaying.....	1221
displaying summary.....	1239
identifying ANCP.....	370
support, technical See technical support	
syntax conventions.....	xxxvii
T	
t1-percentage statement.....	941, 942
t2-percentage statement.....	942
target logical system/routing instance	
domain map.....	135
target-logical-system statement	
domain map.....	943
target-routing-instance statement	
domain map.....	944
technical support	
collecting logs for.....	583
contacting JTAC.....	xxxix

term statement	
PTSP	
forward rule.....	945
rule.....	946
terminate-code statement.....	947
test aaa authd-lite user command.....	1246
test aaa dhcp user command.....	1249
test aaa ppp user command.....	1252
tftp-server statement.....	948
then statement	
PTSP	
forward rule.....	948
rule.....	949
third-party DHCP leases	
overriding.....	209
thresholds	
subscriber service.....	147
timeout statement	
access.....	950
DHCP local server.....	951
timeouts	
idle and session.....	109
token statement	
DHCP local server.....	952
trace operations	
collecting logs for Juniper Networks Technical Support.....	583
filtering output for Diameter base protocol.....	540
trace statement	
DHCP local server.....	953
tracoptions statement	
address-assignment pools.....	961
ANCP.....	954
DHCP local server.....	958
DHCP relay agent.....	958
Diameter base protocol.....	956
general authentication service.....	961
PTSP.....	963
static subscribers.....	965
subscriber management.....	967
subscriber session database replication.....	969
tracing operations	
address-assignment pools.....	559
ANCP.....	553
DHCP local server.....	521
DHCP local server interface-specific.....	770
DHCP relay.....	521
DHCP relay interface-specific.....	770
Diameter base protocol.....	543
general authentication service.....	559
Gx-Plus.....	559
JSRC.....	559
packet-triggered subscribers.....	575, 577
PTSP.....	575, 577
static subscribers.....	571
subscriber management database.....	531
subscriber management session database replication.....	535
traffic shaping	
adjustment of ANCP.....	400, 402, 407
ANCP-agent reported rates for CoS.....	399
traffic-control profiles	
global modification.....	336
modifying.....	335
per-subscriber modification.....	336
transport	
configuring Diameter.....	436
transport statement	
Diameter base protocol	
local.....	970
peer.....	971
trigger statement	
DHCP local server.....	972
troubleshooting subscriber access	
collecting logs for Juniper Networks Technical Support.....	583
trust-option-82 statement.....	973
tunnel profile, L2TP	
domain map.....	139
tunnel switching, L2TP	
domain map configuration.....	140
tunnel-profile statement	
domain map.....	974
U	
underlying-interface statement	
ANCP interface set.....	974
update-interval statement	
access profile.....	975
upstream-rate statement	
ANCP.....	976
L2TP.....	976
use-interface-description statement.....	977
use-option-82 statement.....	979
use-primary statement	
DHCP relay agent.....	980
use-vlan-id statement.....	982

user-prefix statement	
DHCP local server.....	986
DHCP relay agent.....	984
static subscribers.....	985
username	
configuring global static subscriber.....	473
configuring static subscriber group.....	478
username-include statement	
DHCP local server.....	988
DHCP relay agent.....	989
static subscribers.....	987

V

valid-lifetime statement.....	991
dynamic router advertisement.....	990
variables, Junos OS predefined	
corresponding RADIUS attributes and	
VSAs.....	46
vendor-specific attributes	
supported.....	21
violation-action	
DHCP local server.....	992
DHCP relay agent.....	992
vlan-nas-port-stacked-format statement.....	993
vlan-ranges statement.....	994
VLANs	
configuration guidelines for RADIUS	
options.....	62
configuring RADIUS options for.....	63, 68
overview of configuring RADIUS options.....	60
removing inactive.....	112
vrf-name statement	
duplicate accounting.....	995
VSA 26-55	
opaque DHCP options.....	114
RADIUS-sourced DHCP options.....	114
VSAs	
ANCP-related DSL Forum.....	405
corresponding predefined variables.....	46
DSL Forum.....	51
supported.....	21

W

wait-for-acct-on-ack statement	
accounting.....	995
wins-server statement.....	996

