



Junos[®] OS

Broadband Subscriber Management Wholesale Feature Guide



Modified: 2017-08-14

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

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be 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 Management Wholesale Feature Guide
Copyright © 2017 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/>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the Documentation	xvii
	Documentation and Release Notes	xvii
	Supported Platforms	xvii
	Using the Examples in This Manual	xvii
	Merging a Full Example	xviii
	Merging a Snippet	xviii
	Documentation Conventions	xix
	Documentation Feedback	xxi
	Requesting Technical Support	xxi
	Self-Help Online Tools and Resources	xxi
	Opening a Case with JTAC	xxii
Part 1	Configuring DHCP Layer 3 Wholesale Networks	
Chapter 1	Subscriber Management DHCP Layer 3 Wholesale Overview	3
	Layer 2 and Layer 3 Wholesale Overview	3
	Wholesale Network Configuration Options and Considerations	4
	DHCP Layer 3 Wholesale Configuration Interface Support	5
	Layer 3 Wholesale Configuration DHCP Support	5
	Subscriber to Logical System and Routing Instance Relationship	6
	RADIUS VSAs and Broadband Subscriber Management Wholesale Configuration Overview	6
Chapter 2	Configuring DHCPv4 Layer 3 Wholesale Networks	9
	Broadband Subscriber Management DHCPv4 Layer 3 Wholesale Topology and Configuration Elements	9
	DHCPv4 Layer 3 Wholesale Network Topology Overview	10
	Configuring Loopback Interfaces for the DHCPv4 Layer 3 Wholesale Solution	11
	Configuring VLANs for the DHCPv4 Layer 3 Wholesale Network Solution	13
	Configuring Static Customer VLANs for the DHCPv4 Layer 3 Wholesale Network Solution	13
	Configuring Dynamic VLANs for the DHCPv4 Layer 3 Wholesale Network Solution	14
	Configuring Access Components for the DHCP Layer 3 Wholesale Network Solution	16
	Configuring RADIUS Server Access	16
	Configuring a DHCP Wholesaler Access Profile	16
	Configuring DHCP Retailer Access Profiles	17

	Configuring Dynamic Profiles for the DHCPv4 Layer 3 Wholesale Network	
	Solution	18
	Configuring a Wholesale Dynamic Profile for use in the DHCPv4	
	Solution	18
	Configuring a Dynamic Profile for use by a Retailer in the DHCPv4	
	Solution	20
	Configuring Separate Routing Instances for DHCPv4 Service Retailers	21
	Configure Default Forwarding Options for the DHCPv4 Wholesale Network	
	Solution	23
	Example: Wholesaler Dynamic Profile for a DHCPv4 Wholesale Network	26
	Example: Retailer Dynamic Profile for a DHCPv4 Wholesale Network	26
	Example: Default Forwarding Options Configuration for the DHCPv4 Wholesale	
	Network	27
	Example: Retailer Routing Instances for a DHCPv4 Wholesale Network	28
Chapter 3	Configuring DHCPv6 Layer 3 Wholesale Networks	31
	Broadband Subscriber Management DHCPv6 Layer 3 Wholesale Topology and	
	Configuration Elements	31
	DHCPv6 Layer 3 Wholesale Network Topology Overview	33
	Configuring Loopback Interfaces for the DHCPv6 Layer 3 Wholesale Solution	34
	Configuring VLANs for the DHCPv6 Layer 3 Wholesale Network Solution	34
	Configuring Static Customer VLANs for the DHCPv6 Layer 3 Wholesale	
	Network Solution	35
	Configuring Dynamic Customer VLANs for the DHCPv6 Layer 3 Wholesale	
	Network Solution	35
	Configuring Access Components for the DHCP Layer 3 Wholesale Network	
	Solution	37
	Configuring RADIUS Server Access	38
	Configuring a DHCP Wholesaler Access Profile	38
	Configuring DHCP Retailer Access Profiles	39
	Configuring Dynamic Profiles for the DHCPv6 Layer 3 Wholesale Network	
	Solution	40
	Configuring a Wholesale Dynamic Profile for use in the DHCPv6	
	Solution	40
	Configuring a Dynamic Profile for use by Each Retailer in the DHCPv6	
	Solution	41
	Configuring Separate Routing Instances for DHCPv6 Service Retailers	42
	Configuring Address Server Elements for the DHCPv6 Layer 3 Wholesale	
	Solution	43
	Configuring a DHCPv6 Address Assignment Pool	43
	Configuring Extended DHCPv6 Local Server	45
	Example: Retailer Dynamic Profile for a DHCPv6 Wholesale Network	46
	Example: Retailer Routing Instances for a DHCPv6 Wholesale Network	47
	Example: DHCPv6 Address Assignment Pool That Provides Full 128-bit IPV6	
	Addresses for a DHCPv6 Wholesale Network	47
	Example: DHCPv6 Address Assignment Pool That Provides 74-bit IPV6 Prefixes	
	for a DHCPv6 Wholesale Network	48
	Example: Extended DHCPv6 Local Server for a DHCPv6 Wholesale Network	48

Part 2	Configuring PPPoE Layer 3 Wholesale Networks	
Chapter 4	Subscriber Management PPPoE Wholesale Overview	53
	Layer 2 and Layer 3 Wholesale Overview	53
	PPPoE Layer 3 Wholesale Configuration Interface Support	54
	Subscriber to Logical System and Routing Instance Relationship	54
	RADIUS VSAs and Broadband Subscriber Management Wholesale Configuration Overview	55
Chapter 5	Configuring PPPoE Layer 3 Wholesale Networks	57
	Broadband Subscriber Management PPPoE Layer 3 Wholesale Topology and Configuration Elements	57
	PPPoE Layer 3 Wholesale Network Topology Overview	59
	Configuring Loopback Interfaces for the PPPoE Layer 3 Wholesale Solution	59
	Configuring Static Customer VLANs for the PPPoE Layer 3 Wholesale Network Solution	61
	Configuring Access Components for the PPPoE Wholesale Network Solution	61
	Configuring RADIUS Server Access	62
	Configuring a PPPoE Wholesaler Access Profile	62
	Configuring PPPoE Retailer Access Profiles	63
	Configuring Dynamic Profiles for the PPPoE Layer 3 Wholesale Network Solution	64
	Configuring a Wholesale Dynamic Profile for use in the PPPoE Solution	64
	Configuring Separate Routing Instances for PPPoE Service Retailers	66
	Example: Wholesaler Dynamic Profile for a PPPoE Wholesale Network	67
	Example: Retailer Routing Instances for a PPPoE Wholesale Network	67
Part 3	Configuring Layer 2 Wholesale Networks	
Chapter 6	Subscriber Management Layer 2 Wholesale Overview	71
	Layer 2 and Layer 3 Wholesale Overview	71
	Wholesale Network Configuration Options and Considerations	72
	RADIUS VSAs and Broadband Subscriber Management Wholesale Configuration Overview	73
Chapter 7	Configuring Layer 2 Wholesale Networks	75
	Broadband Subscriber Management Layer 2 Wholesale Topology and Configuration Elements	75
	Layer 2 Wholesale Network Topology Overview	77
	Configuring a Retail Dynamic Profile for Use in the Layer 2 Wholesale Solution	79
	Stacking and Rewriting VLAN Tags for the Layer 2 Wholesale Solution	80
	Configuring VLAN Interfaces for the Layer 2 Wholesale Solution	82
	Configuring Encapsulation for Layer 2 Wholesale VLAN Interfaces	83
	Configuring NNI ISP-Facing Interfaces for the Layer 2 Wholesale Solution	84
	Configuring Direct ISP-Facing Interfaces for the Layer 2 Wholesale Solution	85
	Configuring Separate Access Routing Instances for Layer 2 Wholesale Service Retailers	86

	Configuring Separate NNI Routing Instances for Layer 2 Wholesale Service Retailers	89
	Configuring Access Components for the Layer 2 Wholesale Network Solution	91
	Configuring RADIUS Server Access	91
	Configuring a Layer 2 Wholesaler Access Profile	91
	Example: Retailer Dynamic Profile for a Layer 2 Wholesale Network	92
	Example: Access Interface for a Layer 2 Wholesale Network	93
	Example: Retailer Access Routing Instances for a Layer 2 Wholesale Network	93
	Example: Retailer NNI ISP-Facing Interfaces for a Layer 2 Wholesale Network	94
	Example: Retailer Direct ISP-Facing Interface for a Layer 2 Wholesale Network	95
Part 4	Configuring ANCP-Triggered Layer 2 Wholesale Services	
Chapter 8	ANCP-Triggered Layer 2 Wholesale Service Overview	99
	Layer 2 Wholesale with ANCP-Triggered VLANs Overview	99
	RADIUS Authorization for ANCP-Triggered VLANs	102
	Instantiation of an ANCP-Triggered, Autosensed, Dynamic VLAN	103
	Weighted Load Balancing for Subscriber Sessions over Eligible Core-Facing Physical Interfaces	104
	RADIUS Interim Accounting Updates	105
	Removal of the Layer 2 Wholesale Service	106
	Interactions Between In-Band and Out-of-Band VLAN Autosensing	107
	Migration of Subscriber Ownership from Wholesaler to Retailer	109
	Migration of Subscriber Ownership from Retailer to Wholesaler	109
	Migration of Subscriber Ownership Between Retailers	110
	Modification of the Access Line Identifier or Port VLAN Identifier	111
	Disconnecting PPPoE Sessions and Automatically Attempting Reconnection as Layer 2 Wholesale Sessions	112
	Consequences of a State Transition in the Access-Facing Physical Interface	113
	Consequences of a State Transition from Up to Down in the Core-Facing Physical Interface	114
	Consequences of a State Transition from Down to Up in the Core-Facing Physical Interface	116
	Loss of ANCP TCP Adjacency	116
	Junos OS Predefined Variables	118
	Juniper Networks VSAs Supported by the AAA Service Framework	143
	AAA Access Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS	154
	AAA Accounting Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS	160
Chapter 9	Configuring ANCP-Triggered Layer 2 Wholesale Services	165
	Configuring ANCP Neighbors	165
	Configuring the ANCP Agent for ANCP-Triggered, Autosensed Dynamic VLANs	167

	Configuring a Username for Authentication of Out-of-Band Triggered Dynamic VLANs	168
	Configuring Out-of-Band ANCP Messages to Trigger Dynamic VLAN Instantiation	169
	Triggering ANCP OAM to Simulate ANCP Port Down and Port Up Messages . . .	170
	Configuring the ANCP Agent to Dampen the Effects of Short-Term Adjacency Losses	172
	Reestablishing Pending Access Line Sessions for Layer 2 Wholesale	173
	Configuring Multiple Non-Overlapping VLAN Ranges for Core-Facing Physical Interfaces	173
	Clearing ANCP Access Loops	174
Chapter 10	Configuring Flat-File Accounting for Layer 2 Wholesale Services	177
	Flat-File Accounting Overview	177
	Configuring Flat-File Accounting for Layer 2 Wholesale	181
	Configuring Flat-File Accounting for Extensible Subscriber Services Management	185
	Configuring Service Accounting in Local Flat Files	189
Part 5	Configuration Statements and Operational Commands	
Chapter 11	Configuration Statements	195
	accept	199
	accept-out-of-band	200
	access-profile	201
	access-profile (Dynamic VLAN)	202
	access-profile (Dynamic Stacked VLAN)	203
	accounting-server	204
	active-server-group	205
	address	206
	address-assignment (Address-Assignment Pools)	209
	adjacency-loss-hold-time (ANCP)	210
	ancp	211
	authentication	213
	authentication (DHCP Local Server)	214
	authentication (DHCP Relay Agent)	215
	authentication-order	216
	authentication-server	217
	auto-configure	218
	auto-configure-trigger interface (ANCP)	219
	backup-on-failure (Accounting Options)	220
	circuit-id (VLAN Authentication Username)	221
	cleanup-interval (Accounting Options)	222
	compress (Accounting Options)	223
	connectivity-type	224
	core-facing	225
	demux0 (Dynamic Interface)	226
	demux-options (Dynamic Interface)	227
	demux-source (Dynamic IP Demux Interface)	228
	demux-source (Dynamic Underlying Interface)	229

demux-source (Underlying Interface)	230
dhcp-attributes (Address-Assignment Pools)	231
dhcp-local-server	233
dhcp-relay	239
dhcpcv6 (DHCP Local Server)	248
domain-name (Address-Assignment Pools)	251
dynamic-profile (DHCP Local Server)	252
dynamic-profile (DHCP Relay Agent)	253
dynamic-profile (Dynamic PPPoE)	254
dynamic-profile (Stacked VLAN)	255
dynamic-profile (VLAN)	256
dynamic-profiles	257
egress-stats (Flat-File Accounting Options)	266
encapsulation (Dynamic Interfaces)	268
encapsulation (Logical Interface)	271
encapsulation (Physical Interface)	275
exclude (RADIUS)	281
family	286
family (Address-Assignment Pools)	291
family (Dynamic Demux Interface)	292
family (Dynamic PPPoE)	293
family (Dynamic Standard Interface)	294
fields (Flat-File Accounting Options)	296
file (Flat-File Accounting Options)	298
flat-file-profile (Accounting Options)	299
flat-file-profile (Extensible Subscriber Services)	301
flexible-vlan-tagging	302
format (Flat-File Accounting Options)	303
forwarding-options	304
general-param (Flat-File Accounting Options)	305
grace-period	306
group (DHCP Local Server)	307
group (DHCP Relay Agent)	310
ingress-stats (Flat-File Accounting Options)	314
inner-vlan-id (Dynamic VLANs)	315
inner-vlan-id-swap-ranges	316
input-vlan-map (Dynamic Interfaces)	317
interface (DHCP Local Server)	318
interface (DHCP Relay Agent)	320
interface (Dynamic Routing Instances)	322
interface (Routing Instances)	323
interface-mac-limit (VPLS)	324
interfaces	325
interfaces (Static and Dynamic Subscribers)	326
interval (Flat-File Accounting Options)	331
instance-role	332
instance-type	333
ip-address-first	335
keepalives (Dynamic Profiles)	336

l2-stats (Flat-File Accounting Options)	337
mac-validate (Dynamic IP Demux Interface)	338
multicast-replication	339
neighbor (Define ANCP)	340
no-local-switching	340
no-tunnel-services	341
maximum-lease-time	342
overall-packet (Flat-File Accounting Options)	343
output-vlan-map (Dynamic Interfaces)	344
pap (Dynamic PPP)	345
pool (Address-Assignment Pools)	346
pool-match-order	347
pop (Dynamic VLANs)	348
pppoe-options (Dynamic PPPoE)	348
pppoe-underlying-options (Static and Dynamic Subscribers)	349
ppp-options (Dynamic PPP)	350
prefix (Address-Assignment Pools)	351
profile (Access)	352
protocols	357
proxy-arp	360
proxy-arp (Dynamic Profiles)	361
push (Dynamic VLANs)	361
push-backup-to-master (Accounting Options)	362
radius (Access Profile)	363
radius-server	365
range (Address-Assignment Pools)	366
ranges (Dynamic VLAN)	367
remote-id (VLAN Authentication Username)	368
route-distinguisher	369
routing-instances (Dynamic Profiles)	371
routing-instances (Multiple Routing Entities)	373
schema-version (Flat-File Accounting Options)	374
secret	375
server (Dynamic PPPoE)	376
server-group	377
site (VPLS Multihoming for FEC 128)	378
site-identifier (VPLS)	379
site-range	380
stacked-vlan-ranges	381
stacked-vlan-tagging	382
system	382
traceoptions (DHCP)	383
underlying-interface (demux0)	385
underlying-interface (Dynamic PPPoE)	386
unit	387
unit (Dynamic Demux Interface)	394
unit (Dynamic Profiles Standard Interface)	396
unnumbered-address (Dynamic PPPoE)	399
unnumbered-address (Dynamic Profiles)	400

	unnumbered-address (Ethernet)	402
	username-include	403
	user-prefix (DHCP Local Server)	404
	vlan-id (Dynamic VLANs)	405
	vlan-id (VLAN ID to Be Bound to a Logical Interface)	406
	vlan-model	407
	vlan-ranges	408
	vlan-tags	409
	vlan-tags (Stacked VLAN Tags)	410
	vpls (Routing Instance)	412
	vrf-export	414
	vrf-import	415
	vrf-target	416
Chapter 12	Operational Commands	419
	clear ancp access-loop	421
	clear ancp neighbor	423
	clear dhcp relay binding	425
	clear dhcp relay statistics	428
	clear dhcp server binding	431
	clear dhcp server statistics	434
	clear dhcpv6 server binding	436
	clear dhcpv6 server statistics	439
	clear network-access aaa subscriber	440
	request ancp oam port-down	442
	request ancp oam port-up	444
	request auto-configuration reconnect-pending	446
	show ancp neighbor	447
	show auto-configuration out-of-band pending	455
	show dhcp relay binding	456
	show dhcp relay statistics	462
	show dhcp server binding	466
	show dhcp server statistics	473
	show dhcpv6 server binding	477
	show dhcpv6 server statistics	483
	show interfaces (Aggregated Ethernet)	486
	show interfaces (Fast Ethernet)	497
	show interfaces (Gigabit Ethernet)	514
	show interfaces (Loopback)	539
	show interfaces (PPPoE)	546
	show interfaces demux0 (Demux Interfaces)	556
	show interfaces filters	566
	show interfaces l2-routing-instance	568
	show interfaces routing	570
	show interfaces routing-instance	576
	show network-access aaa statistics	578
	show network-access aaa statistics authentication	587
	show network-access aaa subscribers	590
	show network-access address-assignment pool	595

show ppp interface	597
show subscribers	606
show subscribers summary	632
show vpls connections	638
show vpls flood event-queue	649
show vpls flood instance	651
show vpls flood route	653
show vpls mac-table	655
show vpls statistics	660

List of Figures

Part 1	Configuring DHCP Layer 3 Wholesale Networks	
Chapter 2	Configuring DHCPv4 Layer 3 Wholesale Networks	9
	Figure 1: Basic Subscriber Management Layer 3 Wholesale Solution Topology	10
	Figure 2: DHCPv4 Layer 3 Wholesale Network Reference Topology	11
Chapter 3	Configuring DHCPv6 Layer 3 Wholesale Networks	31
	Figure 3: Basic Subscriber Management DHCPv6 Layer 3 Wholesale Solution Topology	32
	Figure 4: DHCPv6 Layer 3 Wholesale Network Reference Topology	33
Part 2	Configuring PPPoE Layer 3 Wholesale Networks	
Chapter 5	Configuring PPPoE Layer 3 Wholesale Networks	57
	Figure 5: Basic Subscriber Management PPPoE Layer 3 Wholesale Solution Topology	58
	Figure 6: PPPoE Layer 3 Wholesale Network Reference Topology	59
Part 3	Configuring Layer 2 Wholesale Networks	
Chapter 7	Configuring Layer 2 Wholesale Networks	75
	Figure 7: Basic Subscriber Management Layer 2 Wholesale Solution Topology	76
	Figure 8: Layer 2 Wholesale Network Reference Topology	78
Part 4	Configuring ANCP-Triggered Layer 2 Wholesale Services	
Chapter 8	ANCP-Triggered Layer 2 Wholesale Service Overview	99
	Figure 9: Sample Layer 2 Wholesale Access Topology	100

List of Tables

	About the Documentation	xvii
	Table 1: Notice Icons	xix
	Table 2: Text and Syntax Conventions	xx
Part 1	Configuring DHCP Layer 3 Wholesale Networks	
Chapter 1	Subscriber Management DHCP Layer 3 Wholesale Overview	3
	Table 3: Required Juniper Networks VSAs for the Broadband Subscriber Management Wholesale Network Solution	6
Part 2	Configuring PPPoE Layer 3 Wholesale Networks	
Chapter 4	Subscriber Management PPPoE Wholesale Overview	53
	Table 4: Required Juniper Networks VSAs for the Broadband Subscriber Management Wholesale Network Solution	55
Part 3	Configuring Layer 2 Wholesale Networks	
Chapter 6	Subscriber Management Layer 2 Wholesale Overview	71
	Table 5: Required Juniper Networks VSAs for the Broadband Subscriber Management Wholesale Network Solution	73
Chapter 7	Configuring Layer 2 Wholesale Networks	75
	Table 6: Rewrite Operations on Single-Tagged and Dual-Tagged Frames	80
	Table 7: Applying Rewrite Operations to VLAN Maps	81
	Table 8: Encapsulation Combinations for Layer 2 Wholesale Interfaces	84
Part 4	Configuring ANCP-Triggered Layer 2 Wholesale Services	
Chapter 8	ANCP-Triggered Layer 2 Wholesale Service Overview	99
	Table 9: Junos OS Predefined Variables and Definitions	118
	Table 10: Supported Juniper Networks VSAs	143
	Table 11: AAA Access Messages—Supported RADIUS Attributes and Juniper Networks VSAs	154
	Table 12: AAA Accounting Messages—Supported RADIUS Attributes and Juniper Networks VSAs	160
Chapter 10	Configuring Flat-File Accounting for Layer 2 Wholesale Services	177
	Table 13: Value of Elements in Sample Accounting Flat File XML Header	178
Part 5	Configuration Statements and Operational Commands	
Chapter 12	Operational Commands	419

Table 14: clear dhcp relay statistics Output Fields	429
Table 15: show ancp neighbor Output Fields	447
Table 16: show auto-configuration out-of-band pending Output Fields	455
Table 17: show dhcp relay binding Output Fields	457
Table 18: show dhcp relay statistics Output Fields	463
Table 19: show dhcp server binding Output Fields	467
Table 20: show dhcp server statistics Output Fields	474
Table 21: show dhcpv6 server binding Output Fields	478
Table 22: show dhcpv6 server statistics Output Fields	484
Table 23: Aggregated Ethernet show interfaces Output Fields	486
Table 24: show interfaces Fast Ethernet Output Fields	497
Table 25: show interfaces (Gigabit Ethernet) Output Fields	515
Table 26: Gigabit Ethernet IQ PIC Traffic and MAC Statistics by Interface Type	530
Table 27: Loopback show interfaces Output Fields	539
Table 28: show interfaces (PPPoE) Output Fields	546
Table 29: show interfaces demux0 (Demux Interfaces) Output Fields	556
Table 30: show interfaces filters Output Fields	566
Table 31: show interfaces l2-routing-instance Output Fields	568
Table 32: show interfaces routing Output Fields	570
Table 33: show network-access aaa statistics Output Fields	579
Table 34: show network-access aaa statistics authentication Output Fields	587
Table 35: show network-access aaa subscribers Output Fields	590
Table 36: show network-access address-assignment pool Output Fields	595
Table 37: show ppp interface Output Fields	597
Table 38: show subscribers Output Fields	610
Table 39: show subscribers summary Output Fields	633
Table 40: show vpls connections Output Fields	639
Table 41: show vpls flood event-queue Output Fields	649
Table 42: show vpls flood instance Output Fields	651
Table 43: show vpls flood route Output Fields	653
Table 44: show vpls mac-table Output fields	656
Table 45: show vpls statistics Output Fields	660

About the Documentation

- Documentation and Release Notes on page xvii
- Supported Platforms on page xvii
- Using the Examples in This Manual on page xvii
- Documentation Conventions on page xix
- Documentation Feedback on page xxi
- Requesting Technical Support on page xxi

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 [CLI Explorer](#).

Documentation Conventions

Table 1 on page xix 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 xx 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
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

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

Convention	Description	Examples
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.
> (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 DHCP Layer 3 Wholesale Networks

- [Subscriber Management DHCP Layer 3 Wholesale Overview on page 3](#)
- [Configuring DHCPv4 Layer 3 Wholesale Networks on page 9](#)
- [Configuring DHCPv6 Layer 3 Wholesale Networks on page 31](#)

CHAPTER 1

Subscriber Management DHCP Layer 3 Wholesale Overview

- [Layer 2 and Layer 3 Wholesale Overview on page 3](#)
- [Wholesale Network Configuration Options and Considerations on page 4](#)
- [DHCP Layer 3 Wholesale Configuration Interface Support on page 5](#)
- [Layer 3 Wholesale Configuration DHCP Support on page 5](#)
- [Subscriber to Logical System and Routing Instance Relationship on page 6](#)
- [RADIUS VSAs and Broadband Subscriber Management Wholesale Configuration Overview on page 6](#)

Layer 2 and Layer 3 Wholesale Overview

In general, wholesaling broadband services allows service providers to resell broadband services and allows other providers to deploy their own services over the incumbent network. There are different methods to partitioning an access network for resale. The two most common approaches are based on either Layer 2 or Layer 3 information. Wholesale access is the process by which the access network provider (the *wholesaler*) partitions the access network into separately manageable and accountable subscriber segments for resale to other network providers (or *retailers*).

In a Layer 3 wholesale configuration, you partition the wholesaler access network at the network layer or the subscriber IP component by associating the IP component with a distinct Layer 3 domain. In a Layer 2 wholesale configuration, you partition the access network at the subscriber circuit or customer VLAN (C-VLAN) by backhauling the connection through the service provider backbone network to the subscribing retailer network where the access traffic can be managed at higher layers.

In a Junos OS Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol over Ethernet (PPPoE) subscriber access configuration, wholesale partitioning is accomplished through the use of logical systems and routing instances within the router. Logical systems offer a stricter partitioning of routing resources than routing instances. The purpose behind the use of logical systems is to distinctly partition the physical router into separate administrative domains. This partitioning enables multiple providers to administer the router simultaneously, with each provider having access only to the portions of the configuration relevant to their logical system. Junos OS supports up to 15 named

logical systems in addition to the default logical system (that is, **inet.0**). Unless otherwise specified in configuration, all interfaces belong to the default logical system.



NOTE: This Junos OS release supports the use of only the default logical system. Partitioning currently occurs through the use of separate routing instances.

A logical system can have one or more routing instances. Typically used in Layer 3 VPN scenarios, a routing instance does not have the same level of administrative separation as a logical system because it does not offer administrative isolation. However, the routing instance defines a distinct routing table, set of routing policies, and set of interfaces.

Related Documentation

- [Broadband Subscriber Management DHCPv4 Layer 3 Wholesale Topology and Configuration Elements on page 9](#)
- [Broadband Subscriber Management PPPoE Layer 3 Wholesale Topology and Configuration Elements on page 57](#)
- [Broadband Subscriber Management Layer 2 Wholesale Topology and Configuration Elements on page 75](#)

Wholesale Network Configuration Options and Considerations

You can configure a wholesale network any number of ways using Juniper Networks hardware and Junos OS software. For information about subscriber management hardware support, see the *Junos OS Broadband Subscriber Management and Services Library*. The general configuration options, and considerations for each, are provided in the following table:

Wholesale Configuration Options	Considerations
Fully Static (all interfaces, VLANs, and routing instances are configured statically)	Providing more control over retailer space and access, this option is more labor intensive and can require more detailed planning of the network, address allocation, and so on.
Static VLANs and Dynamic Demux Interfaces	Service VLANs are created statically and must be managed. Demux interfaces are dynamically created over the service VLANs. This option uses more logical interfaces; one for each VLAN and one for each dynamic demux interface that runs over each VLAN.
Dynamic VLANs Only (dedicated customer VLANs for each subscriber)	Dynamic (auto-sensed) VLANs are authenticated and installed in the correct non-default routing instance before DHCP is instantiated. This method helps to conserve logical interfaces by avoiding the need for additional logical interfaces being created for each demux interface. NOTE: In a customer VLAN model, each VLAN functions on a 1:1 basis for each customer (in this case, per household).

Wholesale Configuration Options	Considerations
Dynamic VLANs and Dynamic Demux Interfaces	Allows for the greatest ease of use and flexibility in configuring subscribers, by enabling access over a service VLAN and targetting more service levels over individual, dynamically-created demux interfaces over the service VLAN. This option uses more logical interfaces; one for each VLAN and one for each demux interface that runs over each VLAN.

DHCP Layer 3 Wholesale Configuration Interface Support

DHCP Layer 3 wholesale currently supports only the use of IP demux interfaces.

For general additional information about configuring IP demux interfaces, see the *Junos OS Network Interfaces Library for Routing Devices*.

Related Documentation

- *Junos OS Network Interfaces Library for Routing Devices*
- *Subscriber Interfaces and Demultiplexing Overview* in the *Junos OS Broadband Subscriber Management and Services Library*.
- *Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles* in the *Junos OS Broadband Subscriber Management and Services Library*.
- *Configuring a Subscriber Interface Using a Set of Static IP Demux Interfaces* in the *Junos OS Broadband Subscriber Management and Services Library*.

Layer 3 Wholesale Configuration DHCP Support

DHCP Layer 3 wholesale supports the following DHCP configuration options:

- DHCP Relay
- DHCP Relay Proxy
- DHCP Local Server



NOTE: All routing instances within the same wholesale network must use the same DHCP configuration option.

For additional information about any of these DHCP options, see the *AAA Service Framework Overview* in the *Junos OS Broadband Subscriber Management and Services Library*.

Related Documentation

- *Extended DHCP Relay Agent Overview* in the *Junos OS Broadband Subscriber Management and Services Library*.
- *DHCP Relay Proxy Overview* in the *Junos OS Broadband Subscriber Management and Services Library*.

- *Extended DHCP Local Server Overview* in the *Junos OS Broadband Subscriber Management and Services Library*.

Subscriber to Logical System and Routing Instance Relationship

As subscriber sessions are established, subscriber to logical system/routing instance memberships are established by the AAA framework configured for the default logical system. When configuring Layer 3 wholesaling, you typically configure global (wholesale) information within the default (master) logical system and default routing instance. Incoming subscribers must then be authenticated, but this authentication can be handled in one of two ways:

- Single (wholesaler only) authentication—Incoming subscribers are authenticated by the wholesaler RADIUS server. After authentication, the subscribers are assigned values specified by dynamic profiles (routing instances, interfaces, and any configuration values) specific to a particular retailer.
- Dual (wholesaler and retailer) authentication—Sometimes referred to as *double-dip authentication*. Incoming subscribers are initially authenticated by RADIUS using the wholesale configuration. Authenticated subscribers are then redirected to other routing instances associated with individual retailer network space. When you redirect subscribers, and those subscribers are to be authenticated by AAA servers owned by individual retailers, the subscribers must be authenticated again by the AAA servers before they are provided an address and any dynamic profile values are assigned. After reauthentication, however, the subscribers are managed normally using any values specific to the retailer routing instance to which they are assigned.

Related Documentation

- See *Routing Instances Overview* in the *Junos OS Routing Protocols Library*.

RADIUS VSAs and Broadband Subscriber Management Wholesale Configuration Overview

You can use RADIUS to assign various values through the use of dynamic variables within dynamic profiles. However, the configuration of at least one of the two VSAs described in [Table 3 on page 6](#) is required for a wholesale network to function.

Table 3: Required Juniper Networks VSAs for the Broadband Subscriber Management Wholesale Network Solution

Attribute Number	Attribute Name	Description	Value
26-1	LSRI-Name	Client logical system/routing instance membership name. Allowed only from RADIUS server for "default" logical system/routing instance membership.	string: logical system:routing instance

Table 3: Required Juniper Networks VSAs for the Broadband Subscriber Management Wholesale Network Solution (*continued*)

Attribute Number	Attribute Name	Description	Value
26-25	Redirect-LSRI-Name	Client logical system/routing instance membership name indicating to which logical system/routing instance membership the request is redirected for user authentication.	string: logical system:routing instance

Specifying the **\$junos-routing-instance** dynamic variable in a dynamic profile triggers a RADIUS access-accept response of either the LSRI-Name VSA or the Redirect-LSRI-Name VSA. Returning an LSRI-Name attribute in the access-accept response provides the logical system and routing instance in which the logical interface is to be created and the router updates the session database with the specified routing instance value. Returning a Redirect-LSRI-Name attribute in the access-accept response results in the router immediately sending a second access-request message (sometimes referred to as a *double-dip*) to the RADIUS server specified by the logical system:routing instance attribute specified by the Redirect-LSRI-Name VSA.



NOTE: Attributes returned as a result of a second access-request message to the logical system/routing instance membership specified by the Redirect-LSRI-Name VSA override any prior attributes returned by initial access-accept responses to the default logical system/routing instance membership.

- Related Documentation**
- [Juniper Networks VSAs Supported by the AAA Service Framework on page 143](#) in the *Junos OS Broadband Subscriber Management and Services Library*.

CHAPTER 2

Configuring DHCPv4 Layer 3 Wholesale Networks

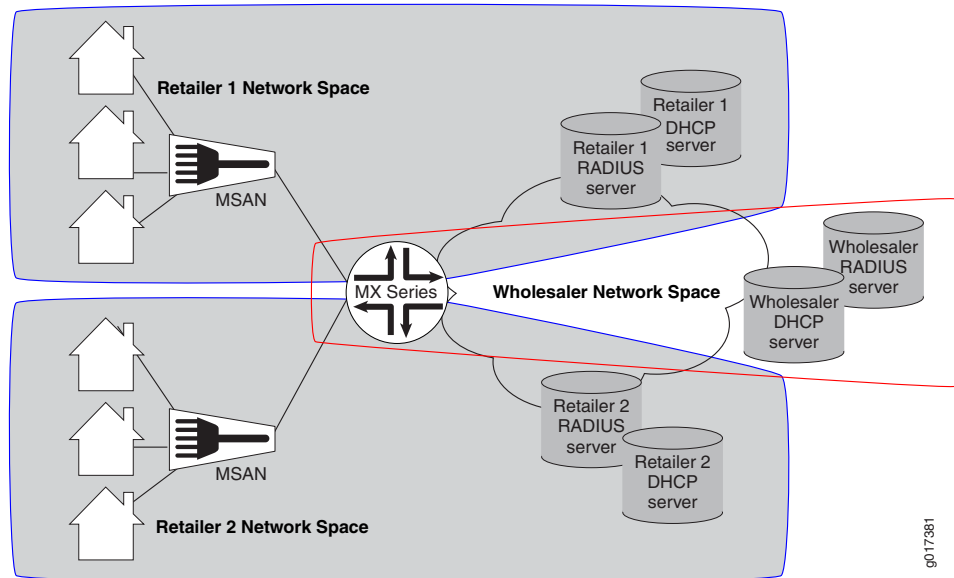
- [Broadband Subscriber Management DHCPv4 Layer 3 Wholesale Topology and Configuration Elements on page 9](#)
- [DHCPv4 Layer 3 Wholesale Network Topology Overview on page 10](#)
- [Configuring Loopback Interfaces for the DHCPv4 Layer 3 Wholesale Solution on page 11](#)
- [Configuring VLANs for the DHCPv4 Layer 3 Wholesale Network Solution on page 13](#)
- [Configuring Access Components for the DHCP Layer 3 Wholesale Network Solution on page 16](#)
- [Configuring Dynamic Profiles for the DHCPv4 Layer 3 Wholesale Network Solution on page 18](#)
- [Configuring Separate Routing Instances for DHCPv4 Service Retailers on page 21](#)
- [Configure Default Forwarding Options for the DHCPv4 Wholesale Network Solution on page 23](#)
- [Example: Wholesaler Dynamic Profile for a DHCPv4 Wholesale Network on page 26](#)
- [Example: Retailer Dynamic Profile for a DHCPv4 Wholesale Network on page 26](#)
- [Example: Default Forwarding Options Configuration for the DHCPv4 Wholesale Network on page 27](#)
- [Example: Retailer Routing Instances for a DHCPv4 Wholesale Network on page 28](#)

Broadband Subscriber Management DHCPv4 Layer 3 Wholesale Topology and Configuration Elements

The network topology for the subscriber management DHCPv4 Layer 3 wholesale solution includes configuring separate routing instances for individual retailers that use a portion of the router. This solution uses a DHCPv4 relay configuration. However, you can also implement DHCPv4 Relay Proxy or DHCPv4 Local Server configuration.

To explain the concept, but to limit complexity, this solution provides a configuration with one wholesaler and only two retailers. [Figure 1 on page 10](#) illustrates a basic Layer 3 wholesale topology model from which you can expand.

Figure 1: Basic Subscriber Management Layer 3 Wholesale Solution Topology



A DHCP Layer 3 wholesale network solution can use various combinations of the following configuration elements:

- Subscriber network VLAN configuration
- DHCPv4 configuration (DHCPv4 Relay, DHCPv4 Relay Proxy, or DHCPv4 Local Server)
- Addressing server or addressing server access configuration (if not using DHCPv4 Local Server)
- RADIUS server access configuration
- Dynamic profile configuration for default (wholesaler) access
- Dynamic profile configuration for retailer access (following subscriber redirection, if applicable)
- Routing instance configuration for individual retailers
- Group configuration and forwarding options for the network
- Core network configuration

Related Documentation

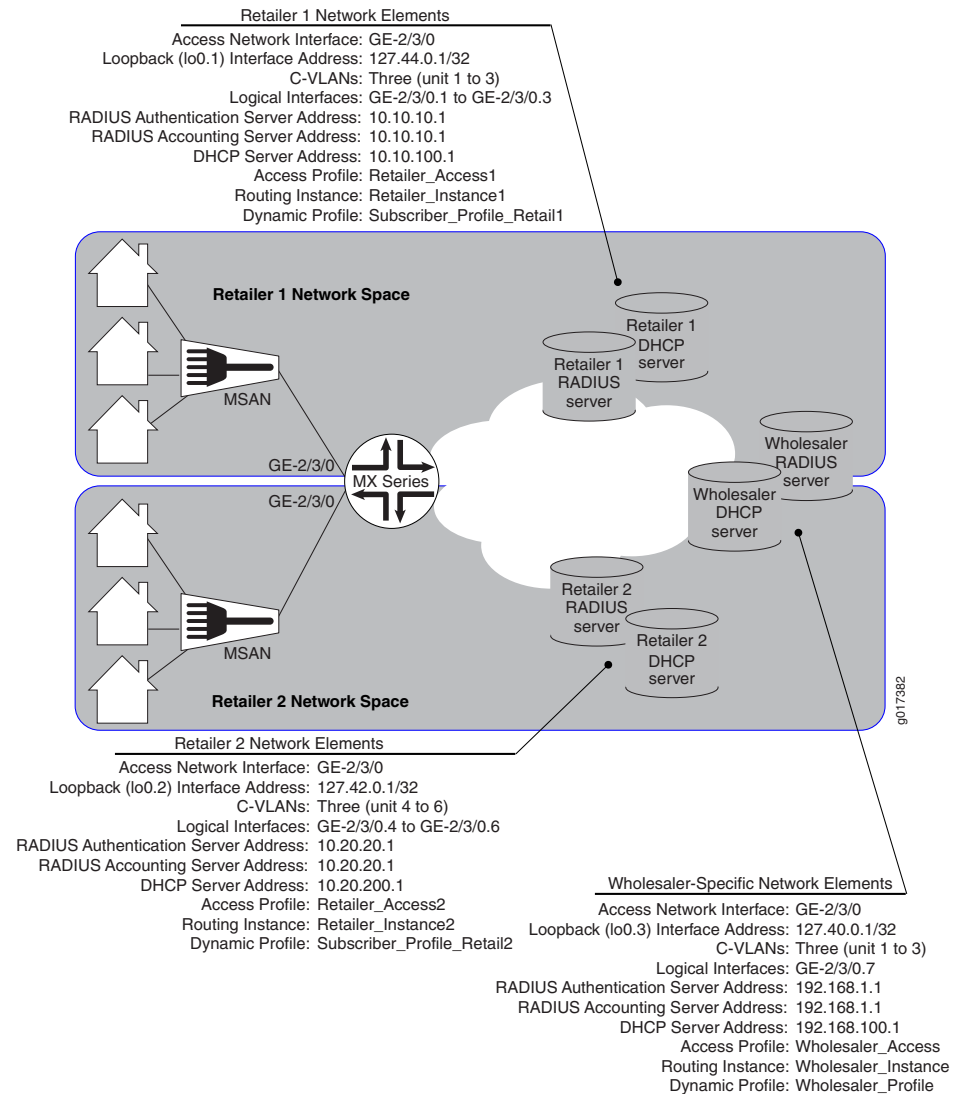
- [Layer 2 and Layer 3 Wholesale Overview on page 3](#)
- [DHCPv4 Layer 3 Wholesale Network Topology Overview on page 10](#)

DHCPv4 Layer 3 Wholesale Network Topology Overview

This configuration explains how to configure a simple DHCPv4 Layer 3 wholesale subscriber access network. This solution incorporates two retailers sharing resources on

a wholesaler router. [Figure 2 on page 11](#) provides the reference topology for this configuration example.

Figure 2: DHCPv4 Layer 3 Wholesale Network Reference Topology



- Related Documentation**
- [Layer 2 and Layer 3 Wholesale Overview on page 3](#)
 - [Broadband Subscriber Management DHCPv4 Layer 3 Wholesale Topology and Configuration Elements on page 9](#)

Configuring Loopback Interfaces for the DHCPv4 Layer 3 Wholesale Solution

You must configure loopback interfaces for use in the subscriber management access network. The loopback interfaces are automatically used for unnumbered interfaces.

To configure loopback interfaces:

1. Edit the loopback interface.

```
[edit]  
user@host# edit interfaces lo0
```

2. Edit the unit for the wholesale loopback interface.

```
[edit interfaces lo0]  
user@host# edit unit 3
```

3. Edit the loopback interface family that belongs to the wholesaler.

```
[edit interfaces lo0 unit 3]  
user@host# edit family inet
```

4. Specify the loopback interface address that belongs to the wholesaler.

```
[edit interfaces lo0 unit 3]  
user@host# set address 127.40.0.1/32
```

5. Edit the unit for a retail loopback interface to be assigned to the retailer.

```
[edit interfaces lo0]  
user@host# edit unit 1
```

6. Edit the loopback interface family that will be assigned to the retailer.

```
[edit interfaces lo0 unit 1]  
user@host# edit family inet
```

7. Specify the loopback interface address that will be assigned to the retailer.

```
[edit interfaces lo0 unit 1]  
user@host# set address 127.42.0.1/32
```

8. Repeat steps 5 through 7 for additional retailers, making sure to use unique unit and address values for each retailer loopback interface.

Related Documentation

- *Junos OS Network Interfaces Library for Routing Devices*

Configuring VLANs for the DHCPv4 Layer 3 Wholesale Network Solution

You can configure either static or dynamic customer VLANs for use in the DHCPv4 wholesale network solution.

- [Configuring Static Customer VLANs for the DHCPv4 Layer 3 Wholesale Network Solution on page 13](#)
- [Configuring Dynamic VLANs for the DHCPv4 Layer 3 Wholesale Network Solution on page 14](#)

Configuring Static Customer VLANs for the DHCPv4 Layer 3 Wholesale Network Solution

In this example configuration, the access interface (**ge-2/3/0**) connects to a device (that is, a DSLAM) on the access side of the network. You can define static VLANs for use by the access network subscribers.

To configure the static VLANs:

1. Edit the access side interface.

```
[edit]
user@host# edit interfaces ge-2/3/0
```

2. Specify the use of stacked VLAN tagging.

```
[edit interfaces ge-2/3/0]
user@host# set stacked-vlan-tagging
```

3. Edit the interface unit for the first VLAN.

```
[edit interfaces ge-2/3/0]
user@host# edit unit 1
```

4. Define the VLAN tags for the first VLAN.

```
[edit interfaces ge-2/3/0 unit 1]
user@host# set vlan-tags outer 3 inner 1
```

5. Specify that you want to create IPv4 demux interfaces.

```
[edit interfaces ge-2/3/0 unit 1]
user@host# set demux-source inet
```

6. Edit the family for the first VLAN.

```
[edit interfaces ge-2/3/0 unit 1]
user@host# edit family inet
```

7. (Optional) Define the unnumbered address and the preferred source address for the first VLAN.

```
[edit interfaces ge-2/3/0 unit 1 family inet]
user@host# set unnumbered-address lo0.1 preferred-source-address 127.44.0.1
```

8. Repeat steps 2 through 7 for additional VLAN interface units.

Configuring Dynamic VLANs for the DHCPv4 Layer 3 Wholesale Network Solution

To configure dynamic VLANs for the solution:

1. Configure a dynamic profile for dynamic VLAN creation.

- a. Name the profile.

```
[edit]
user@host# edit dynamic-profiles VLAN-PROF
```

- b. Define the **interfaces** statement with the internal **\$junos-interface-ifd-name** variable used by the router to match the interface name of the receiving interface.

```
[edit dynamic-profiles VLAN-PROF]
user@host# edit interfaces $junos-interface-ifd-name
```

- c. Define the **unit** statement with the predefined **\$junos-interface-unit** variable:

```
[edit dynamic-profiles VLAN-PROF interfaces "$junos-interface-ifd-name"]
user@host# edit unit $junos-interface-unit
```

- d. (Optional) To configure the router to respond to any ARP request, specify the **proxy-arp** statement.

```
[edit dynamic-profiles VLAN-PROF interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set proxy-arp
```

- e. Specify that you want to create IPv4 demux interfaces.

```
[edit dynamic-profiles VLAN-PROF interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set demux-source inet
```

- f. Specify the VLAN ID variable.

```
[edit dynamic-profiles VLAN-PROF interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set vlan-tags outer $junos-stacked-vlan-id
```

The variable is dynamically replaced with an outer VLAN ID within the VLAN range specified at the **[interfaces]** hierarchy level.

- g. Specify the inner VLAN ID variable.

```
[edit dynamic-profiles VLAN-PROF interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set vlan-tags inner $junos-vlan-id
```

The variable is dynamically replaced with an inner VLAN ID within the VLAN range specified at the **[interfaces]** hierarchy level.

- h. Access the family type.

```
[edit dynamic-profiles VLAN-PROF interfaces "$junos-interface-ifd-name" unit  
"$junos-interface-unit"]  
user@host# edit family inet
```

- i. (Optional) Enable IP and MAC address validation for dynamic IP demux interfaces in a dynamic profile.

```
[edit dynamic-profiles VLAN-PROF interfaces "$junos-interface-ifd-name" unit  
"$junos-interface-unit" family inet]  
user@host# set mac-validate strict
```

- j. (Optional) Specify the unnumbered address and preferred source address.

```
[edit dynamic-profiles VLAN-PROF interfaces "$junos-interface-ifd-name" unit  
"$junos-interface-unit" family inet]  
user@host# set unnumbered-address lo.0 preferred-source-address 127.33.0.1
```

2. Associate the dynamic profile with the interface on which the dynamic VLANs will be created.

- a. Access the interface that you want to use for creating VLANs.

```
[edit interfaces]  
user@host# edit interfaces ge-2/3/0
```

- b. Specify the use of stacked VLAN tagging.

```
[edit interfaces ge-2/3/0]  
user@host# set stacked-vlan-tagging
```

- c. Specify that you want to automatically configure VLAN interfaces.

```
[edit interfaces ge-2/3/0]  
user@host# edit auto-configure
```

- d. Specify that you want to configure stacked VLANs.

```
[edit interfaces ge-2/3/0 auto-configure]  
user@host# edit stacked-vlan-ranges
```

- e. Specify the dynamic VLAN profile that you want the interface to use.

```
[edit interfaces ge-2/3/0 auto-configure stacked-vlan-ranges]  
user@host# set dynamic-profile VLAN-PROF
```

- f. Repeat steps a through e for any other interfaces that you want to use for creating VLANs.

3. Specify the Ethernet packet type that the VLAN dynamic profile can accept.

```
[edit interfaces ge-2/3/0 auto-configure stacked-vlan-ranges dynamic-profile
VLAN-PROF]
user@host# set accept inet
```

4. Define VLAN ranges for use by the dynamic profile when dynamically creating VLAN IDs. For this solution, specify the outer and inner stacked VLAN ranges that you want the dynamic profile to use. The following example specifies an outer stacked VLAN ID range of 3–3 (enabling only the outer range of 3) and an inner stacked VLAN ID range of 1–3 (enabling a range from 1 through 3 for the inner stacked VLAN ID).

```
[edit interfaces ge-0/0/0 auto-configure stacked-vlan-ranges dynamic-profile
VLAN-PROF]
user@host# set stacked-vlan-ranges 3–3,1–3
```

Configuring Access Components for the DHCP Layer 3 Wholesale Network Solution

When configuring a wholesale network, you must configure several components globally. This configuration provides access to RADIUS servers that you want the wholesaler and any configured retailers to use globally. The access configuration includes the following general steps:

- [Configuring RADIUS Server Access on page 16](#)
- [Configuring a DHCP Wholesaler Access Profile on page 16](#)
- [Configuring DHCP Retailer Access Profiles on page 17](#)

Configuring RADIUS Server Access

You can globally define any RADIUS servers in your network that either the wholesale access profile or retailer access profile can use. After you define the global RADIUS servers, you can specify specific RADIUS servers within individual access profiles.

To define RADIUS servers for profile access:

1. Access the `[edit access radius-server]` hierarchy level.

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

2. Specify the address and secret for any RADIUS servers in the network.

```
[edit access radius-server]
user@host# set 192.168.10.1 secret $ABC123$ABC123$ABC123
user@host# set 10.10.10.1 secret $ABC123$ABC123
```

Configuring a DHCP Wholesaler Access Profile

You must define the network and interface over which you want subscribers to initially access the network with a wholesale access profile. When a subscriber attempts to access the network, the access profile provides initial access information including authentication and accounting values that the router uses for the accessing subscriber.

To define a wholesale access profile:

1. Create the wholesale access profile.

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

2. Specify the authentication methods for the profile and the order in which they are used.

```
[edit access profile Wholesaler1]
user@host# set authentication-order radius password
```

3. Specify that you want to configure RADIUS support.

```
[edit access profile Wholesaler1]
user@host# edit radius
```

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

```
[edit access profile Wholesaler1 radius]
user@host# set authentication-server 192.168.10.1
```

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

```
[edit access profile Wholesaler1 radius]
user@host# set accounting-server 192.168.10.1
```

6. Configure any desired options for the RADIUS server.

See Configuring RADIUS Server Options for Subscriber Access.

7. Configure subscriber accounting (RADIUS accounting).

See Configuring Per-Subscriber Session Accounting.

Configuring DHCP Retailer Access Profiles

In this solution, subscribers are redirected to a networking space used by a specific retailer and defined by a unique routing instance. This method requires that you define the network and interface over which you want subscribers to access the network after being redirected by the wholesale access profile.

To define a retailer access profile:

1. Create the retailer access profile.

```
[edit]
user@host# edit access-profile Retailer_Access1
```

2. Specify the authentication methods for the profile and the order in which they are used.

```
[edit access profile Retailer1]
user@host# set authentication-order radius password
```

3. Specify that you want to configure RADIUS support.

```
[edit access profile Retailer1]
user@host# edit radius
```

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

```
[edit access profile Retailer1 radius]
user@host# set authentication-server 10.10.10.1
```

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

```
[edit access profile Retailer1 radius]
user@host# set accounting-server 10.10.10.1
```

6. Configure any desired options for the RADIUS server.

See [Configuring RADIUS Server Options for Subscriber Access](#).

7. Configure subscriber accounting (RADIUS accounting).

See [Configuring Per-Subscriber Session Accounting](#).

Configuring Dynamic Profiles for the DHCPv4 Layer 3 Wholesale Network Solution

A dynamic profile is a set of characteristics, defined in a type of template, that you can use to provide services for broadband applications. These services are assigned dynamically to interfaces as they access the network. When configuring dynamic profiles for the DHCPv4 Layer 3 wholesale network, you can choose to configure one dynamic profile to address all incoming subscribers or you can configure individual dynamic profiles for use by the different network management groups (that is, the wholesaler and any retailers). In fact, you can create multiple dynamic profiles that you can use to roll out different services and selectively apply those dynamic profiles to different subscriber groups as necessary.

In this solution example, one dynamic profile is created for use by the wholesaler when subscribers initially access the network. Other dynamic profiles are created for the subscribers for each individual retailer to use after they are redirected to that retailer network space.

- [Configuring a Wholesale Dynamic Profile for use in the DHCPv4 Solution on page 18](#)
- [Configuring a Dynamic Profile for use by a Retailer in the DHCPv4 Solution on page 20](#)

Configuring a Wholesale Dynamic Profile for use in the DHCPv4 Solution

You can configure a basic access profile to initially manage subscribers that access the network.

To configure a dynamic profile for use by the wholesaler:

1. Create a wholesale dynamic profile.

```
[edit]
user@host# edit dynamic-profiles Wholesaler_Profile
```

2. Specify that you want to configure the **demux0** interface in the dynamic profile.

```
[edit dynamic-profiles Subscriber_Profile_Retail1]
user@host# edit interfaces demux0
```

3. Configure the unit for the **demux0** interface.

- a. Configure the variable for the unit number of the **demux0** interface.

The variable is dynamically replaced with the unit number that DHCP supplies when the subscriber logs in.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 demux0]
user@host# edit unit $junos-interface-unit
```

- b. Configure the variable for the underlying interface of the demux interfaces and specify the **\$junos-underlying-interface** variable.

The variable is dynamically replaced with the underlying interface that DHCP supplies when the subscriber logs in.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 interfaces demux0 unit
"$junos-interface-unit"]
user@host# set demux-options underlying-interface $junos-underlying-interface
```

4. Configure the family for the demux interfaces.

- a. Specify that you want to configure the family.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 interfaces demux0 unit
"$junos-interface-unit"]
user@host# edit family inet
```

- b. Configure the unnumbered address for the family.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 demux0 unit "$junos-interface-unit"
family inet6]
user@host# set unnumbered-address lo0.0
```

- c. Configure the variable for the IPv4 address of the demux interface.

The variable is dynamically replaced with the IPv4 address that DHCP supplies when the subscriber logs in.

```
[edit dynamic-profiles business-profile interfaces demux0 unit "$junos-interface-unit"]
user@host# set demux-source $junos-subscriber-ip-address
```

Configuring a Dynamic Profile for use by a Retailer in the DHCPv4 Solution

To configure a dynamic profile for use with retailer access:

1. Create a retail dynamic profile.

```
[edit]
user@host# edit dynamic-profiles Subscriber_Profile_Retail1
```

2. Define the dynamic routing instance variable in the dynamic profile.

```
[edit dynamic-profiles Subscriber_Profile_Retail1]
user@host# edit routing-instances $junos-routing-instance
```

3. Set the dynamic interface variable for the dynamic routing instance.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 routing-instances
"$junos-routing-instance"]
user@host# set interface $junos-interface-name
```

4. Specify that you want to configure the **demux0** interface in the dynamic profile.

```
[edit dynamic-profiles Subscriber_Profile_Retail1]
user@host# edit interfaces demux0
```

5. Configure the unit for the **demux0** interface.

- a. Configure the variable for the unit number of the **demux0** interface.

The variable is dynamically replaced with the unit number that DHCP supplies when the subscriber logs in.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 demux0]
user@host# edit unit $junos-interface-unit
```

- b. Configure the variable for the underlying interface of the demux interfaces and specify the **\$junos-underlying-interface** variable.

The variable is dynamically replaced with the underlying interface that DHCP supplies when the subscriber logs in.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 interfaces demux0 unit
"$junos-interface-unit"]
user@host# set demux-options underlying-interface $junos-underlying-interface
```

6. Configure the family for the demux interfaces.

- a. Specify that you want to configure the family.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 interfaces demux0 unit
"$junos-interface-unit"]
user@host# edit family inet
```

- b. Configure the unnumbered address for the family.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 demux0 unit "$junos-interface-unit"
family inet6]
user@host# set unnumbered-address lo0.0
```

- c. Configure the variable for the IPv6 address of the demux interface.

The variable is dynamically replaced with the IPv6 address that DHCP supplies when the subscriber logs in.

```
[edit dynamic-profiles business-profile interfaces demux0 unit "$junos-interface-unit"]
user@host# set demux-source $junos-subscriber-ip-address
```

Configuring Separate Routing Instances for DHCPv4 Service Retailers

As the owner of the system, the wholesaler typically uses the default routing instance. You must create separate routing instances for each individual retailer to keep routing information for individual retailers separate and to define any servers and forwarding options specific to each retailer.

To define a retailer routing instance:

1. Create the retailer routing instance.

```
[edit]
user@host# edit routing-instances RetailerInstance1
```

2. Specify the routing instance type for the retailer.

```
[edit routing-instances "RetailerInstance1"]
user@host# set instance-type vrf
```

3. Specify the access profile that you want the routing instance to use.

```
[edit routing-instances "RetailerInstance1"]
user@host# set access-profile Retailer1
```

4. Specify the interface that faces the Retailer1 RADIUS server.

```
[edit routing-instances "RetailerInstance1"]
user@host# set interface ge-11/1/9.10
```

5. Specify the interface that faces the Retailer1 DHCP server.

```
[edit routing-instances "RetailerInstance1"]
user@host# set interface ge-11/1/10.100
```

6. Specify the loopback interface unit for this routing instance.

```
[edit routing-instances "RetailerInstance1"]
user@host# set interface lo0.1
```



NOTE: Loopback interfaces must be unique for each routing instance.

7. Access the DHCP Relay forwarding options hierarchy for the routing instance.

```
[edit routing-instances "RetailerInstance1"]
user@host# edit forwarding-options dhcp-relay
```



NOTE: The configuration for this wholesale solution uses DHCP Relay. However, you can also configure DHCP Proxy Relay or DHCP Local Server for the DHCP Layer 3 wholesale network.

8. Specify that you want to configure authentication options and use external AAA authentication services.

```
[edit routing-instances "RetailerInstance1" forwarding-options dhcp-relay]
user@host# edit authentication
```

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

See *Configuring Passwords for Usernames*.

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

See *Creating Unique Usernames for DHCP Clients*.

11. Specify the default dynamic profile that you want to attach to DHCP subscriber for this retailer.

```
[edit routing-instances "RetailerInstance1" forwarding-options dhcp-relay]
user@host# set dynamic-profile Subscriber_Profile_Retail1
```

12. Specify any overrides for the default DHCP Relay configuration.

See *Overriding the Default DHCP Relay Configuration Settings*.

13. Configure a named server group for the retailer.

```
[edit routing-instances "RetailerInstance1" forwarding-options dhcp-relay]
user@host# edit server-group Retailer1_Group
```

14. Specify the DHCP server address for the retailer group.

```
[edit routing-instances "RetailerInstance1" forwarding-options dhcp-relay server-group
"Retailer1_Group"]
user@host# set 10.10.100.1
```

15. Specify the retailer group as the active server group for this routing instance.

```
[edit routing-instances "RetailerInstance1" forwarding-options dhcp-relay]
user@host# set active-server-group Retailer1_Group
```

16. Configure a group you can use to define the retailer dynamic profile and DHCP access interface.

```
[edit routing-instances "RetailerInstance1" forwarding-options dhcp-relay]
user@host# edit group Retailer1_Group
```

17. Specify the dynamic profile that the retailer DHCP subscribers use.

```
[edit routing-instances "RetailerInstance1" forwarding-options dhcp-relay group
 "Retailer1_Group"]
user@host# set dynamic-profile Subscriber_Profile_Retailer1
```

18. Specify the retailer interface that the retailer DHCP subscribers use.

```
[edit routing-instances "RetailerInstance1" forwarding-options dhcp-relay group
 "Retailer1_Group"]
user@host# set interface ge-2/3/0.2
```

19. (Optional) Configure any passwords that authenticate the username to the external authentication service for the retailer groups that you created.

See [Configuring Passwords for Usernames](#).

20. (Optional) Configure any unique username values for the retailer groups that you created.

See [Creating Unique Usernames for DHCP Clients](#).

21. (Optional) Specify any overrides for any of the DHCP Relay group configurations that you created.

See [Overriding the Default DHCP Relay Configuration Settings](#).

22. Repeat this procedure for other retailers.

Related Documentation

[Configure Default Forwarding Options for the DHCPv4 Wholesale Network Solution](#)

You can use DHCP Relay, DHCP Relay Proxy, or DHCP Local Server configuration in a DHCP wholesale network. DHCP configuration is defined at the **[edit forwarding-options]** hierarchy level.



NOTE: The configuration for this wholesale solution uses DHCP Relay.

To configure DHCPv4 Relay forwarding options:

1. Access the **[edit forwarding-options dhcp-relay]** hierarchy.

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

2. Specify that you want to configure authentication options and use external AAA authentication services.

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

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

See Configuring Passwords for Usernames.

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

See Creating Unique Usernames for DHCP Clients.

5. Specify the default dynamic profile that you want to attach to all DHCP subscriber that access the router.

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

6. Specify any overrides for the default DHCP Relay configuration.

See Overriding the Default DHCP Relay Configuration Settings.

7. Configure a named server group for default (wholesaler) DHCP server access.

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

8. Specify the DHCP server address for the default (wholesale) group.

```
[edit forwarding-options dhcp-relay server-group "Wholesaler_Group"]
user@host# set 192.168.100.1
```

9. Specify the default (wholesale) group as the active server group.

```
[edit forwarding-options dhcp-relay]
user@host# set active-server-group Wholesaler_Group
```

10. Configure a group you can use to define the wholesale DHCP access interface.

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

11. Specify the default (wholesale) interface that all DHCP subscribers use when first accessing the router.

```
[edit forwarding-options dhcp-relay group "Wholesaler_Group"]
user@host# set interface ge-2/3/0.1
```

12. Configure a group you can use to define a retail DHCP interface.

```
[edit forwarding-options dhcp-relay]
user@host# edit group Retailer1_Group
```

13. Specify the logical interface the DHCP subscribers use once redirected.

```
[edit forwarding-options dhcp-relay group "Retailer1_Group"]
user@host# set interface ge-2/3/0.2
```

14. Repeat steps 12 and 13 for other retailer groups.

In this solution example, you configure another group name of "Retailer2_Group" and specify **ge-2/3/0.3** for the logical interface.

15. (Optional) Configure any passwords that authenticate the username to the external authentication service for any of the groups that you created.

See *Configuring Passwords for Usernames*.

16. (Optional) Configure optional features to create a unique username for any of the groups that you created.

See *Creating Unique Usernames for DHCP Clients*.

17. (Optional) Specify any overrides for any of the DHCP Relay group configurations that you created.

See *Overriding the Default DHCP Relay Configuration Settings*.

Related Documentation

- *Extended DHCP Relay Agent Overview*
- *DHCP Relay Proxy Overview*
- *Configuring Passwords for Usernames*
- *Creating Unique Usernames for DHCP Clients*
- *Overriding the Default DHCP Relay Configuration Settings*

Example: Wholesaler Dynamic Profile for a DHCPv4 Wholesale Network

This example specifies a dynamic profile name of *Wholesaler_Profile*, uses dynamic IP demux interfaces, and references the predefined input firewall filter.

```
dynamic-profiles {
  Wholesaler_Profile {
    interfaces {
      demux0 {
        unit "$junos-interface-unit" {
          demux-options {
            underlying-interface "$junos-underlying-interface";
          }
          family inet {
            demux-source {
              $junos-subscriber-ip-address;
            }
          }
          filter {
            input "$junos-input-filter";
          }
          unnumbered-address "$junos-loopback-interface" preferred-source-address
            $junos-preferred-source-address;
        }
      }
    }
  }
}
```

Related Documentation

- [Configuring Dynamic Profiles for the DHCPv4 Layer 3 Wholesale Network Solution on page 18](#)

Example: Retailer Dynamic Profile for a DHCPv4 Wholesale Network

```
dynamic-profiles {
  Subscriber_Profile_Retailer1 {
    routing-instances {
      "$junos-routing-instance" {
        interface "$junos-interface-name";
      }
    }
    interfaces {
      demux0 {
        unit "$junos-interface-unit" {
          demux-options {
            underlying-interface "$junos-underlying-interface";
          }
          family inet {
            demux-source {
              "$junos-subscriber-ip-address";
            }
          }
          unnumbered-address "$junos-loopback-interface" preferred-source-address
            "$junos-preferred-source-address";
        }
      }
    }
  }
}
```



```

    }
  }
}

```

Related Documentation • [Configuring Dynamic Profiles for the DHCPv4 Layer 3 Wholesale Network Solution on page 18](#)

Example: Default Forwarding Options Configuration for the DHCPv4 Wholesale Network

```

forwarding-options {
  dhcp-relay {
    traceoptions {
      file size 1g;
      inactive: flag all;
    }
    authentication {
      password $ABC123;
      username-include {
        user-prefix WholesaleNetwork;
      }
    }
  }
  dynamic-profile Wholesaler_Profile;
  overrides {
    always-write-giaddr;
    always-write-option-82;
    layer2-unicast-replies;
    trust-option-82;
    client-discover-match;
  }
  server-group {
    Wholesaler-Server-Group {
      192.168.100.1;
    }
  }
  active-server-group Wholesaler-Server Group;
  group Wholesaler-Group {
    authentication {
      password $ABC123;
      username-include {
        user-prefix WholesaleNetwork;
      }
    }
  }
  interface ge-2/3/0.1;
}
group Retailer1-Group {
  authentication {
    password $ABC123$ABC123;
    username-include {
      user-prefix WholesaleNetwork_Retailer1;
    }
  }
  interface ge-2/3/0.2;
}

```

```
}
group Retailer2-Group {
  authentication {
    password $ABC123$ABC123$ABC123;
    username-include {
      user-prefix WholesaleNetwork_Retailer1;
    }
  }
  interface ge-2/3/0.3;
}
}
```

Related Documentation

- [Configure Default Forwarding Options for the DHCPv4 Wholesale Network Solution on page 23](#)

Example: Retailer Routing Instances for a DHCPv4 Wholesale Network

```
routing-instances {
  Retailer_Instance1 {
    instance-type vrf;
    access-profile Retailer_Access1;
    interface ge-11/1/9.10;
    interface ge-11/1/10.100;
    interface lo0.1;
    route-distinguisher 1:1;
    forwarding-options {
      dhcp-relay {
        authentication {
          password $ABC123$ABC123;
          username-include {
            user-prefix WholesaleNetwork_Retailer1;
          }
        }
      }
      dynamic-profile Subscriber_Profile_Retailer1;
      overrides {
        always-write-giaddr;
        always-write-option-82;
        layer2-unicast-replies;
        trust-option-82;
        client-discover-match;
      }
      server-group {
        Retailer1-Server-Group {
          10.10.100.1;
        }
      }
      active-server-group Retailer1-Server-Group;
      group Retailer1-Group {
        authentication {
          password $ABC123$ABC123;
          username-include {
            user-prefix WholesaleNetwork_Retailer1;
          }
        }
      }
    }
  }
}
```

```

    }
    dynamic-profile Subscriber_Profile_Retailer1;
    overrides {
        always-write-giaddr;
        trust-option-82;
        client-discover-match;
    }
    interface ge-2/3/0.2;
}
}
}
}
Retailer_Instance2 {
    instance-type vrf;
    access-profile Retailer_Access2;
    interface ge-7/1/9.10;
    interface ge-7/1/9.100;
    interface lo0.2;
    route-distinguisher 2:2;
    forwarding-options {
        dhcp-relay {
            authentication {
                password $ABC123$ABC123$ABC123;
                username-include {
                    user-prefix WholesaleNetwork_Retailer2;
                }
            }
        }
        dynamic-profile Subscriber_Profile_Retailer2;
        overrides {
            always-write-giaddr;
            trust-option-82;
            client-discover-match;
        }
        server-group {
            Retailer2-Group {
                10.20.200.1;
            }
        }
        active-server-group Retailer2-Group;
        group Retailer2-Group {
            authentication {
                password $ABC123$ABC123$ABC123;
                username-include {
                    user-prefix psswd2;
                }
            }
        }
        dynamic-profile Subscriber_Profile_Retailer2;
        overrides {
            always-write-giaddr;
            trust-option-82;
            client-discover-match;
        }
        interface ge-2/3/0.3;
    }
}
}
}

```

```
}  
}
```

Related Documentation • [Configuring Separate Routing Instances for DHCPv4 Service Retailers on page 21](#)

CHAPTER 3

Configuring DHCPv6 Layer 3 Wholesale Networks

- Broadband Subscriber Management DHCPv6 Layer 3 Wholesale Topology and Configuration Elements on page 31
- DHCPv6 Layer 3 Wholesale Network Topology Overview on page 33
- Configuring Loopback Interfaces for the DHCPv6 Layer 3 Wholesale Solution on page 34
- Configuring VLANs for the DHCPv6 Layer 3 Wholesale Network Solution on page 34
- Configuring Access Components for the DHCP Layer 3 Wholesale Network Solution on page 37
- Configuring Dynamic Profiles for the DHCPv6 Layer 3 Wholesale Network Solution on page 40
- Configuring Separate Routing Instances for DHCPv6 Service Retailers on page 42
- Configuring Address Server Elements for the DHCPv6 Layer 3 Wholesale Solution on page 43
- Example: Retailer Dynamic Profile for a DHCPv6 Wholesale Network on page 46
- Example: Retailer Routing Instances for a DHCPv6 Wholesale Network on page 47
- Example: DHCPv6 Address Assignment Pool That Provides Full 128-bit IPV6 Addresses for a DHCPv6 Wholesale Network on page 47
- Example: DHCPv6 Address Assignment Pool That Provides 74-bit IPV6 Prefixes for a DHCPv6 Wholesale Network on page 48
- Example: Extended DHCPv6 Local Server for a DHCPv6 Wholesale Network on page 48

Broadband Subscriber Management DHCPv6 Layer 3 Wholesale Topology and Configuration Elements

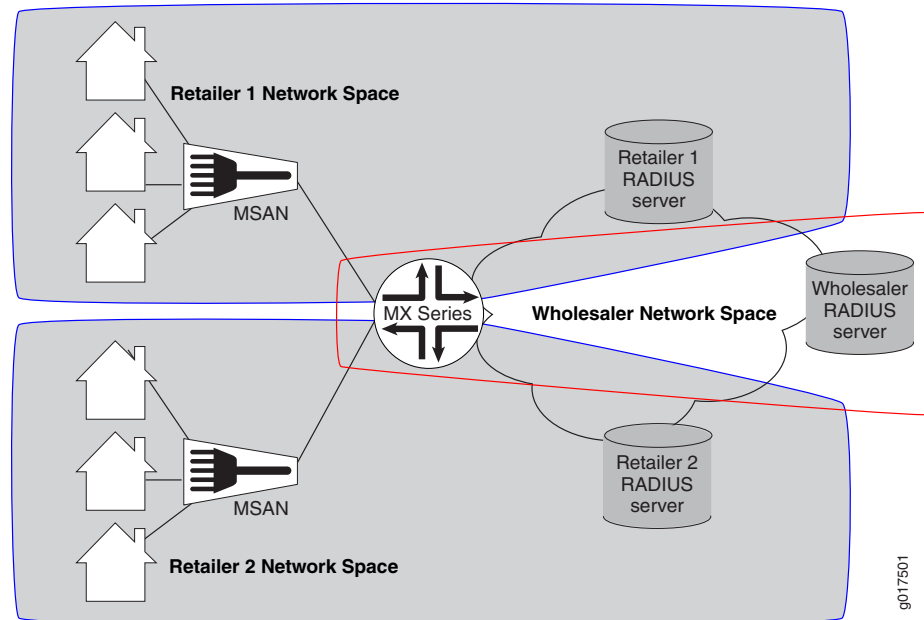
The network topology for the subscriber management DHCPv6 Layer 3 wholesale solution includes configuring separate routing instances for individual retailers that use a portion of the router. This solution uses a DHCPv6 local server configuration.



NOTE: Only DHCPv6 local server is currently supported for DHCPv6 Layer 3 wholesale configuration.

To explain the concept, but to limit complexity, this solution provides a configuration with one wholesaler and only two retailers. [Figure 3 on page 32](#) illustrates a basic Layer 3 wholesale topology model from which you can expand.

Figure 3: Basic Subscriber Management DHCPv6 Layer 3 Wholesale Solution Topology



A DHCPv6 Layer 3 wholesale network solution can use various combinations of the following configuration elements:

- Subscriber network VLAN configuration
- DHCPv6 configuration (local server only)
- RADIUS server access configuration
- Dynamic profile configuration for default (wholesaler) access
- Dynamic profile configuration for retailer access (following subscriber redirection, if applicable)
- Routing instance configuration for individual retailers
- Group configuration and forwarding options for the network
- Core network configuration

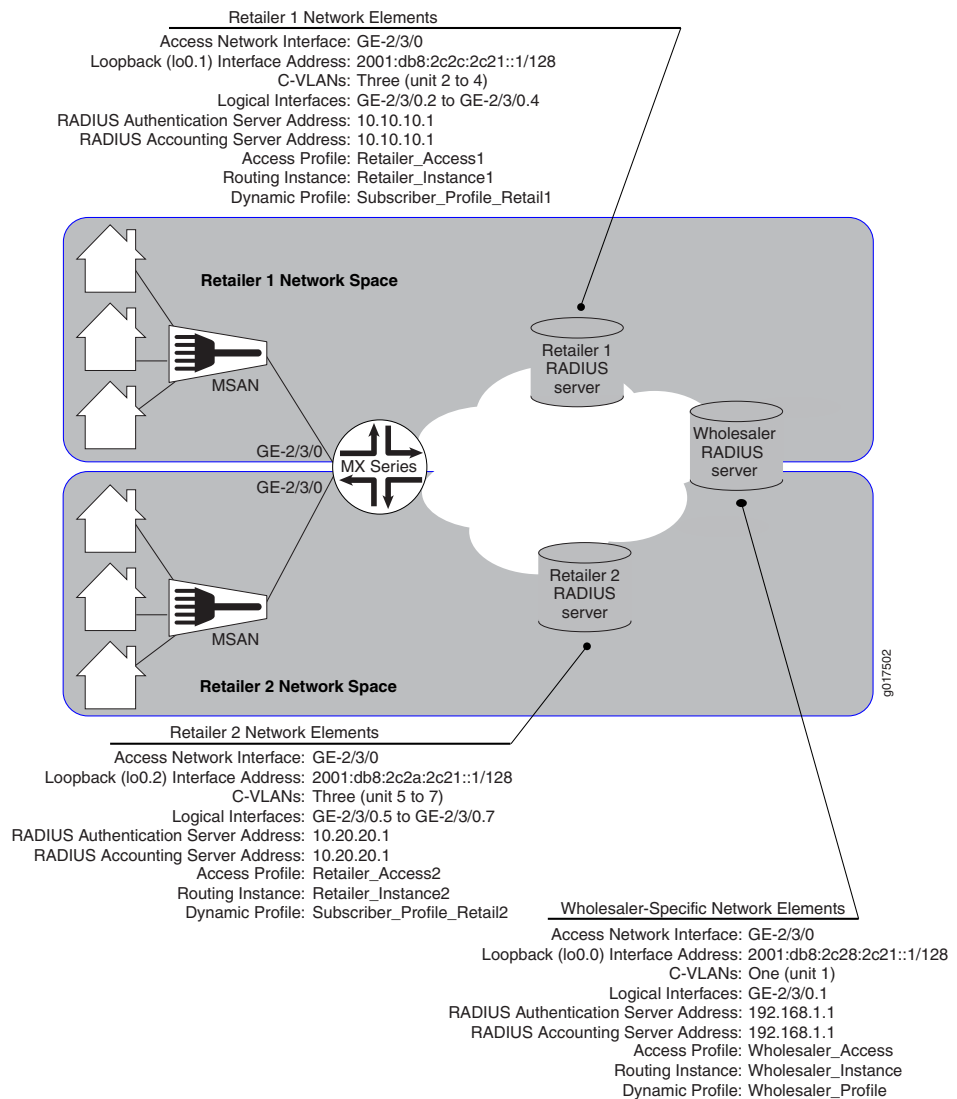
Related Documentation

- [Layer 2 and Layer 3 Wholesale Overview on page 3](#)
- [DHCPv6 Layer 3 Wholesale Network Topology Overview on page 33](#)

DHCPv6 Layer 3 Wholesale Network Topology Overview

This configuration explains how to configure a simple DHCPv6 Layer 3 wholesale subscriber access network. This solution incorporates two retailers sharing resources on a wholesaler router. [Figure 4 on page 33](#) provides the reference topology for this configuration example.

Figure 4: DHCPv6 Layer 3 Wholesale Network Reference Topology



Related Documentation • [Layer 2 and Layer 3 Wholesale Overview on page 3](#)

- [Broadband Subscriber Management DHCPv4 Layer 3 Wholesale Topology and Configuration Elements on page 9](#)

Configuring Loopback Interfaces for the DHCPv6 Layer 3 Wholesale Solution

You must configure loopback interfaces for use in the subscriber management access network. The loopback interfaces are automatically used for unnumbered interfaces.

To configure loopback interfaces:

1. Edit the loopback interface.

```
[edit]
user@host# edit interfaces lo0
```

2. Edit the unit for the loopback interface that you want to use for the wholesaler.

```
[edit interfaces lo0]
user@host# edit unit 0
```

3. Edit the loopback interface family that belongs to the wholesaler.

```
[edit interfaces lo0 unit 0]
user@host# edit family inet6
```

4. Specify the wholesale loopback interface address.

```
[edit interfaces lo0 unit 0]
user@host# set address 2001:db8:2c28:2c21::1/128
```

5. Edit the unit for a retail loopback interface.

```
[edit interfaces lo0]
user@host# edit unit 1
```

6. Edit the retail loopback interface family.

```
[edit interfaces lo0 unit 1]
user@host# edit family inet6
```

7. Specify the retail loopback interface address.

```
[edit interfaces lo0 unit 1]
user@host# set address 2001:db8:2c2c:2c21::1/128
```

8. Repeat steps 5 through 7 for additional retailers, making sure to use unique unit and address values for each retailer loopback interface.

Configuring VLANs for the DHCPv6 Layer 3 Wholesale Network Solution

You can configure either static or dynamic customer VLANs for use in the DHCPv6 wholesale network solution.

- [Configuring Static Customer VLANs for the DHCPv6 Layer 3 Wholesale Network Solution on page 35](#)
- [Configuring Dynamic Customer VLANs for the DHCPv6 Layer 3 Wholesale Network Solution on page 35](#)

Configuring Static Customer VLANs for the DHCPv6 Layer 3 Wholesale Network Solution

In this example configuration, the access interface (**ge-2/3/0**) connects to a device (that is, a DSLAM) on the access side of the network. You can define static VLANs for use by access network subscribers.

To configure the static VLANs:

1. Edit the access side interface.

```
[edit]
user@host# edit interfaces ge-2/3/0
```

2. Specify the use of stacked VLAN tagging.

```
[edit interfaces ge-2/3/0]
user@host# set stacked-vlan-tagging
```

3. Edit the interface unit for the first VLAN.

```
[edit interfaces ge-2/3/0]
user@host# edit unit 1
```

4. Define the VLAN tags for the first VLAN.

```
[edit interfaces ge-2/3/0 unit 1]
user@host# set vlan-tags outer 3 inner 1
```

5. Specify that you want to create IPv6 demux interfaces.

```
[edit interfaces ge-2/3/0 unit 1]
user@host# set demux-source inet6
```

6. Edit the family for the first VLAN.

```
[edit interfaces ge-2/3/0 unit 1]
user@host# edit family inet6
```

7. (Optional) Define the unnumbered address and the preferred source address for the first VLAN.

```
[edit interfaces ge-2/3/0 unit 1 family inet6]
user@host# set unnumbered-address lo0.1 preferred-source-address
2001:db8:2c28:2c21::1/128
```

8. Repeat steps 2 through 7 for additional VLAN interface units.

Configuring Dynamic Customer VLANs for the DHCPv6 Layer 3 Wholesale Network Solution

To configure dynamic VLANs for the solution:

1. Configure a dynamic profile for dynamic VLAN creation.

- a. Name the profile.

```
[edit]
user@host# edit dynamic-profiles VLAN-PROF
```

- b. Define the **interfaces** statement with the internal **\$junos-interface-ifd-name** variable used by the router to match the interface name of the receiving interface.

```
[edit dynamic-profiles VLAN-PROF]
user@host# edit interfaces $junos-interface-ifd-name
```

- c. Define the **unit** statement with the predefined **\$junos-interface-unit** variable:

```
[edit dynamic-profiles VLAN-PROF interfaces "$junos-interface-ifd-name"]
user@host# edit unit $junos-interface-unit
```

- d. Specify that you want to create IPv6 demux interfaces.

```
[edit dynamic-profiles VLAN-PROF interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set demux-source inet6
```

- e. Specify the VLAN ID variable.

```
[edit dynamic-profiles VLAN-PROF interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set vlan-tags outer $junos-stacked-vlan-id
```

The variable is dynamically replaced with an outer VLAN ID within the VLAN range specified at the **[interfaces]** hierarchy level.

- f. Specify the inner VLAN ID variable.

```
[edit dynamic-profiles VLAN-PROF interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# set vlan-tags inner $junos-vlan-id
```

The variable is dynamically replaced with an inner VLAN ID within the VLAN range specified at the **[interfaces]** hierarchy level.

- g. Access the family type.

```
[edit dynamic-profiles VLAN-PROF interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit"]
user@host# edit family inet6
```

- h. (Optional) Specify the unnumbered address and preferred source address.

```
[edit dynamic-profiles VLAN-PROF interfaces "$junos-interface-ifd-name" unit
"$junos-interface-unit" family inet6]
user@host# set unnumbered-address lo.0 preferred-source-address
2001:db8:2c28:2c21::1/128
```

2. Associate the dynamic profile with the interface on which you want the VLANs created.

- a. Access the interface that you want to use for creating VLANs.

```
[edit interfaces]
user@host# edit interfaces ge-2/3/0
```

- b. Specify the use of stacked VLAN tagging.

```
[edit interfaces ge-2/3/0]
user@host# set stacked-vlan-tagging
```

- c. Specify that you want to automatically configure VLAN interfaces.

```
[edit interfaces ge-2/3/0]
user@host# edit auto-configure
```

- d. Specify that you want to configure stacked VLANs.

```
[edit interfaces ge-2/3/0 auto-configure]
user@host# edit stacked-vlan-ranges
```

- e. Specify the dynamic VLAN profile that you want the interface to use.

```
[edit interfaces ge-2/3/0 auto-configure stacked-vlan-ranges]
user@host# set dynamic-profile VLAN-PROF
```

- f. Repeat steps a through e for any other interfaces that you want to use for creating VLANs.

3. Specify the Ethernet packet type that the VLAN dynamic profile can accept.

```
[edit interfaces ge-2/3/0 auto-configure stacked-vlan-ranges dynamic-profile
VLAN-PROF]
user@host# set accept inet6
```

4. Define VLAN ranges for use by the dynamic profile when dynamically creating VLAN IDs. For this solution, specify the outer and inner stacked VLAN ranges that you want the dynamic profile to use. The following example specifies an outer stacked VLAN ID range of 3–3 (enabling only the outer range of 3) and an inner stacked VLAN ID range of 1–3 (enabling a range from 1 through 3 for the inner stacked VLAN ID).

```
[edit interfaces ge-0/0/0 auto-configure stacked-vlan-ranges dynamic-profile
VLAN-PROF]
user@host# set stacked-vlan-ranges 3–3,1–3
```

Configuring Access Components for the DHCP Layer 3 Wholesale Network Solution

When configuring a wholesale network, you must configure several components globally. This configuration provides access to RADIUS servers that you want the wholesaler and any configured retailers to use globally. The access configuration includes the following general steps:

- [Configuring RADIUS Server Access on page 38](#)
- [Configuring a DHCP Wholesaler Access Profile on page 38](#)
- [Configuring DHCP Retailer Access Profiles on page 39](#)

Configuring RADIUS Server Access

You can globally define any RADIUS servers in your network that either the wholesale access profile or retailer access profile can use. After you define the global RADIUS servers, you can specify specific RADIUS servers within individual access profiles.

To define RADIUS servers for profile access:

1. Access the **[edit access radius-server]** hierarchy level.

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

2. Specify the address and secret for any RADIUS servers in the network.

```
[edit access radius-server]
user@host# set 192.168.10.1 secret $ABC123$ABC123$ABC123
user@host# set 10.10.10.1 secret $ABC123$ABC123
```

Configuring a DHCP Wholesaler Access Profile

You must define the network and interface over which you want subscribers to initially access the network with a wholesale access profile. When a subscriber attempts to access the network, the access profile provides initial access information including authentication and accounting values that the router uses for the accessing subscriber.

To define a wholesale access profile:

1. Create the wholesale access profile.

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

2. Specify the authentication methods for the profile and the order in which they are used.

```
[edit access profile Wholesaler1]
user@host# set authentication-order radius password
```

3. Specify that you want to configure RADIUS support.

```
[edit access profile Wholesaler1]
user@host# edit radius
```

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

```
[edit access profile Wholesaler1 radius]
user@host# set authentication-server 192.168.10.1
```

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

```
[edit access profile Wholesaler1 radius]
user@host# set accounting-server 192.168.10.1
```

6. Configure any desired options for the RADIUS server.

See Configuring RADIUS Server Options for Subscriber Access.

7. Configure subscriber accounting (RADIUS accounting).

See Configuring Per-Subscriber Session Accounting.

Configuring DHCP Retailer Access Profiles

In this solution, subscribers are redirected to a networking space used by a specific retailer and defined by a unique routing instance. This method requires that you define the network and interface over which you want subscribers to access the network after being redirected by the wholesale access profile.

To define a retailer access profile:

1. Create the retailer access profile.

```
[edit]
user@host# edit access-profile Retailer_Access1
```

2. Specify the authentication methods for the profile and the order in which they are used.

```
[edit access profile Retailer1]
user@host# set authentication-order radius password
```

3. Specify that you want to configure RADIUS support.

```
[edit access profile Retailer1]
user@host# edit radius
```

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

```
[edit access profile Retailer1 radius]
user@host# set authentication-server 10.10.10.1
```

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

```
[edit access profile Retailer1 radius]
user@host# set accounting-server 10.10.10.1
```

6. Configure any desired options for the RADIUS server.

See Configuring RADIUS Server Options for Subscriber Access.

7. Configure subscriber accounting (RADIUS accounting).

See Configuring Per-Subscriber Session Accounting.

Configuring Dynamic Profiles for the DHCPv6 Layer 3 Wholesale Network Solution

A dynamic profile is a set of characteristics, defined in a type of template, that you can use to provide services for broadband applications. These services are assigned dynamically to interfaces as they access the network. When configuring dynamic profiles for the DHCPv6 Layer 3 wholesale network, you can choose to configure one dynamic profile to address all incoming subscribers or you can configure individual dynamic profiles for use by the different network management groups (that is, the wholesaler and any retailers). In fact, you can create multiple dynamic profiles that you can use to roll out different services and selectively apply those dynamic profiles to different subscriber groups as necessary.

In this solution example, one dynamic profile is created for use by the wholesaler when subscribers initially access the network. Other dynamic profiles are created for the subscribers for each individual retailer to use after they are redirected to that retailer network space.

- [Configuring a Wholesale Dynamic Profile for use in the DHCPv6 Solution on page 40](#)
- [Configuring a Dynamic Profile for use by Each Retailer in the DHCPv6 Solution on page 41](#)

Configuring a Wholesale Dynamic Profile for use in the DHCPv6 Solution

You can configure a basic access profile to initially manage subscribers that access the network.

To configure a dynamic profile for use by the wholesaler:

1. Create a wholesale dynamic profile.

```
[edit]
user@host# edit dynamic-profiles Wholesaler_Profile
```

2. Specify that you want to configure the **demux0** interface in the dynamic profile.

```
[edit dynamic-profiles Wholesaler_Profile]
user@host# edit interfaces demux0
```

3. Configure the unit for the **demux0** interface.

- a. Configure the variable for the unit number of the **demux0** interface.

The variable is dynamically replaced with the unit number that DHCP supplies when the subscriber logs in.

```
[edit dynamic-profiles Wholesaler_Profile demux0]
user@host# edit unit $junos-interface-unit
```

- b. Configure the variable for the underlying interface of the demux interfaces and specify the **\$junos-underlying-interface** variable.

The variable is dynamically replaced with the underlying interface that DHCP supplies when the subscriber logs in.

```
[edit dynamic-profiles Wholesaler_Profile interfaces demux0 unit
 "$junos-interface-unit"]
user@host# set demux-options underlying-interface $junos-underlying-interface
```

4. Configure the family for the demux interfaces.

- a. Specify that you want to configure the family.

```
[edit dynamic-profiles Wholesaler_Profile interfaces demux0 unit
 "$junos-interface-unit"]
user@host# edit family inet6
```

- b. Configure the unnumbered address for the family.

```
[edit dynamic-profiles Wholesaler_Profile demux0 unit "$junos-interface-unit"
 family inet6]
user@host# set unnumbered-address lo0.0
```

- c. Configure the variable for the IPv6 address of the demux interface.

The variable is dynamically replaced with the IPv6 address that DHCP supplies when the subscriber logs in.

```
[edit dynamic-profiles Wholesaler_Profile interfaces demux0 unit
 "$junos-interface-unit"]
user@host# set demux-source $junos-subscriber-ipv6-address
```

Configuring a Dynamic Profile for use by Each Retailer in the DHCPv6 Solution

To configure a dynamic profile for use with retailer access:

1. Create a retail dynamic profile.

```
[edit]
user@host# edit dynamic-profiles Subscriber_Profile_Retail1
```

2. Define the dynamic routing instance variable in the dynamic profile.

```
[edit dynamic-profiles Subscriber_Profile_Retail1]
user@host# edit routing-instances $junos-routing-instance
```

3. Set the dynamic interface variable for the dynamic routing instance.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 routing-instances
 "$junos-routing-instance"]
user@host# set interface $junos-interface-name
```

4. Specify that you want to configure the **demux0** interface in the dynamic profile.

```
[edit dynamic-profiles Subscriber_Profile_Retail1]
user@host# edit interfaces demux0
```

5. Configure the unit for the **demux0** interface.

a. Configure the variable for the unit number of the **demux0** interface.

The variable is dynamically replaced with the unit number that DHCP supplies when the subscriber logs in.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 demux0]
user@host# edit unit $junos-interface-unit
```

b. Configure the variable for the underlying interface of the demux interfaces and specify the **\$junos-underlying-interface** variable.

The variable is dynamically replaced with the underlying interface that DHCP supplies when the subscriber logs in.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 interfaces demux0 unit
"$junos-interface-unit"]
user@host# set demux-options underlying-interface $junos-underlying-interface
```

6. Configure the family for the demux interfaces.

a. Specify that you want to configure the family.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 interfaces demux0 unit
"$junos-interface-unit"]
user@host# edit family inet6
```

b. Configure the unnumbered address and preferred source address for the family.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 demux0 unit "$junos-interface-unit"
family inet6]
user@host# set unnumbered-address $junos-loopback-interface
preferred-source-address $junos-preferred-source-address
```

c. Configure the variable that identifies the demux interface on the logical interface.

The variable is dynamically replaced with the IPv6 address that DHCP supplies when the subscriber logs in.

```
[edit dynamic-profiles business-profile interfaces demux0 unit "$junos-interface-unit"]
user@host# set demux-source $junos-subscriber-ipv6-address
```

Configuring Separate Routing Instances for DHCPv6 Service Retailers

As the owner of the system, the wholesaler typically uses the default routing instance. You must create separate routing instances for each individual retailer to keep routing information for individual retailers separate and to define any servers and forwarding options specific to each retailer.

To define a retailer routing instance:

1. Create the retailer routing instance.


```
[edit]
user@host# edit routing-instances Retailer_Instance1
```

- Specify the routing instance type for the retailer.

```
[edit routing-instances "Retailer_Instance1"]
user@host# set instance-type vrf
```

- Specify the access profile that you want the routing instance to use.

```
[edit routing-instances "Retailer_Instance1"]
user@host# set access-profile Retailer_Access1
```

- Specify the interface that faces the Retailer1 RADIUS server.

```
[edit routing-instances "Retailer_Instance1"]
user@host# set interface ge-11/1/9.10
```

- Specify the loopback interface unit for this routing instance.

```
[edit routing-instances "Retailer_Instance1"]
user@host# set interface lo0.1
```



NOTE: Loopback interfaces must be unique for each routing instance.

- Repeat this procedure for other retailers.

Related Documentation

Configuring Address Server Elements for the DHCPv6 Layer 3 Wholesale Solution

- [Configuring a DHCPv6 Address Assignment Pool on page 43](#)
- [Configuring Extended DHCPv6 Local Server on page 45](#)

Configuring a DHCPv6 Address Assignment Pool

Address assignment pools enable you to specify groups of IPv6 addresses that different client applications can share. In this configuration, the extended DHCPv6 local server configuration uses the address pool to provide addresses to subscribers that are accessing the network. You must create separate address assignment pools for each retailer routing instance.

You can create address assignment pools that provide full 128 bit IPv6 addresses or pools that provide prefixes of a specified length.

To configure an address assignment pool that provides full 128 -bit IPv6 addresses:

- Create and name an address assignment pool.

```
[edit]
user@host# edit access address-assignment pool AddressPool_1
```

2. Edit the address pool family.

```
[edit access address-assignment pool AddressPool_1]
user@host# edit family inet6
```

3. Define the IPv6 network prefix.

```
[edit access address-pool AddressPool_1 family inet6]
user@host# set prefix 2001:db8:2121::0/64
```

4. Define a named address range for the pool of IPv6 addresses.

```
[edit access address-assignment pool AddressPool_1 family inet6]
user@host# set range Range1 low 2001:db8:2121::a/128
user@host# set range Range1 high 2001:db8:2121::7ffe/128
```

5. (Optional) Edit the family DHCP attributes.

```
[edit access address-assignment pool AddressPool_1 family inet6]
user@host# edit dhcp-attributes
```

6. (Optional) Set the maximum lease time.

```
[edit access address-assignment pool AddressPool_1 family inet dhcp-attributes]
user@host# set maximum-lease-time 3600
```

7. (Optional) Set the grace period.

```
[edit access address-assignment pool AddressPool_1 family inet dhcp-attributes]
user@host# set grace-period 60
```

To configure an address assignment pool that provides shorter, 74-bit IPv6 prefixes:

1. Create and name an address assignment pool.

```
[edit]
user@host# edit access address-assignment pool AddressPool_2
```

2. Edit the address pool family.

```
[edit access address-assignment pool AddressPool_2]
user@host# edit family inet6
```

3. Define the IPv6 network prefix.

```
[edit access address-pool AddressPool_2 family inet6]
user@host# set prefix 2001:db8:2222::0/64
```

4. Define a named address range limit for the pool of IPv6 addresses.

```
[edit access address-assignment pool AddressPool_2 family inet6]
user@host# set range BitLimit prefix-length 74
```

5. (Optional) Edit the family DHCP attributes.

```
[edit access address-assignment pool AddressPool_2 family inet6]
user@host# edit dhcp-attributes
```

6. (Optional) Set the maximum lease time.

```
[edit access address-assignment pool AddressPool_2 family inet dhcp-attributes]
user@host# set maximum-lease-time 3600
```

7. (Optional) Set the grace period.

```
[edit access address-assignment pool AddressPool_2 family inet dhcp-attributes]
user@host# set grace-period 60
```

Configuring Extended DHCPv6 Local Server

You can enable the MX Series router to function as an extended DHCPv6 local server. The extended DHCPv6 local server provides IPv6 addresses and other configuration information to a subscriber logging into the network. You must configure extended DHCPv6 local server for the wholesaler (default) routing instance and also for each retailer routing instance.

To configure the DHCPv6 local server:

1. Edit the routing system services.

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

2. Edit the DHCPv6 local server.

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

3. Define the DHCP pool match order.

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

4. Set the authentication password.

```
[edit system services dhcp-local-server]
user@host# set authentication password $ABC123
```

5. (Optional) Edit the values you want included with the username.

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

6. (Optional) Set the values you want included with the username.

```
[edit system services dhcp-local-server username-include]
user@host# set domain-name example.com
user@host# set user-prefix user-defined-prefix
```

7. Access the DHCPv6-specific service configuration.

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

8. Create and name a DHCPv6 local server group.

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

9. Specify a dynamic profile that you want the DHCPv6 local server group to use.

```
[edit system services dhcp-local-server dhcpv6 group dhcp-ls-group]
user@host# set dynamic-profile Wholesaler_Profile
```

10. Assign interfaces to the group.

```
[edit system services dhcp-local-server dhcpv6 group dhcp-ls-group]
user@host# set interface ge-1/3/0.1 upto ge-1/3/0.5
```

11. Edit the DHCPv6 local server trace options.

```
[edit system processes dhcp-service]
user@host# edit traceoptions
```

12. Specify a log file into which you want trace option information to be saved.

```
[edit system processes dhcp-service traceoptions]
user@host# set file dhcp-server-msgs.log
```

13. Specify the DHCPv6 local server message operations that you want saved in the log file.

```
[edit system processes dhcp-service traceoptions]
user@host# set flag all
```

- Related Documentation**
- *Address-Assignment Pools Overview*
 - *DHCPv6 Local Server Overview*

Example: Retailer Dynamic Profile for a DHCPv6 Wholesale Network

```
dynamic-profiles {
  Subscriber_Profile_Retailer1 {
    routing-instances {
      "$junos-routing-instance" {
        interface "$junos-interface-name";
      }
    }
    interfaces {
      demux0 {
        unit "$junos-interface-unit" {
          demux-options {
            underlying-interface "$junos-underlying-interface";
          }
        }
        family inet6 {
          demux-source {
            "$junos-subscriber-ip-address";
          }
        }
      }
    }
  }
}
```

```

    }
    unnumbered-address "$junos-loopback-interface" preferred-source-address
    "$junos-preferred-source-address";
  }
}
}
}
}

```

Related Documentation • [Configuring Dynamic Profiles for the DHCPv6 Layer 3 Wholesale Network Solution on page 40](#)

Example: Retailer Routing Instances for a DHCPv6 Wholesale Network

```

routing-instances {
  Retailer_Instance1 {
    instance-type vrf;
    access-profile Retailer_Access1;
    interface ge-11/1/9.10;
    interface lo0.1;
    route-distinguisher 1:1;
  }
  Retailer_Instance2 {
    instance-type vrf;
    access-profile Retailer_Access2;
    interface ge-7/1/9.10;
    interface lo0.2;
  }
}

```

Related Documentation • [Configuring Separate Routing Instances for DHCPv6 Service Retailers on page 42](#)

Example: DHCPv6 Address Assignment Pool That Provides Full 128-bit IPV6 Addresses for a DHCPv6 Wholesale Network

```

access {
  address-assignment {
    pool AddressPool_1 {
      family inet6 {
        prefix 2001:db8:2121::0/64;
        range Range1 {
          low 2001:db8:2121::a/128;
          high 2001:db8:2121::7ffe/128;
        }
        dhcp-attributes {
          maximum-lease-time 3600;
          grace-period 60;
        }
      }
    }
  }
}

```

- Related Documentation**
- [DHCPv6 Address Assignment Pool That Provides Full 128-bit IPV6 Addresses for a DHCPv6 Wholesale Network](#)

Example: DHCPv6 Address Assignment Pool That Provides 74-bit IPV6 Prefixes for a DHCPv6 Wholesale Network

```
access {
  address-assignment {
    pool AddressPool_2 {
      family inet6 {
        prefix 2001:db8:2222::0/64;
        range BitLimit prefix-length 74;
        dhcp-attributes {
          maximum-lease-time 3600;
          grace-period 60;
        }
      }
    }
  }
}
```

- Related Documentation**
- [Configuring Address Server Elements for the DHCPv6 Layer 3 Wholesale Solution on page 43](#)

Example: Extended DHCPv6 Local Server for a DHCPv6 Wholesale Network

```
system {
  services {
    dhcp-local-server {
      traceoptions {
        file dhcp-server-msgs.log;
        flag all;
      }
    }
    dhcpv6 {
      group dhcp-ls-group {
        dynamic-profile Wholesaler_Profile;
        interface ge-1/3/0.1 {
          upto ge-1/3/0.5;
        }
      }
    }
    pool-match-order {
      ip-address-first;
    }
    authentication {
      password $ABC123;
      username-include {
        domain-name example.com;
        user-prefix user-defined-prefix;
      }
    }
  }
}
```

```
}  
}  
}  
}
```

Related Documentation

- [Configuring Address Server Elements for the DHCPv6 Layer 3 Wholesale Solution on page 43](#)

PART 2

Configuring PPPoE Layer 3 Wholesale Networks

- [Subscriber Management PPPoE Wholesale Overview on page 53](#)
- [Configuring PPPoE Layer 3 Wholesale Networks on page 57](#)

CHAPTER 4

Subscriber Management PPPoE Wholesale Overview

- [Layer 2 and Layer 3 Wholesale Overview on page 53](#)
- [PPPoE Layer 3 Wholesale Configuration Interface Support on page 54](#)
- [Subscriber to Logical System and Routing Instance Relationship on page 54](#)
- [RADIUS VSAs and Broadband Subscriber Management Wholesale Configuration Overview on page 55](#)

Layer 2 and Layer 3 Wholesale Overview

In general, wholesaling broadband services allows service providers to resell broadband services and allows other providers to deploy their own services over the incumbent network. There are different methods to partitioning an access network for resale. The two most common approaches are based on either Layer 2 or Layer 3 information. Wholesale access is the process by which the access network provider (the *wholesaler*) partitions the access network into separately manageable and accountable subscriber segments for resale to other network providers (or *retailers*).

In a Layer 3 wholesale configuration, you partition the wholesaler access network at the network layer or the subscriber IP component by associating the IP component with a distinct Layer 3 domain. In a Layer 2 wholesale configuration, you partition the access network at the subscriber circuit or customer VLAN (C-VLAN) by backhauling the connection through the service provider backbone network to the subscribing retailer network where the access traffic can be managed at higher layers.

In a Junos OS Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol over Ethernet (PPPoE) subscriber access configuration, wholesale partitioning is accomplished through the use of logical systems and routing instances within the router. Logical systems offer a stricter partitioning of routing resources than routing instances. The purpose behind the use of logical systems is to distinctly partition the physical router into separate administrative domains. This partitioning enables multiple providers to administer the router simultaneously, with each provider having access only to the portions of the configuration relevant to their logical system. Junos OS supports up to 15 named logical systems in addition to the default logical system (that is, **inet.0**). Unless otherwise specified in configuration, all interfaces belong to the default logical system.



NOTE: This Junos OS release supports the use of only the default logical system. Partitioning currently occurs through the use of separate routing instances.

A logical system can have one or more routing instances. Typically used in Layer 3 VPN scenarios, a routing instance does not have the same level of administrative separation as a logical system because it does not offer administrative isolation. However, the routing instance defines a distinct routing table, set of routing policies, and set of interfaces.

- Related Documentation**
- [Broadband Subscriber Management DHCPv4 Layer 3 Wholesale Topology and Configuration Elements on page 9](#)
 - [Broadband Subscriber Management PPPoE Layer 3 Wholesale Topology and Configuration Elements on page 57](#)
 - [Broadband Subscriber Management Layer 2 Wholesale Topology and Configuration Elements on page 75](#)

PPPoE Layer 3 Wholesale Configuration Interface Support

PPPoE Layer 3 wholesale requires the use of PPP interfaces. This means that you must specify the PPO interface when configuring Layer 3 wholesaling in a PPPoE network.

For general additional information about configuring PPPoE interfaces, see the *Junos OS Network Interfaces Library for Routing Devices*.

- Related Documentation**
- *Junos OS Network Interfaces Library for Routing Devices*
 - *Configuring a PPPoE Dynamic Profile in the Junos OS Broadband Subscriber Management and Services Library.*
 - *Configuring Dynamic PPPoE Subscriber Interfaces in the Junos OS Broadband Subscriber Management and Services Library.*

Subscriber to Logical System and Routing Instance Relationship

As subscriber sessions are established, subscriber to logical system/routing instance memberships are established by the AAA framework configured for the default logical system. When configuring Layer 3 wholesaling, you typically configure global (wholesale) information within the default (master) logical system and default routing instance. Incoming subscribers must then be authenticated, but this authentication can be handled in one of two ways:

- Single (wholesaler only) authentication—Incoming subscribers are authenticated by the wholesaler RADIUS server. After authentication, the subscribers are assigned values specified by dynamic profiles (routing instances, interfaces, and any configuration values) specific to a particular retailer.

- Dual (wholesaler and retailer) authentication—Sometimes referred to as *double-dip authentication*. Incoming subscribers are initially authenticated by RADIUS using the wholesale configuration. Authenticated subscribers are then redirected to other routing instances associated with individual retailer network space. When you redirect subscribers, and those subscribers are to be authenticated by AAA servers owned by individual retailers, the subscribers must be authenticated again by the AAA servers before they are provided an address and any dynamic profile values are assigned. After reauthentication, however, the subscribers are managed normally using any values specific to the retailer routing instance to which they are assigned.

**Related
Documentation**

- See *Routing Instances Overview* in the *Junos OS Routing Protocols Library*.

RADIUS VSAs and Broadband Subscriber Management Wholesale Configuration Overview

You can use RADIUS to assign various values through the use of dynamic variables within dynamic profiles. However, the configuration of at least one of the two VSAs described in [Table 3 on page 6](#) is required for a wholesale network to function.

Table 4: Required Juniper Networks VSAs for the Broadband Subscriber Management Wholesale Network Solution

Attribute Number	Attribute Name	Description	Value
26-1	LSRI-Name	Client logical system/routing instance membership name. Allowed only from RADIUS server for “default” logical system/routing instance membership.	string: logical system:routing instance
26-25	Redirect-LSRI-Name	Client logical system/routing instance membership name indicating to which logical system/routing instance membership the request is redirected for user authentication.	string: logical system:routing instance

Specifying the **\$junos-routing-instance** dynamic variable in a dynamic profile triggers a RADIUS access-accept response of either the LSRI-Name VSA or the Redirect-LSRI-Name VSA. Returning an LSRI-Name attribute in the access-accept response provides the logical system and routing instance in which the logical interface is to be created and the router updates the session database with the specified routing instance value. Returning a Redirect-LSRI-Name attribute in the access-accept response results in the router immediately sending a second access-request message (sometimes referred to

as a *double-dip*) to the RADIUS server specified by the logical system:routing instance attribute specified by the Redirect-LSRI-Name VSA.



NOTE: Attributes returned as a result of a second access-request message to the logical system/routing instance membership specified by the Redirect-LSRI-Name VSA override any prior attributes returned by initial access-accept responses to the default logical system/routing instance membership.

- Related Documentation**
- [Juniper Networks VSAs Supported by the AAA Service Framework on page 143](#) in the *Junos OS Broadband Subscriber Management and Services Library*.

CHAPTER 5

Configuring PPPoE Layer 3 Wholesale Networks

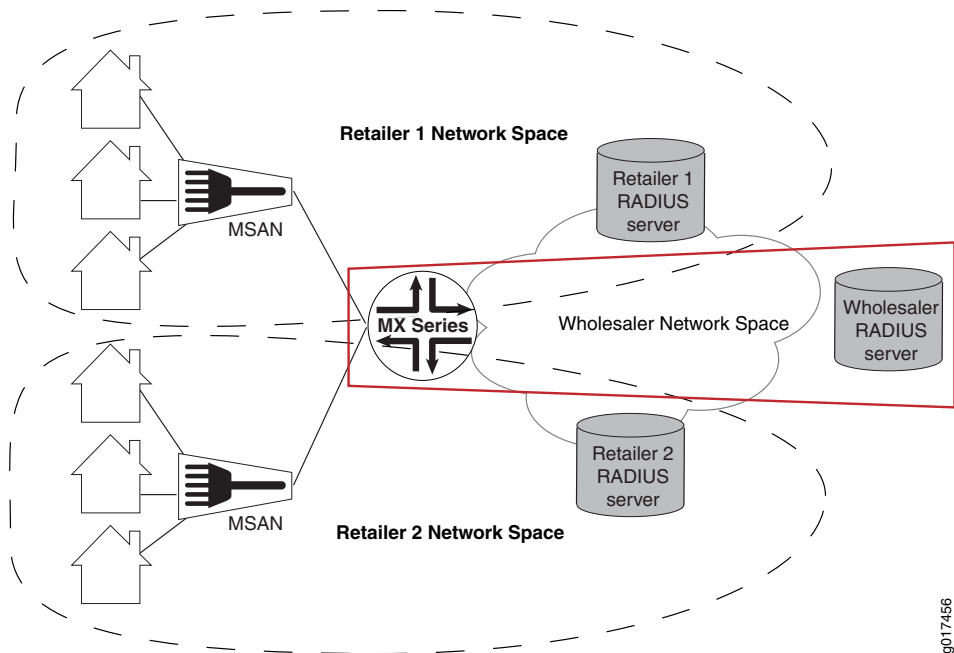
- Broadband Subscriber Management PPPoE Layer 3 Wholesale Topology and Configuration Elements on page 57
- PPPoE Layer 3 Wholesale Network Topology Overview on page 59
- Configuring Loopback Interfaces for the PPPoE Layer 3 Wholesale Solution on page 59
- Configuring Static Customer VLANs for the PPPoE Layer 3 Wholesale Network Solution on page 61
- Configuring Access Components for the PPPoE Wholesale Network Solution on page 61
- Configuring Dynamic Profiles for the PPPoE Layer 3 Wholesale Network Solution on page 64
- Configuring Separate Routing Instances for PPPoE Service Retailers on page 66
- Example: Wholesaler Dynamic Profile for a PPPoE Wholesale Network on page 67
- Example: Retailer Routing Instances for a PPPoE Wholesale Network on page 67

Broadband Subscriber Management PPPoE Layer 3 Wholesale Topology and Configuration Elements

The network topology for the subscriber management PPPoE Layer 3 wholesale solution includes configuring separate routing instances for individual retailers that use a portion of the router.

To explain the concept, but to limit complexity, this solution provides a configuration with one wholesaler and only two retailers. [Figure 5 on page 58](#) illustrates a basic PPPoE Layer 3 wholesale topology model from which you can expand.

Figure 5: Basic Subscriber Management PPPoE Layer 3 Wholesale Solution Topology



9017456

When you are configuring a PPPoE Layer 3 wholesale network solution, the following configuration elements are required:

- Subscriber network VLAN configuration
- Addressing server or addressing server access configuration
- RADIUS server access configuration
- Dynamic profile configuration for default (wholesaler) access
- Routing instance configuration for individual retailers
- Group configuration and forwarding options for the network
- Core network configuration

This implementation of PPPoE Layer 3 wholesale supports the following:

- Dynamic PPPoE interface creation.
- Static VLAN use only.
- AAA server assignment of subscribers to different routing instances within the same (default) logical system only.

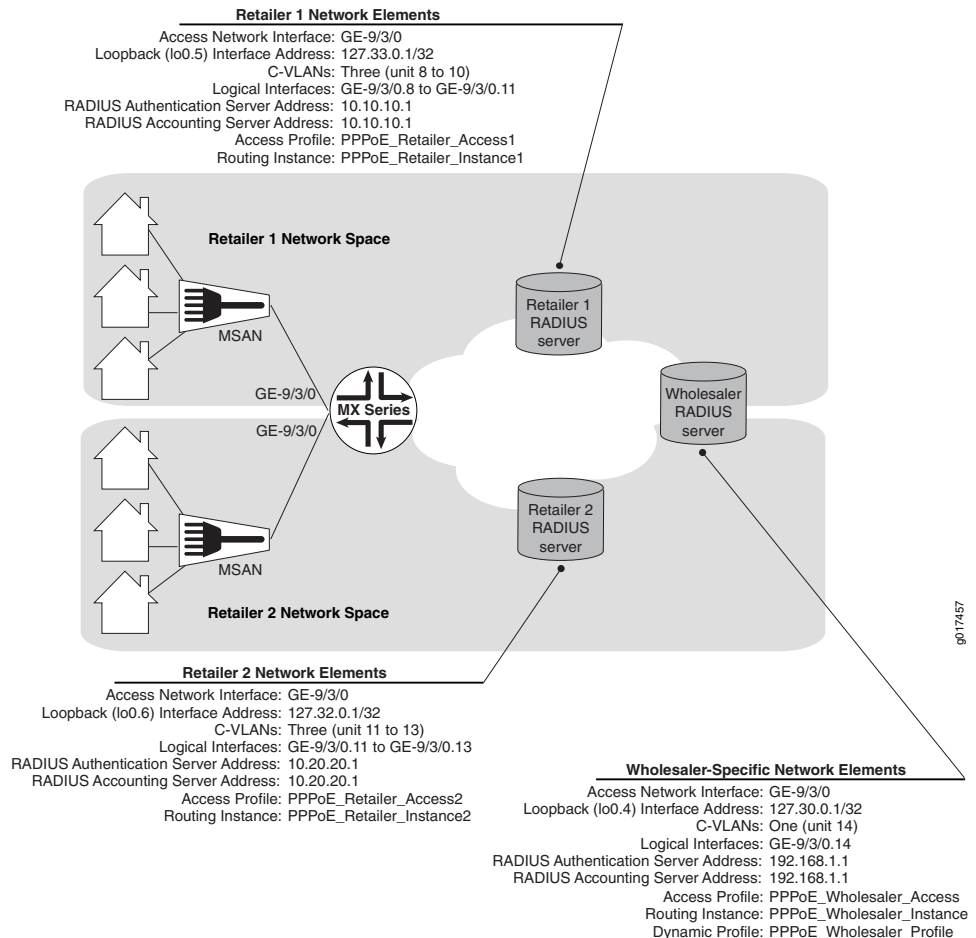
Related Documentation

- [Layer 2 and Layer 3 Wholesale Overview on page 3](#)
- [PPPoE Layer 3 Wholesale Network Topology Overview on page 59](#)

PPPoE Layer 3 Wholesale Network Topology Overview

This configuration explains how to configure a simple PPPoE Layer 3 wholesale subscriber access network. This solution incorporates two retailers sharing resources on a wholesaler router. [Figure 6 on page 59](#) provides the reference topology for this configuration example.

Figure 6: PPPoE Layer 3 Wholesale Network Reference Topology



Related Documentation

- [Layer 2 and Layer 3 Wholesale Overview on page 3](#)
- [Broadband Subscriber Management DHCPv4 Layer 3 Wholesale Topology and Configuration Elements on page 9](#)

Configuring Loopback Interfaces for the PPPoE Layer 3 Wholesale Solution

You must configure loopback interfaces for use in the subscriber management access network. The loopback interfaces are automatically used for unnumbered interfaces.



NOTE: If you do not configure the loopback interface, the routing platform chooses the first interface to come online as the default. If you configure more than one address on the loopback interface, we recommend that you configure one to be the primary address to ensure that it is selected for use with unnumbered interfaces. By default, the primary address is used as the source address when packets originate from the interface.

To configure loopback interfaces:

1. Edit the loopback interface.

```
[edit]
user@host# edit interfaces lo0
```

2. Edit the unit for the wholesale loopback interface.

```
[edit interfaces lo0]
user@host# edit unit 4
```

3. Edit the wholesale loopback interface family.

```
[edit interfaces lo0 unit 4]
user@host# edit family inet
```

4. Specify the wholesale loopback interface address.

```
[edit interfaces lo0 unit 4 family inet]
user@host# set address 127.30.0.1/32
```

5. (Optional) Specify the loopback interface address as the primary loopback interface.

```
[edit interfaces lo0 unit 4 family inet]
user@host# set address 127.30.0.2/32 primary
```

6. Edit the unit for a retail loopback interface.

```
[edit interfaces lo0]
user@host# edit unit 5
```

7. Edit the retail loopback interface family.

```
[edit interfaces lo0 unit 5]
user@host# edit family inet
```

8. Specify the retail loopback interface address.

```
[edit interfaces lo0 unit 5 family inet]
user@host# set address 127.33.0.1/32
```

9. (Optional) Specify the loopback interface address as the primary loopback interface.

```
[edit interfaces lo0 unit 5 family inet]
user@host# set address 127.33.0.2/32 primary
```

10. Repeat steps 7 through 10 for additional retailers, making sure to use unique unit and address values for each retailer loopback interface.

Related Documentation • [Junos OS Network Interfaces Library for Routing Devices](#)

Configuring Static Customer VLANs for the PPPoE Layer 3 Wholesale Network Solution

In this example configuration, the access interface (**ge-9/3/0**) connects to a device (that is, a DSLAM) on the access side of the network. You can define static customer VLANs (C-VLANs) for use by the wholesaler and any access network subscribers.

To configure the customer VLANs:

1. Edit the access side interface.

```
[edit]
user@host# edit interfaces ge-9/3/0
```

2. Specify the use of flexible VLAN tagging.

```
[edit interfaces ge-9/3/0]
user@host# set flexible-vlan-tagging
```

3. Edit the interface unit for the wholesaler VLAN.

```
[edit interfaces ge-9/3/0]
user@host# edit unit 14
```

4. Specify the type of encapsulation that you want the wholesaler VLAN to use.

```
[edit interfaces ge-9/3/0 unit 14]
user@host# set encapsulation ppp-over-ether
```

5. (Optional) Specify that you want the wholesaler VLAN to use Proxy ARP.

```
[edit interfaces ge-9/3/0 unit 14]
user@host# set proxy-arp
```

6. Define a unique VLAN ID for the wholesaler VLAN.

```
[edit interfaces ge-9/3/0 unit 14]
user@host# set vlan-id 14
```

7. Specify the dynamic profile that you want the wholesaler VLAN to use.

```
[edit interfaces ge-9/3/0 unit 14]
user@host# set pppoe-underlying-options dynamic-profile PPPoE_Wholesaler_Profile
```

Configuring Access Components for the PPPoE Wholesale Network Solution

When configuring a wholesale network, you must configure several components globally. This configuration provides access to RADIUS servers (if used) that you want the wholesaler and any configured retailers to use globally. The access configuration includes the following general steps:

- [Configuring RADIUS Server Access on page 62](#)
- [Configuring a PPPoE Wholesaler Access Profile on page 62](#)
- [Configuring PPPoE Retailer Access Profiles on page 63](#)

Configuring RADIUS Server Access

You can globally define any RADIUS servers in your network that either the wholesale access profile or retailer access profile can use. After you define the global RADIUS servers, you can specify specific RADIUS servers within individual access profiles.

To define RADIUS servers for profile access:

1. Access the **[edit access radius-server]** hierarchy level.

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

2. Specify the address and secret for any RADIUS servers in the network.

```
[edit access radius-server]
user@host# set 192.168.10.1 secret $ABC123$ABC123$ABC123
user@host# set 10.10.10.1 secret $ABC123$ABC123
```

Configuring a PPPoE Wholesaler Access Profile

You must define the network and interface over which you want subscribers to initially access the network with a wholesale access profile. When a subscriber attempts to access the network, the access profile provides initial access information including authentication and accounting values that the router uses for the accessing subscriber.

To define a wholesale access profile:

1. Create the wholesale access profile.

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

2. Specify the authentication methods for the profile and the order in which they are used.

```
[edit access profile PPPoE_Wholesaler_Access]
user@host# set authentication-order radius
```

3. Specify that you want to configure RADIUS support.

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

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

```
[edit access profile PPPoE_Wholesaler_Access radius]
user@host# set authentication-server 192.168.10.1
```

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

```
[edit access profile PPPoE_Wholesaler_Access radius]
user@host# set accounting-server 192.168.10.1
```

6. Configure any desired options for the RADIUS server.

See Configuring RADIUS Server Options for Subscriber Access.

7. Configure subscriber accounting (RADIUS accounting).

See Configuring Per-Subscriber Session Accounting.

Configuring PPPoE Retailer Access Profiles

In this solution, subscribers are redirected to a networking space used by a specific retailer and defined by a unique routing instance. This method requires that you define the network and interface over which you want subscribers to access the network after being redirected by the wholesale access profile.

To define a retailer access profile:

1. Create the retailer access profile.

```
[edit]
user@host# edit access profile PPPoE_Retailer_Access1
```

2. Specify the authentication methods for the profile and the order in which they are used.

```
[edit access profile PPPoE_Retailer_Access1]
user@host# set authentication-order radius
```

3. Specify that you want to configure RADIUS support.

```
[edit access profile PPPoE_Retailer_Access1]
user@host# edit radius
```

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

```
[edit access profile PPPoE_Retailer_Access1 radius]
user@host# set authentication-server 10.10.10.1
```

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

```
[edit access profile PPPoE_Retailer_Access1 radius]
user@host# set accounting-server 10.10.10.1
```

6. Configure any desired options for the RADIUS server.

See Configuring RADIUS Server Options for Subscriber Access.

7. Configure subscriber accounting (RADIUS accounting).

See Configuring Per-Subscriber Session Accounting.

Configuring Dynamic Profiles for the PPPoE Layer 3 Wholesale Network Solution

A dynamic profile is a set of characteristics, defined in a type of template, that you can use to provide services for broadband applications. These services are assigned dynamically to interfaces as they access the network. When configuring dynamic profiles for the PPPoE Layer 3 wholesale network, you can choose to configure one dynamic profile to address all incoming subscribers or you can configure individual dynamic profiles for use by the different network management groups (that is, the wholesaler and any retailers). In fact, you can create multiple dynamic profiles that you can use to roll out different services and selectively apply those dynamic profiles to different subscriber groups as necessary.

In this solution example, one dynamic profile is created for use by the wholesaler when subscribers initially access the network. Subscribers are assigned by the wholesaler RADIUS server to a particular retailer routing instance and can then be redirected to that retailer network space.

- [Configuring a Wholesale Dynamic Profile for use in the PPPoE Solution on page 64](#)

Configuring a Wholesale Dynamic Profile for use in the PPPoE Solution

You can configure a basic access profile to initially manage PPPoE subscribers that access the network.

To configure a dynamic profile for use by the wholesaler:

1. Create a wholesale dynamic profile.

```
[edit]
user@host# edit dynamic-profiles PPPoE_Wholesaler_Profile
```

2. Define the dynamic routing instance variable in the dynamic profile.

```
[edit dynamic-profiles PPPoE_Wholesaler_Profile]
user@host# edit routing-instances $junos-routing-instance
```

3. Set the dynamic interface variable for the dynamic routing instance.

```
[edit dynamic-profiles PPPoE_Wholesaler_Profile routing-instances
"$junos-routing-instance"]
user@host# set interface $junos-interface-name
```

4. Specify that you want to configure the **pp0** interface in the dynamic profile.

```
[edit dynamic-profiles PPPoE_Wholesaler_Profile]
user@host# edit interfaces pp0
```

5. Configure the unit for the **pp0** interface.

- a. Configure the variable for the unit number of the **pp0** interface.

The variable is dynamically replaced with the unit number that RADIUS supplies when the subscriber logs in.

```
[edit dynamic-profiles PPPoE_Wholesaler_Profile interfaces pp0]
user@host# edit unit $junos-interface-unit
```

- b. Configure PAP or CHAP (or both) to function on the interface.

```
[edit dynamic-profiles PPPoE_Wholesaler_Profile interfaces pp0 unit
"$junos-interface-unit"]
user@host# set ppp-options chap pap
```

- c. Configure the variable for the underlying interface of the pp0 interfaces.

The variable is dynamically replaced with the underlying interface that RADIUS supplies when the subscriber logs in.

```
[edit dynamic-profiles PPPoE_Wholesaler_Profile interfaces pp0 unit
"$junos-interface-unit"]
user@host# set pppoe-options underlying-interface $junos-underlying-interface
```

- d. Configure the router to act as a PPPoE server.

```
[edit dynamic-profiles PPPoE_Wholesaler_Profile interfaces pp0 unit
"$junos-interface-unit"]
user@host# set pppoe-options server
```

6. (Optional) Modify the PPPoE keepalive interval.

```
[edit dynamic-profiles PPPoE_Wholesaler_Profile interfaces pp0 unit
"$junos-interface-unit"]
user@host# set keepalives interval 15
```

7. Configure the family for the pp0 interface.

- a. Specify that you want to configure the family.



NOTE: You can specify `inet` for IPv4 and `inet6` for IPv6. However, this solution provides the IPv4 configuration only.

```
[edit dynamic-profiles PPPoE_Wholesaler_Profile interfaces pp0 unit
"$junos-interface-unit"]
user@host# edit family inet
```

- b. Configure the unnumbered address for the family.

```
[edit dynamic-profiles PPPoE_Wholesaler_Profile interfaces pp0 unit
"$junos-interface-unit" family inet]
user@host# set unnumbered-address $junos-loopback-interface
```

Configuring Separate Routing Instances for PPPoE Service Retailers

As the owner of the system, the wholesaler uses the default routing instance. You must create separate routing instances for each individual retailer to keep routing information for individual retailers separate and to define any servers and forwarding options specific to each retailer.

To define a retailer routing instance:

1. Create the retailer routing instance.

```
[edit]
user@host# edit routing-instances PPPoE_Retailer_Instance1
```

2. Specify the routing instance type for the retailer.

```
[edit routing-instances "PPPoE_Retailer_Instance1"]
user@host# set instance-type vrf
```

3. Specify the access profile that you want the routing instance to use.

```
[edit routing-instances "PPPoE_Retailer_Instance1"]
user@host# set access-profile PPPoE_Retailer_Access1
```

4. Specify the interface that faces the Retailer1 RADIUS server.

```
[edit routing-instances "PPPoE_Retailer_Instance1"]
user@host# set interface ge-11/1/9.10
```

5. Specify the loopback interface unit for this routing instance.

```
[edit routing-instances "PPPoE_Retailer_Instance1"]
user@host# set interface lo0.5
```



NOTE: Loopback interfaces must be unique for each routing instance.

6. Specify an identifier to distinguish the VPN to which the route belongs.

```
[edit routing-instances "PPPoE_Retailer_Instance1"]
user@host# set route-distinguisher 1:1
```

7. Specify how routes are imported into the local PE router's VPN routing table from the remote PE router.

```
[edit routing-instances "PPPoE_Retailer_Instance1"]
user@host# set vrf-import policyImport
```

8. Specify which routes are exported from the local instance table to the remote PE router.


```
[edit routing-instances "PPPoE_Retailer_Instance1"]
user@host# set vrf-export policyExport
```

9. Repeat this procedure for other retailers.

Related Documentation

Example: Wholesaler Dynamic Profile for a PPPoE Wholesale Network

This example specifies a dynamic profile name of *PPPoE_Wholesaler_Profile*, uses *pp0* interfaces, and references the predefined input firewall filter.

```
PPPoE_Wholesaler_Profile {
  routing-instances {
    "$junos-routing-instance" {
      interface "$junos-interface-name";
    }
  }
  interfaces {
    pp0 {
      unit "$junos-interface-unit" {
        ppp-options {
          chap;
          pap;
        }
        pppoe-options {
          underlying-interface "$junos-underlying-interface";
          server;
        }
        keepalives interval 15;
        family inet {
          filter {
            input "$junos-input-filter";
            output "$junos-output-filter";
          }
          unnumbered-address "$junos-loopback-interface";
        }
      }
    }
  }
}
```

- Related Documentation
- [Configuring Dynamic Profiles for the PPPoE Layer 3 Wholesale Network Solution on page 64](#)

Example: Retailer Routing Instances for a PPPoE Wholesale Network

```
routing-instances {
  PPPoE_Retailer_Instance1 {
    instance-type vrf;
```

```
access-profile PPPoE_Retailer_Access1;
interface ge-11/1/9.10;
interface lo0.5;
route-distinguisher 1:1;
vrf-import policyImport;
vrf-export policyExport;
}
Retailer_Instance2 {
instance-type vrf;
access-profile PPPoE_Retailer_Access2;
interface ge-11/1/9.10;
interface lo0.6;
route-distinguisher 2:2;
vrf-import policyImport;
vrf-export policyExport;
}
}
```

**Related
Documentation**

- [Configuring Separate Routing Instances for PPPoE Service Retailers on page 66](#)

PART 3

Configuring Layer 2 Wholesale Networks

- [Subscriber Management Layer 2 Wholesale Overview on page 71](#)
- [Configuring Layer 2 Wholesale Networks on page 75](#)

CHAPTER 6

Subscriber Management Layer 2 Wholesale Overview

- [Layer 2 and Layer 3 Wholesale Overview on page 71](#)
- [Wholesale Network Configuration Options and Considerations on page 72](#)
- [RADIUS VSAs and Broadband Subscriber Management Wholesale Configuration Overview on page 73](#)

Layer 2 and Layer 3 Wholesale Overview

In general, wholesaling broadband services allows service providers to resell broadband services and allows other providers to deploy their own services over the incumbent network. There are different methods to partitioning an access network for resale. The two most common approaches are based on either Layer 2 or Layer 3 information. Wholesale access is the process by which the access network provider (the *wholesaler*) partitions the access network into separately manageable and accountable subscriber segments for resale to other network providers (or *retailers*).

In a Layer 3 wholesale configuration, you partition the wholesaler access network at the network layer or the subscriber IP component by associating the IP component with a distinct Layer 3 domain. In a Layer 2 wholesale configuration, you partition the access network at the subscriber circuit or customer VLAN (C-VLAN) by backhauling the connection through the service provider backbone network to the subscribing retailer network where the access traffic can be managed at higher layers.

In a Junos OS Dynamic Host Configuration Protocol (DHCP) or Point-to-Point Protocol over Ethernet (PPPoE) subscriber access configuration, wholesale partitioning is accomplished through the use of logical systems and routing instances within the router. Logical systems offer a stricter partitioning of routing resources than routing instances. The purpose behind the use of logical systems is to distinctly partition the physical router into separate administrative domains. This partitioning enables multiple providers to administer the router simultaneously, with each provider having access only to the portions of the configuration relevant to their logical system. Junos OS supports up to 15 named logical systems in addition to the default logical system (that is, **inet.0**). Unless otherwise specified in configuration, all interfaces belong to the default logical system.



NOTE: This Junos OS release supports the use of only the default logical system. Partitioning currently occurs through the use of separate routing instances.

A logical system can have one or more routing instances. Typically used in Layer 3 VPN scenarios, a routing instance does not have the same level of administrative separation as a logical system because it does not offer administrative isolation. However, the routing instance defines a distinct routing table, set of routing policies, and set of interfaces.

Related Documentation

- [Broadband Subscriber Management DHCPv4 Layer 3 Wholesale Topology and Configuration Elements on page 9](#)
- [Broadband Subscriber Management PPPoE Layer 3 Wholesale Topology and Configuration Elements on page 57](#)
- [Broadband Subscriber Management Layer 2 Wholesale Topology and Configuration Elements on page 75](#)

Wholesale Network Configuration Options and Considerations

You can configure a wholesale network any number of ways using Juniper Networks hardware and Junos OS software. For information about subscriber management hardware support, see the *Junos OS Broadband Subscriber Management and Services Library*. The general configuration options, and considerations for each, are provided in the following table:

Wholesale Configuration Options	Considerations
Fully Static (all interfaces, VLANs, and routing instances are configured statically)	Providing more control over retailer space and access, this option is more labor intensive and can require more detailed planning of the network, address allocation, and so on.
Static VLANs and Dynamic Demux Interfaces	Service VLANs are created statically and must be managed. Demux interfaces are dynamically created over the service VLANs. This option uses more logical interfaces; one for each VLAN and one for each dynamic demux interface that runs over each VLAN.
Dynamic VLANs Only (dedicated customer VLANs for each subscriber)	Dynamic (auto-sensed) VLANs are authenticated and installed in the correct non-default routing instance before DHCP is instantiated. This method helps to conserve logical interfaces by avoiding the need for additional logical interfaces being created for each demux interface. NOTE: In a customer VLAN model, each VLAN functions on a 1:1 basis for each customer (in this case, per household).
Dynamic VLANs and Dynamic Demux Interfaces	Allows for the greatest ease of use and flexibility in configuring subscribers, by enabling access over a service VLAN and targetting more service levels over individual, dynamically-created demux interfaces over the service VLAN. This option uses more logical interfaces; one for each VLAN and one for each demux interface that runs over each VLAN.

RADIUS VSAs and Broadband Subscriber Management Wholesale Configuration Overview

You can use RADIUS to assign various values through the use of dynamic variables within dynamic profiles. However, the configuration of at least one of the two VSAs described in [Table 3 on page 6](#) is required for a wholesale network to function.

Table 5: Required Juniper Networks VSAs for the Broadband Subscriber Management Wholesale Network Solution

Attribute Number	Attribute Name	Description	Value
26-1	LSRI-Name	Client logical system/routing instance membership name. Allowed only from RADIUS server for "default" logical system/routing instance membership.	string: logical system:routing instance
26-25	Redirect-LSRI-Name	Client logical system/routing instance membership name indicating to which logical system/routing instance membership the request is redirected for user authentication.	string: logical system:routing instance

Specifying the `$junos-routing-instance` dynamic variable in a dynamic profile triggers a RADIUS access-accept response of either the LSRI-Name VSA or the Redirect-LSRI-Name VSA. Returning an LSRI-Name attribute in the access-accept response provides the logical system and routing instance in which the logical interface is to be created and the router updates the session database with the specified routing instance value. Returning a Redirect-LSRI-Name attribute in the access-accept response results in the router immediately sending a second access-request message (sometimes referred to as a *double-dip*) to the RADIUS server specified by the logical system:routing instance attribute specified by the Redirect-LSRI-Name VSA.



NOTE: Attributes returned as a result of a second access-request message to the logical system/routing instance membership specified by the Redirect-LSRI-Name VSA override any prior attributes returned by initial access-accept responses to the default logical system/routing instance membership.

Related Documentation

- [Juniper Networks VSAs Supported by the AAA Service Framework on page 143](#) in the *Junos OS Broadband Subscriber Management and Services Library*.

CHAPTER 7

Configuring Layer 2 Wholesale Networks

- [Broadband Subscriber Management Layer 2 Wholesale Topology and Configuration Elements on page 75](#)
- [Layer 2 Wholesale Network Topology Overview on page 77](#)
- [Configuring a Retail Dynamic Profile for Use in the Layer 2 Wholesale Solution on page 79](#)
- [Stacking and Rewriting VLAN Tags for the Layer 2 Wholesale Solution on page 80](#)
- [Configuring VLAN Interfaces for the Layer 2 Wholesale Solution on page 82](#)
- [Configuring Encapsulation for Layer 2 Wholesale VLAN Interfaces on page 83](#)
- [Configuring NNI ISP-Facing Interfaces for the Layer 2 Wholesale Solution on page 84](#)
- [Configuring Direct ISP-Facing Interfaces for the Layer 2 Wholesale Solution on page 85](#)
- [Configuring Separate Access Routing Instances for Layer 2 Wholesale Service Retailers on page 86](#)
- [Configuring Separate NNI Routing Instances for Layer 2 Wholesale Service Retailers on page 89](#)
- [Configuring Access Components for the Layer 2 Wholesale Network Solution on page 91](#)
- [Example: Retailer Dynamic Profile for a Layer 2 Wholesale Network on page 92](#)
- [Example: Access Interface for a Layer 2 Wholesale Network on page 93](#)
- [Example: Retailer Access Routing Instances for a Layer 2 Wholesale Network on page 93](#)
- [Example: Retailer NNI ISP-Facing Interfaces for a Layer 2 Wholesale Network on page 94](#)
- [Example: Retailer Direct ISP-Facing Interface for a Layer 2 Wholesale Network on page 95](#)

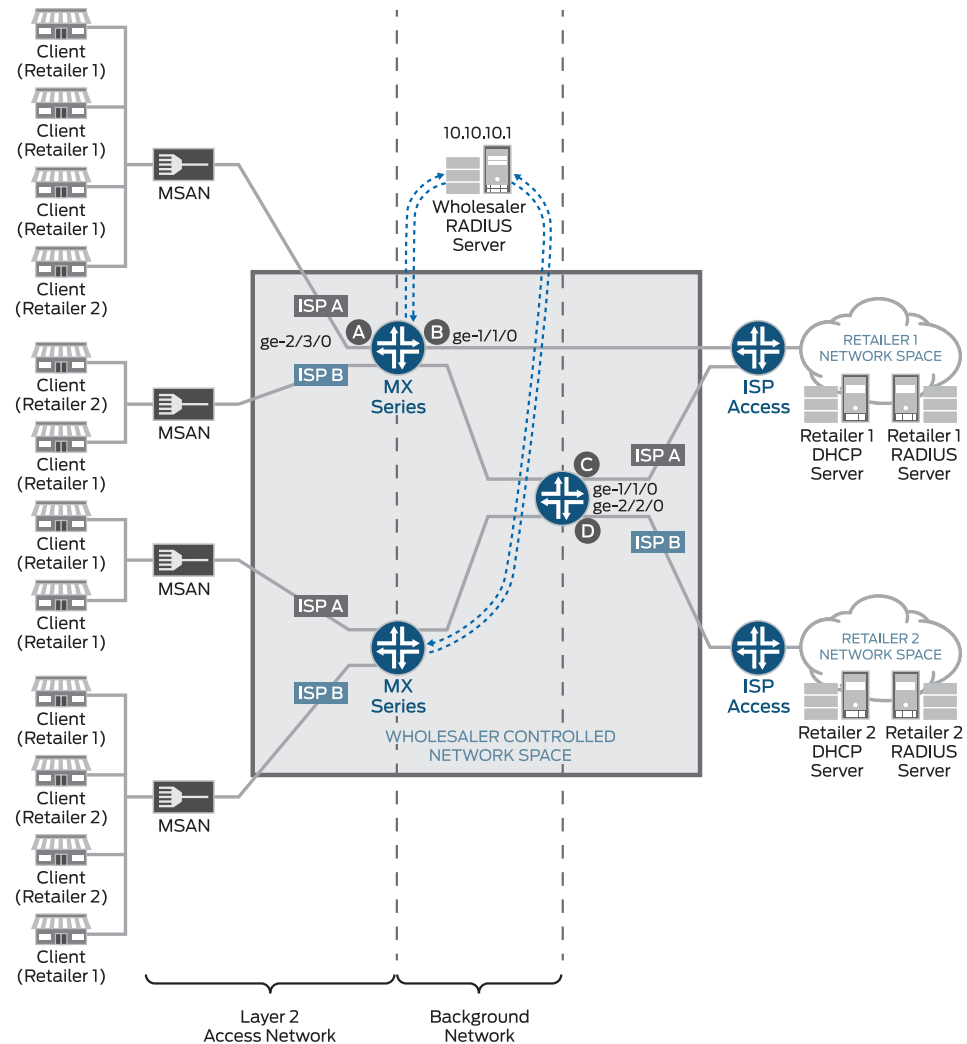
Broadband Subscriber Management Layer 2 Wholesale Topology and Configuration Elements

The network topology for the subscriber management Layer 2 wholesale solution includes configuring separate routing instances for individual retailers that use a portion of the router. This solution uses a Virtual Private LAN Service (VPLS) configuration.

Layer 2 wholesale networks are supported on MPC/MIC interfaces.

To explain the concept but limit complexity, this solution provides a configuration with one wholesaler and only two retailers. [Figure 7 on page 76](#) illustrates a basic Layer 2 wholesale topology model from which you can expand.

Figure 7: Basic Subscriber Management Layer 2 Wholesale Solution Topology



- A Wholesaler Access PE Router Network Elements**
 Access Network Interface: GE-2/3/0
 RADIUS Authentication Server Address: 10.10.10.1
 RADIUS Accounting Server Address: 10.10.10.1
 Access Profile: AccessProfile
 Routing Instances: Retailer_Instance1
 Retailer_Instance2
 Dynamic Profile: 1.2_Access_Profile

- B Wholesaler Direct ISP-Facing Interface**
 Interface facing ISP Retailer 1: GE-1/1/0.1
 VPLS Routing Instances: Retailer_Instance1
- C Wholesaler NNI-1-ISP-Facing Interface**
 Interface facing ISP Retailer 1: GE-1/1/0.0
 VPLS Routing Instances: Retailer_Instance1
- D Wholesaler NNI-2-ISP-Facing Interface**
 Interface facing ISP Retailer 2: GE-2/2/0.0
 VPLS Routing Instances: Retailer_Instance2

80-4212

When you are configuring a Layer 2 wholesale network solution, the following configuration elements are required:

- Subscriber access dynamic VLAN configuration including dynamic profile configuration for retailer routing instances
- Routing instance configuration for individual retailers on provider edge (PE) routers and network-to-network interface (NNI) routers.
- VLAN interface configuration
- RADIUS server access configuration
- Core network configuration

**Related
Documentation**

- [Layer 2 and Layer 3 Wholesale Overview on page 3](#)
- [Layer 2 Wholesale Network Topology Overview on page 77](#)

Layer 2 Wholesale Network Topology Overview

This configuration explains how to configure a simple Layer 2 wholesale subscriber access network. This solution illustrates two Internet Service Provider (ISP) retailers sharing access to a wholesaler network. The wholesaler network contains a Layer 2 Network access router and two Virtual Private LAN Service (VPLS) network-to-network interface (NNI) routers.



NOTE: You can have more than one ISP router connecting to a single VPLS NNI router with VPLS interfaces configured with routing instances specific to each different ISP-facing interfaces.

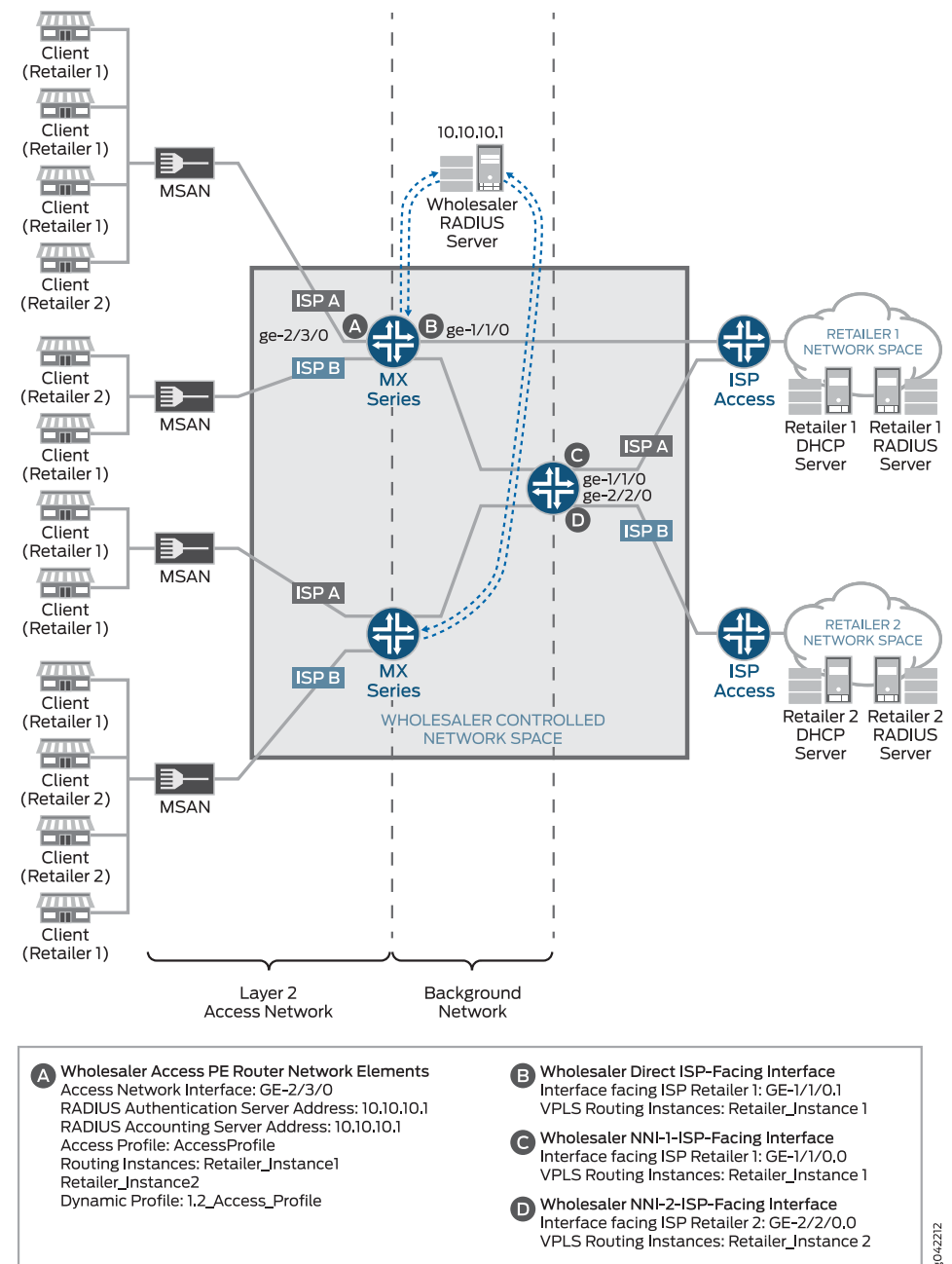
The example also shows two different connection options from one subscriber access router to one of the individual ISP access routers. One connection option uses an interface on the subscriber access router to connect directly to the ISP access router. Another connection option uses two routers: a subscriber access router and another NNI router that connects to the ISP access router.



NOTE: When using the NNI router connection option, use a standard BGP or MPLS configuration between the subscriber access routers and the edge router that connects to the ISP access routers. See the *Junos OS Routing Protocols Library* for information about BGP configuration. See the *Junos OS MPLS Applications Library for Routing Devices* for information about MPLS configuration.

Figure 8 on page 78 provides the reference topology for this configuration example.

Figure 8: Layer 2 Wholesale Network Reference Topology



Related Documentation

- [Layer 2 and Layer 3 Wholesale Overview on page 3](#)
- [Broadband Subscriber Management Layer 2 Wholesale Topology and Configuration Elements on page 75](#)

Configuring a Retail Dynamic Profile for Use in the Layer 2 Wholesale Solution

To configure a dynamic profile for use with retailer access:

1. Create a retail dynamic profile.

```
[edit]
user@host# edit dynamic-profiles Subscriber_Profile_Retail1
```

2. Define the dynamic routing instance variable in the dynamic profile.

```
[edit dynamic-profiles Subscriber_Profile_Retail1]
user@host# edit routing-instances $junos-routing-instance
```

3. Set the dynamic interface variable for the dynamic routing instance.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 routing-instances
 "$junos-routing-instance"]
user@host# set interface $junos-interface-name
```

4. Define the dynamic interfaces variable for the dynamic profile.

```
[edit dynamic-profiles Subscriber_Profile_Retail1]
user@host# set interfaces $junos-interface-ifd-name
```

5. Define the dynamic interface unit variable for the dynamic profile.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 interfaces "$junos-interface-ifd-name"]
user@host# set unit $junos-interface-unit
```

6. (Optional) Define the VLAN encapsulation for the dynamic interfaces.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 interfaces "$junos-interface-ifd-name"
 unit "$junos-interface-unit"]
user@host# set encapsulation vlan-vpls
```



NOTE: If you choose not to specify an encapsulation for the logical interface, you must specify encapsulation for the physical interface.

7. Define the VLAN tag variables for the dynamic profile:



NOTE: This solution example uses stacked VLAN tagging. However, you can also specify single-tag VLANs. For additional information about configuring dynamic VLANs, see the *Junos OS Broadband Subscriber Management and Services Library*.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 interfaces "$junos-interface-ifd-name"
 unit "$junos-interface-unit"]
user@host# set vlan-tags outer $junos-stacked-vlan-id inner $junos-vlan-id
```

8. Define the input and output VLAN maps. See [“Stacking and Rewriting VLAN Tags for the Layer 2 Wholesale Solution” on page 80](#) for details.

9. Specify the unit family as **vpls** at the **[edit dynamic-profiles *profile-name* interfaces “\$junos-interface-ifd-name” unit “\$junos-interface-unit” family]** hierarchy level.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 interfaces “$junos-interface-ifd-name”
 unit “$junos-interface-unit”]
user@host# set family vpls
```

Stacking and Rewriting VLAN Tags for the Layer 2 Wholesale Solution

Stacking and rewriting VLAN tags allows you to use an additional (outer) VLAN tag to differentiate between routers in the Layer 2 wholesale network. A frame can be received on an interface, or it can be internal to the system (as a result of the **input-vlan-map** statement).

You can configure rewrite operations to stack (**push**), remove (**pop**), or rewrite (**swap**) tags on single-tagged frames and dual-tagged frames. If a port is not tagged, rewrite operations are not supported on any logical interface on that port.

You can configure the following single-action VLAN rewrite operations:

- **pop**—Remove a VLAN tag from the top of the VLAN tag stack. The outer VLAN tag of the frame is removed.
- **push**—Add a new VLAN tag to the top of the VLAN stack. An outer VLAN tag is pushed in front of the existing VLAN tag.
- **swap**—Replace the inner VLAN tag of the incoming frame with a user-specified VLAN tag value.

You configure VLAN rewrite operations for logical interfaces in the input VLAN map for incoming frames and in the output VLAN map for outgoing frames.

You can include both the **input-vlan-map** and **output-vlan-map** statements at the **[edit dynamic-profiles *profile-name* interface “\$junos-interface-ifd-name” unit “\$junos-interface-unit”]** hierarchy level.

The type of VLAN rewrite operation permitted depends upon whether the frame is single-tagged or dual-tagged. [Table 6 on page 80](#) shows supported rewrite operations and whether they can be applied to single-tagged frames or dual-tagged frames. The table also indicates the number of tags being added or removed during the operation.

Table 6: Rewrite Operations on Single-Tagged and Dual-Tagged Frames

Rewrite Operation	Single-Tagged	Dual-Tagged	Number of Tags
pop	Yes	Yes	– 1
push	Yes	Yes	+1

Table 6: Rewrite Operations on Single-Tagged and Dual-Tagged Frames (*continued*)

Rewrite Operation	Single-Tagged	Dual-Tagged	Number of Tags
swap	Yes	Yes	0

Depending on the VLAN rewrite operation, you configure the rewrite operation for the interface in the input VLAN map, the output VLAN map, or both. [Table 7 on page 81](#) shows what rewrite operation combinations you can configure. “None” means that no rewrite operation is specified for the VLAN map.

Table 7: Applying Rewrite Operations to VLAN Maps

Input VLAN Map	Output VLAN Map			
	none	push	pop	swap
none	Yes	No	No	Yes
push	No	No	Yes	No
pop	No	Yes	No	No
swap	Yes	No	No	Yes

To configure the input VLAN map:



NOTE: You configure the `input-vlan-map` statement only when there is a need either to push an outer tag on a single-tagged subscriber packet or to modify the outer tag in a subscriber dual-tagged packet.

1. Include the `input-vlan-map` statement.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 interfaces "$junos-interface-ifd-name"
 unit "$junos-interface-unit"]
user@host# edit input-vlan-map
```

2. Specify the action that you want the input VLAN map to take.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 interfaces "$junos-interface-ifd-name"
 unit "$junos-interface-unit" input-vlan-map]
user@host# set push
```

3. Include the `vlan-id` statement along with the `$junos-vlan-map-id` dynamic variable.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 interfaces "$junos-interface-ifd-name"
 unit "$junos-interface-unit" input-vlan-map]
user@host# set vlan-id $junos-vlan-map-id
```

To configure the output VLAN map:



NOTE: You configure the `output-vlan-map` statement only when there is a need to either pop or modify the outer tag found in a dual-tagged packet meant for the subscriber.

1. Include the **output-vlan-map** statement.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 interfaces "$junos-interface-ifd-name"
 unit "$junos-interface-unit"]
user@host# edit output-vlan-map
```

2. Specify the action that you want the output VLAN map to take.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 interfaces "$junos-interface-ifd-name"
 unit "$junos-interface-unit" output-vlan-map]
user@host# set pop
```

You must know whether the VLAN rewrite operation is valid and is applied to the input VLAN map or the output VLAN map. You must also know whether the rewrite operation requires you to include statements to configure the inner and outer tag protocol identifiers (TPIDs) and inner and outer VLAN IDs in the input VLAN map or output VLAN map. For information about configuring inner and outer TPIDs and inner and outer VLAN IDs, see *Configuring Inner and Outer TPIDs and VLAN IDs*.

Configuring VLAN Interfaces for the Layer 2 Wholesale Solution

Clients access the Layer 2 Wholesale network through a specific interface. After they access this interface, and when they are authenticated, VLANs are dynamically created to carry the client traffic.

To configure a VLAN interface for dynamic access of clients:

1. Access the physical interface that you want to use for dynamically creating VLAN interfaces.

```
[edit interfaces]
user@host# edit interfaces ge-2/3/0
```

2. Specify the desired VLAN tagging.



NOTE: This example uses flexible VLAN tagging to simultaneously support transmission of 802.1Q VLAN single-tag and dual-tag frames on logical interfaces on the same Ethernet port.

```
[edit interfaces ge-2/3/0]
user@host# set flexible-vlan-tagging
```


3. Specify that you want to automatically configure VLAN interfaces.

```
[edit interfaces ge-2/3/0]
user@host# edit auto-configure
```

4. Specify that you want to configure single VLANs.

```
[edit interfaces ge-2/3/0 auto-configure]
user@host# edit vlan-ranges
```

5. Define the VLAN ranges for the configuration.

```
[edit interfaces ge-2/3/0 auto-configure vlan-ranges]
user@host# set ranges any, any
```

6. Specify the dynamic VLAN profile that you want the interface to use.

```
[edit interfaces ge-2/3/0 auto-configure vlan-ranges]
user@host# set dynamic-profile Subscriber_Profile_Retail1
```

7. Specify that any type of VLAN Ethernet packet is accepted by the interface.

```
[edit interfaces ge-2/3/0 auto-configure vlan-ranges dynamic-profile
"Subscriber_Profile_Retail1"]
user@host# set accept any
```

8. Repeat steps for any other interfaces that you want to use for creating VLANs.

9. Specify the encapsulation type for the VLAN interfaces.

```
[edit interfaces ge-2/3/0]
user@host# edit encapsulation flexible-ethernet-services
```

Related Documentation

- [Configuring Encapsulation for Layer 2 Wholesale VLAN Interfaces on page 83](#)

Configuring Encapsulation for Layer 2 Wholesale VLAN Interfaces

Each dynamic VLAN interface in a Layer 2 wholesale network must use encapsulation. You can configure encapsulation dynamically for each VLAN interface by using the **encapsulation** statement at the **[edit dynamic-profiles *profile-name* interface "\$junos-interface-ifd-name" unit "\$junos-interface-unit"]** hierarchy level or configure encapsulation for the physical interfaces at the **[edit interfaces *interface-name*]** hierarchy level for each dynamically created VLAN interface to use. However, how you choose to configure (or not configure) encapsulation at the **[edit dynamic-profiles *profile-name* interface "\$junos-interface-ifd-name" unit "\$junos-interface-unit"]** hierarchy level affects how you configure encapsulation at the **[edit interfaces *interface-name*]** hierarchy level.

[Table 8 on page 84](#) provides the valid encapsulation combinations for both dynamic profiles and physical interfaces in the Layer 2 wholesale network.

Table 8: Encapsulation Combinations for Layer 2 Wholesale Interfaces

Dynamic Profile Encapsulation	Physical Interface Encapsulation	Usage Notes
vlan-vpls	vlan-vpls	Using the vlan-vpls encapsulation type in both the dynamic profile and when configuring the physical interface limits the VLAN ID value to a number greater than or equal to 512.
vlan-vpls	flexible-ethernet-services	Using the flexible-ethernet-services encapsulation type removes any VLAN ID value limitation.
vlan-vpls	extended-vlan-vpls	The extended-vlan-vpls encapsulation type can support multiple TPIDs. Using this encapsulation type removes any VLAN ID value limitation.
No encapsulation type	extended-vlan-vpls	The extended-vlan-vpls encapsulation type can support multiple TPIDs. Using this encapsulation type removes any VLAN ID value limitation.

To configure encapsulation for Layer 2 wholesale VLAN interfaces:

1. (Optional) Define the VLAN encapsulation for the dynamic interfaces.

```
[edit dynamic-profiles Subscriber_Profile_Retail1 interfaces "$junos-interface-ifd-name"
 unit "$junos-interface-unit"]
user@host# set encapsulation encapsulation-type
```

2. Specify the encapsulation type for the physical VLAN interface.

```
[edit interfaces ge-2/3/0]
user@host# edit encapsulation encapsulation-type
```



NOTE: If you choose not to specify an encapsulation for the logical interface, you must specify **extended-vlan-vpls** encapsulation for the physical interface.

Related Documentation

- [Configuring a Retail Dynamic Profile for Use in the Layer 2 Wholesale Solution on page 79](#)
- [Configuring VLAN Interfaces for the Layer 2 Wholesale Solution on page 82](#)

Configuring NNI ISP-Facing Interfaces for the Layer 2 Wholesale Solution

You must configure separate, ISP-facing interfaces on each NNI ISP-facing router that connect to individual retailer ISP access routers in the Layer 2 Wholesale solution.



NOTE: On the network-to-network (NNI) or egress interfaces of provider edge (PE) routers, you cannot configure the inner-range *vid1—vid2* option with the *vlan-tags* statement for ISP-facing interfaces.

To configure an NNI ISP-facing interface:

1. Access the physical interface that you want to use to access the retailer ISP network.

```
[edit interfaces]
user@host# edit interfaces ge-1/1/0
```

2. Specify the encapsulation type for the VLAN interfaces.

```
[edit interfaces ge-1/1/0]
user@host# edit encapsulation ethernet-vpls
```

3. Specify the interface unit that you want ISP clients to use.

```
[edit interfaces ge-1/1/0]
user@host# edit unit 0
```

4. Repeat these steps for any other NNI ISP-facing interfaces that you want to use. In this example, you must also configure interface **ge-2/2/0.0**.

Related Documentation

- [Configuring Direct ISP-Facing Interfaces for the Layer 2 Wholesale Solution on page 85](#)
- [Configuring Separate Access Routing Instances for Layer 2 Wholesale Service Retailers on page 86](#)

Configuring Direct ISP-Facing Interfaces for the Layer 2 Wholesale Solution

When connecting a subscriber access router directly to an ISP access router, you must define any ISP-facing interfaces that connect to the retailer ISP access routers as core-facing interfaces.

To configure a direct ISP-facing interface:

1. Access the physical interface that you want to use to access the retailer ISP network.

```
[edit interfaces]
user@host# edit interfaces ge-1/1/0
```

2. Specify the encapsulation type for the VLAN interfaces.

```
[edit interfaces ge-1/1/0]
user@host# edit encapsulation ethernet-vpls
```

3. Specify the interface unit that you want ISP clients to use.

```
[edit interfaces ge-1/1/0]
```

```
user@host# edit unit 1
```

4. Specify the unit family.

```
[edit interfaces ge-1/1/0 unit 1]  
user@host# set family vpls
```

5. Define the interface as core-facing to ensure that the network does not improperly treat the interface as a client interface..

```
[edit interfaces ge-1/1/0 unit 1 family vpls]  
user@host# set core-facing
```

6. Repeat steps for any other direct ISP-facing interfaces that you want to use..

Related Documentation

- [Configuring NNI ISP-Facing Interfaces for the Layer 2 Wholesale Solution on page 84](#)
- [Configuring Separate Access Routing Instances for Layer 2 Wholesale Service Retailers on page 86](#)

Configuring Separate Access Routing Instances for Layer 2 Wholesale Service Retailers

As the owner of the system, the wholesaler uses the default routing instance. You must create separate routing instances for each individual retailer to keep routing information for individual retailers separate and to define any servers and forwarding options specific to each retailer.

When creating separate routing instances, it is important to understand the role that the router plays in the Layer 2 Wholesale network and specify that role (either access or NNI) in the routing instance configuration. If the router connects directly to an ISP network (or ISP-controlled device), you must configure the routing instances as an NNI routing instance. See “[Configuring Separate NNI Routing Instances for Layer 2 Wholesale Service Retailers](#)” on page 89.

To define an access retailer routing instance:

1. Create the retailer routing instance.

```
[edit]  
user@host# edit routing-instances RetailerInstance1
```

2. Specify the VLAN model that you want the retailer to follow.

```
[edit routing-instances RetailerInstance1]  
user@host# set vlan-model one-to-one
```

3. Specify the role that you want the routing instance to take.

```
[edit routing-instances RetailerInstance1]  
user@host# set instance-role access
```

4. Specify the routing instance type for the retailer.

```
[edit routing-instances RetailerInstance1]  
user@host# set instance-type l2backhaul-vpn
```

5. Specify the access interface for the retailer.

```
[edit routing-instances RetailerInstance1]  
user@host# set interface ge-2/3/0.0
```

6. Specify that access ports in this VLAN domain do not forward packets to each other.

```
[edit routing-instances RetailerInstance1]  
user@host# set no-local-switching
```

7. Specify a unique identifier attached to a route that enables you to distinguish to which VPN the route belongs.

```
[edit routing-instances RetailerInstance1]  
user@host# set route-distinguisher 10.10.1.1
```

8. (Optional) Specify a VRF target community.

```
[edit routing-instances RetailerInstance1]  
user@host# set vrf-target target:100:1
```



NOTE: The purpose of the vrf-target statement is to simplify the configuration by allowing you to configure most statements at the [edit routing-instances] hierarchy level.

9. Define the VPLS protocol for the routing instance.

- a. Access the routing instance **protocols** hierarchy.

```
[edit routing-instances RetailerInstance1]  
user@host# edit protocols
```

- b. Enable VPLS on the routing instance.

```
[edit routing-instances RetailerInstance1 protocols]  
user@host# edit vpls
```

- c. Specify the maximum number of sites allowed for the VPLS domain.

```
[edit routing-instances RetailerInstance1 protocols vpls]  
user@host# set site-range 10
```

- d. Specify the size of the VPLS MAC address table for the routing instance.

```
[edit routing-instances RetailerInstance1 protocols vpls]  
user@host# set mac-table-size 6000
```

- e. Specify the maximum number of MAC addresses that can be learned by the VPLS routing instance.

```
[edit routing-instances RetailerInstance1 protocols vpls]  
user@host# set interface-mac-limit 2000
```

- f. (Optional) Specify the **no-tunnel-services** statement if the router does not have a Tunnel Services PIC.

```
[edit routing-instances RetailerInstance1 protocols vpls]  
user@host# set no-tunnel-services
```

- g. Specify a site name.

```
[edit routing-instances RetailerInstance1 protocols vpls]  
user@host# set site A-PE
```

- h. Specify a site identifier.

```
[edit routing-instances RetailerInstance1 protocols vpls site A-PE]  
user@host# set site-identifier 1
```

10. Repeat this procedure for other retailers. In this example, you must configure a routing instance for Retailer 2.

**Related
Documentation**

- [Configuring VPLS Routing Instances](#)
- [Configuring NNI ISP-Facing Interfaces for the Layer 2 Wholesale Solution on page 84](#)
- [Configuring Separate NNI Routing Instances for Layer 2 Wholesale Service Retailers on page 89](#)

Configuring Separate NNI Routing Instances for Layer 2 Wholesale Service Retailers

As the owner of the system, the wholesaler uses the default routing instance. You must create separate routing instances for each individual retailer to keep routing information for individual retailers separate and to define any servers and forwarding options specific to each retailer.

When creating separate routing instances, it is important to understand the role that the router plays in the Layer 2 Wholesale network and specify that role (either access or NNI) in the routing instance configuration. If the router connects to the access portion of the network (for example, to an MSAN device), you must configure the routing instances as an access routing instance. See [“Configuring Separate Access Routing Instances for Layer 2 Wholesale Service Retailers”](#) on page 86.

To define a retailer routing instance:

1. Create the retailer routing instance.

```
[edit]
user@host# edit routing-instances RetailerInstance1
```

2. Specify the VLAN model that you want the retailer to follow.

```
[edit routing-instances RetailerInstance1]
user@host# set vlan-model one-to-one
```

3. Specify the role that you want the routing instance to take.

```
[edit routing-instances RetailerInstance1]
user@host# set instance-role nni
```

4. Specify the routing instance type for the retailer.

```
[edit routing-instances RetailerInstance1]
user@host# set instance-type l2backhaul-vpn
```

5. Define the NNI ISP-facing interface for this retailer.

```
[edit routing-instances RetailerInstance1]
user@host# set interface ge-1/1/0.0
```

6. Specify that access ports in this VLAN domain do not forward packets to each other.

```
[edit routing-instances RetailerInstance1]
user@host# set no-local-switching
```

7. Specify a unique identifier attached to a route that enables you to distinguish to which VPN the route belongs.

```
[edit routing-instances RetailerInstance1]
user@host# set route-distinguisher 10.10.10.1:1
```

8. (Optional) Specify a VRF target community.

```
[edit routing-instances RetailerInstance1]
user@host# set vrf-target target:100:1
```



NOTE: The purpose of the `vrf-target` statement is to simplify the configuration by allowing you to configure most statements at the `[edit routing-instances]` hierarchy level.

9. Define the VPLS protocol for the routing instance.

- a. Access the routing instance **protocols** hierarchy.

```
[edit routing-instances RetailerInstance1]
user@host# edit protocols
```

- b. Enable VPLS on the routing instance.

```
[edit routing-instances RetailerInstance1 protocols]
user@host# edit vpls
```

- c. Specify the maximum number of sites allowed for the VPLS domain.

```
[edit routing-instances RetailerInstance1 protocols vpls]
user@host# set site-range 1000
```

- d. (Optional) Specify the **no-tunnel-services** statement if the router does not have a Tunnel Services PIC.

```
[edit routing-instances RetailerInstance1 protocols vpls]
user@host# set no-tunnel-services
```

- e. Specify a site name.

```
[edit routing-instances RetailerInstance1 protocols vpls]
user@host# set site A-PE
```

- f. Specify a site identifier.

```
[edit routing-instances RetailerInstance1 protocols vpls site A-PE]
user@host# set site-identifier 1
```

- g. Define the connectivity of the VPLS routing instance as **permanent** to keep the VPLS connection up until specifically taken down.

```
[edit routing-instances RetailerInstance1 protocols vpls]
user@host# set connectivity-type permanent
```

10. Repeat this procedure for other retailers.

- Related Documentation**
- [Configuring VPLS Routing Instances](#)
 - [Configuring VLAN Interfaces for the Layer 2 Wholesale Solution on page 82](#)
 - [Configuring Separate Access Routing Instances for Layer 2 Wholesale Service Retailers on page 86](#)

Configuring Access Components for the Layer 2 Wholesale Network Solution

When configuring a wholesale network, you must configure several components globally. This configuration provides access to RADIUS servers (if used) that you want the wholesaler and any configured retailers to use globally. The access configuration includes the following general steps:

- [Configuring RADIUS Server Access on page 91](#)
- [Configuring a Layer 2 Wholesaler Access Profile on page 91](#)

Configuring RADIUS Server Access

You can globally define any RADIUS servers in your network that either the wholesale access profile or retailer access profile can use. After you define the global RADIUS servers, you can specify specific RADIUS servers within individual access profiles.

To define RADIUS servers for profile access:

1. Access the **[edit access radius-server]** hierarchy level.

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

2. Specify the address and secret for any RADIUS servers in the network.

```
[edit access radius-server]
user@host# set 192.168.10.1 secret $ABC123$ABC123$ABC123
user@host# set 10.10.10.1 secret $ABC123$ABC123
```

Configuring a Layer 2 Wholesaler Access Profile

You must define the network and interface over which you want subscribers to initially access the network with a wholesale access profile. When a subscriber attempts to access the network, the access profile provides initial access information including authentication and accounting values that the router uses for the accessing subscriber.

To define a wholesale access profile:

1. Create the wholesale access profile.

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

2. Specify the authentication methods for the profile and the order in which they are used.

```
[edit access profile AccessProfile]
user@host# set authentication-order radius password
```

3. Specify that you want to configure RADIUS support.

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

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

```
[edit access profile AccessProfile radius]
user@host# set authentication-server 10.10.10.1
```

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

```
[edit access profile AccessProfile radius]
user@host# set accounting-server 10.10.10.1
```

6. Configure any desired options for the RADIUS server.

See [Configuring RADIUS Server Options for Subscriber Access](#).

7. Configure subscriber accounting (RADIUS accounting).

See [Configuring Per-Subscriber Session Accounting](#).

Example: Retailer Dynamic Profile for a Layer 2 Wholesale Network

```
dynamic-profiles {
  Subscriber_Profile_Retail {
    routing-instances {
      "$junos-routing-instance" {
        interface "$junos-interface-name";
      }
    }
    interfaces {
      "$junos-interface-ifd-name" {
        unit "$junos-interface-unit" {
          encapsulation vlan-vpls;
          vlan-tags outer "$junos-stacked-vlan-id" inner "$junos-vlan-id";
          input-vlan-map {
            swap;
            vlan-id "$junos-vlan-map-id";
          }
          output-vlan-map swap;
          family vpls;
        }
      }
    }
  }
}
```

Related Documentation

- [Layer 2 and Layer 3 Wholesale Overview on page 3](#)

- [Layer 2 Wholesale Network Topology Overview on page 77](#)
- [Configuring a Retail Dynamic Profile for Use in the Layer 2 Wholesale Solution on page 79](#)

Example: Access Interface for a Layer 2 Wholesale Network

```

interfaces {
  ge-2/3/0 {
    flexible-vlan-tagging;
    auto-configure {
      stacked-vlan-ranges {
        dynamic-profile Subscriber_Profile_Retail1 {
          accept any;
          ranges {
            any,any;
          }
        }
      }
      access-profile AccessProfile;
    }
  }
  encapsulation flexible-ethernet-services;
}

```

Related Documentation

- [Layer 2 and Layer 3 Wholesale Overview on page 3](#)
- [Layer 2 Wholesale Network Topology Overview on page 77](#)
- [Configuring VLAN Interfaces for the Layer 2 Wholesale Solution on page 82](#)

Example: Retailer Access Routing Instances for a Layer 2 Wholesale Network

You need to create a routing instance for each retailer to keep routing information for different retailers separate and to define servers and forwarding options specific to each retailer.

There are two types of routing instances that you can create: access or NNI. The following code snippets show how to configure separate access routing instances for two retailers: Retailer_Instance1 and Retailer_Instance2.

```

routing-instances {
  Retailer_Instance1 {
    vlan-model one-to-one;
    instance-role access;
    instance-type l2backhaul-vpn;
    interface ge-1/1/0.0
    no-local-switching;
    route-distinguisher 10.10.1.1:1;
    vrf-target target:100:1;
    protocols {
      vpls {
        site-range 10;
      }
    }
  }
}

```

```
        mac-table-size {
            6000;
        }
        interface-mac-limit {
            2000;
        }
        no-tunnel-services;
        site A-PE {
            site-identifier 1;
        }
    }
}
Retailer_Instance2 {
    vlan-model one-to-one;
    instance-role access;
    instance-type l2backhaul-vpn;
    interface ge-2/2/0.0
    no-local-switching;
    route-distinguisher 10.10.1.1:2;
    vrf-target target:300:1;
    protocols {
        vpls {
            site-range 1000;
            no-tunnel-services;
            site A-PE {
                site-identifier 1;
            }
        }
    }
}
```

- Related Documentation**
- [Layer 2 and Layer 3 Wholesale Overview on page 3](#)
 - [Layer 2 Wholesale Network Topology Overview on page 77](#)
 - [Configuring Separate Access Routing Instances for Layer 2 Wholesale Service Retailers on page 86](#)

Example: Retailer NNI ISP-Facing Interfaces for a Layer 2 Wholesale Network

```
interfaces {
    ge-1/1/0 {
        description Retailer 1 NNI ISP-facing interface;
        encapsulation ethernet-vpls;
        unit 0 {
        }
    }
    interfaces {
        ge-2/2/0 {
            description Retailer 2 NNI ISP-facing interface;
            encapsulation ethernet-vpls;
            unit 0;
        }
    }
}
```

- Related Documentation**
- [Layer 2 and Layer 3 Wholesale Overview on page 3](#)
 - [Layer 2 Wholesale Network Topology Overview on page 77](#)
 - [Configuring Separate NNI Routing Instances for Layer 2 Wholesale Service Retailers on page 89](#)

Example: Retailer Direct ISP-Facing Interface for a Layer 2 Wholesale Network

```
interfaces {
  ge-1/1/0 {
    description Retailer 1 Direct ISP-facing interface;
    encapsulation ethernet-vpls;
    unit 1
      family vpls {
        core-facing;
      }
    }
  }
```

- Related Documentation**
- [Layer 2 and Layer 3 Wholesale Overview on page 3](#)
 - [Layer 2 Wholesale Network Topology Overview on page 77](#)
 - [Configuring Direct ISP-Facing Interfaces for the Layer 2 Wholesale Solution on page 85](#)

PART 4

Configuring ANCP-Triggered Layer 2 Wholesale Services

- [ANCP-Triggered Layer 2 Wholesale Service Overview on page 99](#)
- [Configuring ANCP-Triggered Layer 2 Wholesale Services on page 165](#)
- [Configuring Flat-File Accounting for Layer 2 Wholesale Services on page 177](#)

CHAPTER 8

ANCP-Triggered Layer 2 Wholesale Service Overview

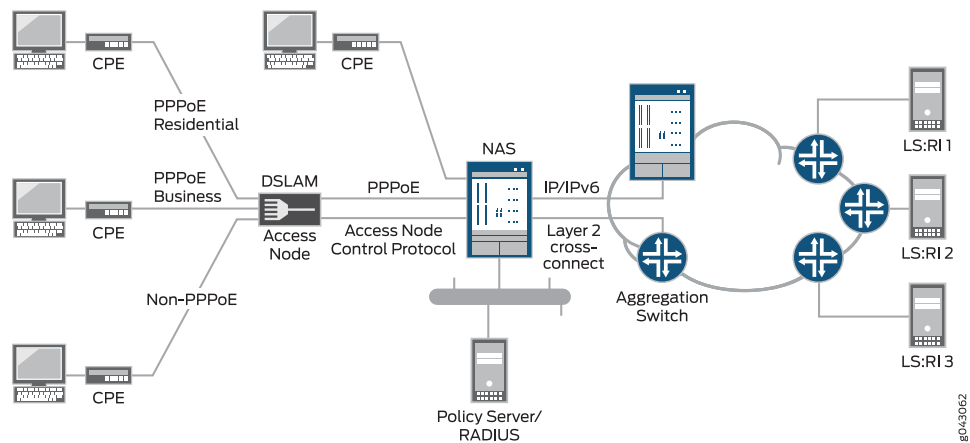
- [Layer 2 Wholesale with ANCP-Triggered VLANs Overview on page 99](#)
- [Junos OS Predefined Variables on page 118](#)
- [Juniper Networks VSAs Supported by the AAA Service Framework on page 143](#)
- [AAA Access Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS on page 154](#)
- [AAA Accounting Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS on page 160](#)

Layer 2 Wholesale with ANCP-Triggered VLANs Overview

The conventional mechanism for triggering autosensed dynamic VLANs relies on access line attributes provided by PPPoE or DHCP traffic in upstream control packets. Packets of a specified type are exceptioned and authorization depends on fields extracted from the packet as specified in a dynamic profile assigned to the autosensed VLAN range. However, for some wholesale networks, the traffic might not be PPPoE or DHCP. In this case, a different mechanism is required.

[Figure 9 on page 100](#) shows a sample topology with direct connections between the wholesaler's BNG and the NSP (network service provider) routers for the retailers. Each retailer's network resides in a dedicated routing instance. The wholesaler uses Layer 2 cross-connects to implement the retail networks with 1:1 autosensed, dynamic VLANs and VLAN tag swapping. Core-facing physical interfaces are dedicated to forwarding subscriber connections to the retailer's router. The traffic for an entire outer VLAN can be wholesaled this way. This direct-connect model supports any combination of wholesaler-owned and wholesaled connections for the entire access-facing VLAN range.

Figure 9: Sample Layer 2 Wholesale Access Topology



A wholesaler providing Layer 2 bitstream access to NSP partners might use this model. Bitstream access enables retailers to offer bidirectional transmission of broadband data and other high-speed services directly to customers across the wholesaler's network. In this topology, the PPPoE residential and subscriber customers are retained by the wholesaler (access provider). The non-PPPoE connections (here multiple connections and subscribers are represented by a single line) can be wholesaled to retail NSPs.

In this model, dynamic VLAN detection and creation for the wholesaled connections do not use in-band control packets. Instead, they rely on an out-of-band protocol, ANCP. ANCP Port Up messages both announce to the ANCP agent on the BNG that new access lines are operational and provide updates about previously announced lines. The messages include ANCP DSL attributes that correspond to Juniper Networks DSL VSAs and DSL Forum VSAs.

Starting in Junos OS Release 16.1R4, you can configure the ANCP agent to trigger the creation of an autosensed VLAN when the ANCP agent receives a Port Up message where the DSL-Line-State attribute has a value of Showtime. The Showtime state indicates that ports are configured, the subscriber is connected, and the DSL modem is online and ready to transfer data. The other possible values of the attribute, Idle and Silent, are ignored for this purpose and are used by the ANCP agent only to update the ANCP session database (SDB).

During VLAN authorization, RADIUS determines which traffic belongs to the access provider's own subscribers and which belongs to the wholesale customer (retail NSP) based on identification of the subscriber's access line by the agent remote identifier.

When the ANCP agent receives the Port Up message, the agent triggers the autoconfiguration daemon, `autoconfd`, to initiate the VLAN detection, authorization, and creation processes. Those processes require the following information:

- Three ANCP subscriber access loop attributes (TLVs) that identify the access line and are conveyed in the Port Up message:
 - Access-Loop-Circuit-ID—Access loop circuit identifier used by the ANCP agent to determine which logical interface or interface set corresponds to the subscriber; corresponds to the Juniper Networks Acc-Loop-Cir-ID VSA (26-110).
 - Access-Loop-Remote-ID—Unique identifier of the access line; corresponds to the Juniper Networks Acc-Loop-Remote-ID VSA (26-182).
 - Access-Aggregation-Circuit-ID-Binary—Identifier that represents the outer VLAN tag that the access node inserts on upstream traffic; corresponds to the Juniper Networks Acc-Aggr-Cir-Id-Bin VSA (26-111).
- The name of the physical interface facing the subscriber. This name derives from the local mapping of an ANCP neighbor to the corresponding subscriber-facing access port.

The Access-Aggregation-Circuit-ID-Binary attribute and the access-facing interface name together provide information equivalent to that used for conventional autosensed VLAN detection.

ANCP Port Down messages indicate that the subscriber access loop is not present or at least is no longer operational. This message triggers the automatic destruction of the dynamic VLAN, regardless of the value of any other ANCP line attribute.

VLAN logical interfaces are created in the default routing-instance unless a nondefault routing instance is provided by local authorization (domain map) or external authorization (RADIUS). Multiple routing instances are required when both access-provider-owned and wholesaled connections are supported at the same time. One routing instance is required for the access provider's own subscribers. An additional routing instance is required for each retail NSP. Consequently, the routing-instance has to be specified when the VLAN is authorized. The RADIUS-based VLAN authorization process determines whether the subscriber access-loop identified by the attributes in the Port Up message is wholesaled to a partner NSP—and therefore maintained as a unique routing-instance—or managed as a subscriber owned by the access provider.

- [RADIUS Authorization for ANCP-Triggered VLANs on page 102](#)
- [Instantiation of an ANCP-Triggered, Autosensed, Dynamic VLAN on page 103](#)
- [Weighted Load Balancing for Subscriber Sessions over Eligible Core-Facing Physical Interfaces on page 104](#)
- [RADIUS Interim Accounting Updates on page 105](#)
- [Removal of the Layer 2 Wholesale Service on page 106](#)
- [Interactions Between In-Band and Out-of-Band VLAN Autosensing on page 107](#)
- [Migration of Subscriber Ownership from Wholesaler to Retailer on page 109](#)
- [Migration of Subscriber Ownership from Retailer to Wholesaler on page 109](#)

- [Migration of Subscriber Ownership Between Retailers on page 110](#)
- [Modification of the Access Line Identifier or Port VLAN Identifier on page 111](#)
- [Disconnecting PPPoE Sessions and Automatically Attempting Reconnection as Layer 2 Wholesale Sessions on page 112](#)
- [Consequences of a State Transition in the Access-Facing Physical Interface on page 113](#)
- [Consequences of a State Transition from Up to Down in the Core-Facing Physical Interface on page 114](#)
- [Consequences of a State Transition from Down to Up in the Core-Facing Physical Interface on page 116](#)
- [Loss of ANCP TCP Adjacency on page 116](#)

RADIUS Authorization for ANCP-Triggered VLANs

When a subscriber logs in, the Access-Request message that is sent to the RADIUS server includes a username and optionally a password generated locally on the router. You can configure the router to create a unique username with the value of ANCP TLVs—Access-Loop-Circuit-ID, Access-Loop-Remote-Id, or both—as received in the ANCP Port Up message from the access node. Alternatively, if you configure the router to convey ANCP-sourced access loop attributes as Juniper Networks VSAs—in this case Acc-Loop-Cir-Id (26-110) and Acc-Loop-Remote-Id (26-182)—then the Access-Request message includes sufficient unique access line information for the RADIUS server to determine whether the access loop is wholesaled to a retailer or retained for the wholesaler.

The RADIUS server responds to the Access-Request with one of the following messages:

- **Access-Accept**—In this case, the VLAN triggered by the Port Up message is wholesaled to a retail NSP. Authorization is similar to that for PPPoE sessions. The Access-Accept includes the Virtual-Router VSA (26-1) with a value that corresponds to the NSP's unique, nondefault routing instance. The message can optionally include client services, such as attributes for parameterized CoS, firewall filters and policies for the logical interface, and Layer 2 service activations.
- **Access-Reject**—In this case, either the VLAN triggered by the Port Up message is one of the wholesaler's own subscribers or RADIUS refuses to grant access to the network. In either case, the VLAN entry is removed from the ANCP SDB. Unless a Port Down message is received first, the router ignores subsequent Port Up messages for this subscriber. However, conventional dynamic stacked VLAN autosensing may be initiated by access protocol negotiation, such as PPPoE.

Instantiation of an ANCP-Triggered, Autosensed, Dynamic VLAN

When the RADIUS server returns an Access-Accept message, the dynamic profile assigned to the autosensed VLAN range is instantiated with the following results:

1. The dynamic VLAN logical interface that represents the Layer 2 wholesale service within the NSP's unique routing instance is created.
2. A core-facing physical interface is selected by a weighted load distribution method from the set of eligible interfaces assigned to the NSP's routing instance. A physical interface is eligible when it is operationally up and has at least one VLAN tag that is available for assignment.
3. The access-facing, autosensed outer VLAN tag is mapped to a unique inner VLAN tag. The outer VLAN tag is derived from the Access-Aggregation-Circuit-ID-Binary TLV carried in the ANCP Port Up message. The inner VLAN tag is allocated from the VLAN range configured for the core-facing physical interface.
4. The inner VLAN tag is swapped with (replaces) the outer VLAN tag when the subscriber traffic is tunneled to the NSP. In the dynamic profile, the inner VLAN tag is provided by the predefined variable, **\$junos-inner-vlan-map-id**.
5. The autosensed outer VLAN tag is swapped with the inner VLAN tag when downstream packets from the NSP (which include the allocated inner VLAN tag) are forwarded to the subscriber.

You can configure each core-facing physical interface with a range of up to 4094 VLAN IDs. The inner VLAN swap range is assigned to the physical interface locally. This means that inner VLAN ranges for different physical interfaces can overlap each other completely, partially, or not at all.

6. Optionally, before the subscriber packets are forwarded to an NSP, the outer VLAN tag protocol identifier (TPID) in the subscriber packets can be swapped with a TPID to meet the requirements of an individual NSP. In this case, the original value is swapped with the NSP TPID for packets forwarded to the subscriber.
7. An additional VLAN tag, the Trunk VLAN ID, is used internally to identify the provisioned core-facing physical interface so that the subscriber traffic can be tunneled to the allocated interface. In the dynamic profile, this ID is provided by the predefined variable, **\$junos-vlan-map-id**. This identifier differentiates among multiple core-facing trunk physical interfaces for the same NSP.
8. Any client services, such as CoS or firewall filters, are applied to the subscriber session. These services are optionally specified in the RADIUS configuration and conveyed in the RADIUS message as Juniper Networks VSAs.

9. The VLAN session is activated after the logical interface is created and configured for the dynamic VLAN session. Session activation initiates a RADIUS Accounting-Start message. Any services that were received from RADIUS during authorization are now activated.
10. After the dynamic VLAN has been created, subsequent ANCP Port Up messages do not cause a re-authorization of the dynamic VLAN session. Instead, when the ANCP agent receives another Port Up message for the access loop, it updates the ANCP SDB with any changes in ANCP attributes.

Weighted Load Balancing for Subscriber Sessions over Eligible Core-Facing Physical Interfaces

The router uses weighted load distribution instead of round-robin distribution to assign Layer 2 wholesale subscriber sessions across multiple core-facing physical interfaces according to the weight of the interface. The weight of an interface correlates with the number of VLAN tags available from the aggregate inner (core-facing) VLAN ID swap ranges on the interface.

How you configure the inner VLAN ID swap ranges determines the relative weights of the interfaces:

- The interface with the highest number of available inner VLAN ID tags has the highest weight.
- The interface with the next-highest number of tags has the next-highest weight, and so on.
- The interface with the lowest number of available tags has the lowest weight.

Using the available inner VLAN ID tags from the swap ranges rather than the aggregate total VLAN tags means that the relative weights of the interfaces are more dynamic. The weighted load distribution mechanism can respond more quickly to subscriber logouts, migration of subscriber ownership from wholesaler to retailer and retailer to wholesaler, core-facing physical interface state transitions (including movement to the remaining eligible core-facing interfaces when an interface state transitions from Up to Down), and failures of any of the core-facing physical interfaces. When an interface recovers (transitions from Down to Up), weighted load distribution generally favors this interface for either pending sessions or for new Layer 2 wholesale sessions that subsequently occur.



NOTE: Core-facing physical interface selection and session distribution are probability based; the load is not strictly distributed according to weight.

With weighted load distribution the router selects interfaces randomly, but the sessions are distributed across interfaces proportionally in relationship to the weight of the interfaces. The router generates a random number within a range equal to the aggregate total of all available inner VLAN ID tags from the swap ranges of all the core-facing physical interfaces. The router then associates part of the range—a pool of numbers—with each interface proportional to the interface's weight. An interface with a higher weight

is associated with a greater portion of the range—a larger pool—than an interface with a lower weight. An interface is selected when the random number is in its associated pool of numbers. The random number is more likely, on average, to be in a larger pool, so an interface with a higher weight (larger pool) is more likely to be selected than an interface with a lower weight (smaller pool).

For example, consider two core-facing physical interfaces, IFD1 and IFD2. Based on the inner VLAN ID swap ranges configured for these two interfaces, IFD1 has 1000 available VLAN tags and IFD2 has only 500 available tags. The subscriber sessions are randomly distributed across the two interfaces based on their relative weights; IFD1 has a higher weight than IFD2. Because IFD1 has twice as many available tags as IFD2, the pool of numbers associated with IFD1 is also twice as many as for IFD2. The random number generated by the router is twice as likely to be in the pool for IFD1 than for IFD2. Consequently, IFD1 is favored 2:1 over IFD2, and subscriber sessions are twice as likely to be assigned to IFD1 as IFD2.

RADIUS Interim Accounting Updates

Interim accounting reports sent to AAA for out-of-band triggered, autosensed dynamic VLANs are supported in the same manner as for conventional autosensed, dynamic, authorized VLANs or client sessions (such as PPPoE sessions). The ANCP agent sends a notification to AAA when it receives an update from the access node. By default, AAA only reports the update to the RADIUS server at the configured interval.

You can configure the ANCP agent so that when it notifies AAA, an interim update Accounting-Request message is immediately sent to the RADIUS server. Immediate interim accounting updates can be sent for an ANCP-triggered dynamic VLAN session only when a change occurs in certain key ANCP attributes for the associated access line that can influence system behavior. To prevent an additional load on the RADIUS server for changes to less critical ANCP attributes, changes to any other ANCP attributes do not trigger immediate accounting-interim-update messages. Instead, those changes are reported in the next scheduled Accounting-Interim-Update message.

Immediate interim accounting updates can be sent for changes to any of the following ANCP attributes for an existing session that corresponds to the access line (based on the Access-Loop-Circuit-ID TLV):

- **Actual-Net-Data-Rate-Upstream**—When the calculated (adjusted) upstream rate results in a change to this attribute, the accounting message reports the attribute in the Juniper Networks Act-Data-Rate-Up VSA (26-113). The calculated speed change is reported in the Upstream-Calculated-QoS-Rate VSA (26-142).
- **Actual-Net-Data-Rate-Downstream**—When the calculated (adjusted) downstream rate results in a change to this attribute, the accounting message reports the attribute in the Juniper Networks Act-Data-Rate-Dn VSA (26-114). The calculated speed change is reported in the Downstream-Calculated-QoS-Rate VSA (26-141).

When the **ancp-speed-change-immediate-update** statement is configured at the **[edit access profile *profile-name* accounting]** hierarchy level, RADIUS immediate interim accounting updates are sent for changes to the Actual-Net-Data-Rate-Upstream and Actual-Net-Data-Rate-Downstream TLVs.

When in addition the **auto-configure-trigger interface *interface-name*** statement is configured at the **[edit protocols ancp neighbor *ip-address*]** hierarchy level, immediate interim accounting updates are also sent for changes to the Access-Loop-Remote-ID and Access-Aggregation-Circuit-ID-Binary TLVs.

For more information about RADIUS immediate interim accounting updates, see *Configuring Immediate Interim Accounting Updates to RADIUS in Response to ANCP Notifications*.

Removal of the Layer 2 Wholesale Service

Any of the following events can remove the logical interface for the dynamic VLAN that represents the access service provided by the Layer 2 wholesaler:

- The receipt of an ANCP Port Down message for the corresponding access loop. The same ANCP attributes that initiate dynamic VLAN creation also initiate dynamic VLAN destruction.

No action is taken for an ANCP Port Down message for which any of the following is true:

- No corresponding subscriber session exists.
- A corresponding subscriber session is present, but is in the process of being deleted.
- The message refers to a conventional autosensed session (which is removed by normal protocol processing).
- An explicit reset of the connection between the ANCP agent and the access node, which triggers a mass logout of all affected dynamic VLAN sessions that support the wholesaled Layer 2 access connections. Sessions for the wholesaler's own subscribers are not affected.
- The deletion or transition to an operational down state of the subscriber-facing physical interface or the core-facing physical interface.
- The loss of adjacency between the neighbor and the ANCP agent.
- The issuance of the **clear auto-configuration interfaces** command to log out the VLAN or the **clear ancp access-loop** command to force a subscriber reset.
- The receipt of a RADIUS-initiated disconnect message.

Any of these events also deactivates the subscriber session to prevent future service activations and issues a RADIUS Accounting-Stop message for related services and for the dynamic VLAN subscriber session. The dynamic profile is then de-instantiated to remove first the dynamic VLAN logical interface and then the corresponding session entry in the VLAN SDB.

You can monitor the number of Layer 2 cross-connected subscriber sessions per port. Use the **show subscribers summary port extensive** command to display the number of subscribers per port by client type (VLAN-OOB) and connection type (Corss-connected). Additionally, the object ID `jnxSubscriberPortL2CrossConnectCounter` in the `jnxSubscriberPortCountTable` in the Juniper Networks enterprise-specific Subscriber MIB

displays the number of Layer 2 cross-connected subscriber sessions on ports that have active sessions.

Interactions Between In-Band and Out-of-Band VLAN Autosensing

The ANCP-triggered Layer 2 wholesale implementation accommodates both subscribers wholesaled to a retailer and subscribers belonging to the wholesaler. Any subscriber session detected on the access-facing physical interface can be one or the other. This means that an overlap exists between the outer tag range for the out-of-band autosensed VLANs and that for in-band, autosensed, stacked VLANs.

Both a PPPoE session and a wholesaled session might be attempted for the same access loop. To avoid the undesirable load on the router and the RADIUS server that can ensue when that happens, the order of session negotiation is determined by the order in which packets (PPPoE PADI or ANCP Port Up message) are received for the same access-facing physical interface and VLAN outer tag.



NOTE: The following sequences assume that the `remove-when-no-subscribers` statement is included at the `[edit interfaces interface-name auto-configure]` hierarchy level for the access-facing physical interface.

The following sequence of events occurs when a PPPoE PADI packet is received on an in-band control channel before an ANCP Port Up message is received on an out-of-band control channel, for the same access loop:

1. The PADI receipt triggers creation of a dynamic stacked VLAN logical interface. PPPoE and PPP negotiation are in progress.
2. The ANCP Port-Up message is received for the access loop. Because the corresponding in-band VLAN logical interface already exists for the same access-facing physical interface and outer VLAN tag, the ANCP agent simply stores the ANCP access line attributes and the name of the physical interface in the session database. The agent takes no other action for the message as long as the PPP session (PPP logical interface and the underlying dynamic VLAN logical interface) is maintained.
3. PPP negotiation terminates due to authentication failure (RADIUS Access-Reject response) or a normal logout, which triggers clean-up of the PPP session and removal of the PPP logical interface.
4. Because the `remove-when-no-subscribers` statement is configured, deletion of the PPP logical interface results in deletion of the dynamic stacked VLAN.
5. The next event depends on whether authorization of the ANCP Port Up message has been attempted before.

- If authorization was not previously attempted:
 - a. A VLAN-OOB SDB session is created and authorization of the access-loop is initiated.
 - b. All exceptioned PPPoE PADI packets received by in-band VLAN auto-sensing are ignored until RADIUS responds to the authorization request.
 - c. The authorization result determines what happens next:
 - If the authorization succeeds (RADIUS returns an Access-Accept message), then a dynamic Layer 2 wholesale logical interface is created within the retailer NSP's routing-instance.
 - If the authorization fails (RADIUS returns an Access-Reject message), then the VLAN-OOB session is cleaned up. Processing resumes for any exceptioned PPPoE PADI packets that are subsequently received by in-band VLAN autosensing.
- If authorization was previously attempted, then no action is taken because the failure of the PPP session negotiation is assumed to be a login failure outside the Layer2 wholesale context. This behavior prevents unnecessary authorization in response to the ANCP Port-Up message every time a PPPoE session terminates and cleans up from a normal subscriber logout.

The following sequence of events occurs when an ANCP Port Up message is received on an out-of-band control channel before a PPPoE PADI packet for an access loop is received on an in-band control channel, both for the same access loop:

1. Receipt of the ANCP Port Up message triggers authorization of the access loop.
2. A PPPoE PADI packet is received. The packet is ignored because authorization is already in progress for the same access-facing physical interface and outer VLAN tag.
3. The authorization result determines what happens next:
 - If authorization succeeds (RADIUS returns an Access-Accept message)—represented by a VLAN-OOB session in the SDB—then dynamic creation of the VLAN logical interface is initiated for a Layer 2 wholesale session. When the interface is created, subsequent PPPoE PADI packets detected by in-band VLAN autosensing are ignored and no longer exceptioned.
 - If authorization fails (RADIUS returns an Access-Reject message), the VLAN-OOB session is cleaned up.
 - a. Receipt of a subsequent PPPoE PADI packet initiates creation of a dynamic stacked VLAN.
 - b. PPPoE and PPP negotiation takes place and events proceed as usual for a conventional, dynamic autosensed VLAN.

Migration of Subscriber Ownership from Wholesaler to Retailer

The wholesaler-owned subscribers are connected by means of dynamic PPPoE interfaces over dynamic VLANs. For each subscriber, the PPPoE session must be disconnected and the corresponding PPP logical interface deleted before ANCP Port Up messages for the same underlying physical interface and VLAN outer tag can serve as out-of-band triggers for dynamic VLAN autosensing.

One approach to migrating from wholesale to retail ownership is to do the following:

1. Update the RADIUS server database so that subscriber authentication for the relevant access lines results in a RADIUS Access-Reject response. This causes subsequent attempts to negotiate PPPoE for the access line to fail.
2. Initiate logout of the dynamic PPPoE sessions; for example, by issuing a RADIUS-initiated disconnect. This triggers cleanup of the PPPoE logical interface and associated services, which includes issuing RADIUS Accounting-Stop messages for the session and active services, as well as removing the dynamic PPPoE logical interface.

If the migration requires swapping out the current CPE device for another, and the PPPoE session is not otherwise gracefully logged out, then turning off the CPE results in a PPP keepalive failure on the router and triggers session logout.

3. Remove the underlying dynamic VLAN logical interface. This occurs automatically when the **remove-when-no-subscribers** statement is included at the **[edit interfaces interface-name auto-configure]** hierarchy level for the access-facing physical interface. Otherwise, issue the **clear auto-configuration interfaces interface-name** command to remove the dynamic VLAN logical interface.
4. Trigger a Port Up notification to initiate dynamic VLAN detection, authorization, and creation by one of the following methods:
 - Power cycle the CPE, with a sufficient delay between turning off and turning back on the device so that a Port Down message is sent followed by a Port Up message and the router is given enough time to detect a keepalive failure indicating loss of the session.
 - Issue a **clear ancp access-loop** command.
 - Issue a **request ancp oam port-up** command.

Migration of Subscriber Ownership from Retailer to Wholesaler

One approach to migrating from retail to wholesale ownership is to do the following:

1. Update the RADIUS server database so that dynamic VLAN authorization for the relevant access lines results in a RADIUS Access-Reject response. Doing this causes subsequent ANCP Port Up messages to be ignored.

2. Initiate logout of the dynamic VLAN sessions supporting the wholesale access service; for example, by issuing a RADIUS-initiated disconnect. Doing this triggers cleanup of the session, which includes issuing RADIUS Accounting-Stop messages for the session, removal of the dynamic VLAN logical interface and active services, and freeing the allocated inner VLAN tag associated with the core-facing physical interface for assignment to a different Layer 2 wholesale subscriber session.

If the migration requires swapping out the current CPE device for another, then turning off the CPE results in an ANCP Port Down message that triggers session logout and cleanup.

3. Allow subscribers to connect to the wholesaler's network using conventional dynamic VLAN autosensing followed by PPPoE and PPP negotiation and creation of PPP logical interfaces.

Migration of Subscriber Ownership Between Retailers

Typically, you migrate access between NSP retailers by triggering a restart of the existing dynamic VLAN session. The restart initiates a logout from the session followed by immediate dynamic VLAN detection, authorization, and creation within the routing-instance corresponding to the new NSP. A restart is a logical Port Down and Port Up sequence for the VLAN's corresponding access loop. You can use any of the following methods to restart a given dynamic VLAN logical interface:

- Initiate a RADIUS Disconnect-Request message or configure your RADIUS server to send the message. The message must have the Acct-Terminate-Cause RADIUS attribute (49) set to a value of 16 (callback). This cause is processed as a disconnect (logout) followed immediately by a reconnect (login) only for dynamic VLANs created by an ANCP Port Up message. Other clients respond to this value with only a disconnect.
- Include the **reconnect** option when you log out subscribers with the **clear network-access aaa subscriber** command. You can specify subscribers by either the session identifier or the username. This option attempts to reconnect a cleared session as a Layer 2 wholesale session when the subscriber session has been fully logged out. This behavior is equivalent to issuing a RADIUS-initiated disconnect that is configured for reconnect; that is, when the message includes Acct-Terminate-Cause (RADIUS attribute 49) with a value of callback (16).
- Trigger a Port Down message followed by a Port UP message by one of the following methods:
 - Power cycle the CPE, with a sufficient delay between turning off and turning back on the device so that a Port Down message is sent followed by a Port Up message and the router is given enough time to detect a keepalive failure indicating loss of the session.
 - Issue a **clear ancp access-loop** command.

Modification of the Access Line Identifier or Port VLAN Identifier

When the line identifier or port VLAN identifier for an access loop is modified, the access node reports the change in a Port Up message to the ANCP agent. The message conveys the line ID in the Access-Loop-Remote-ID TLV and the port VLAN ID in the Access-Aggregation-Circuit-ID-Binary TLV.

The access node should send a Port Down message for the access loop before it modifies any of the identification attributes for an existing session. The Port Down message triggers clean up of the corresponding Layer 2 wholesale session. If the access node does not send a Port Down in this case, then the following behavior has the same effect as inserting the Port Down message that the access node failed to send:

- For a line ID change, the ANCP agent treats the reconfiguration as a logical Port Down message for the access line identified by the previous Access-Loop-Remote-Id, followed by a Port Up message for the access line identified by the new Access-Loop-Remote-Id.
- For a port VLAN ID change, the ANCP agent treats the reconfiguration as a logical Port Down message for the access line identified by the previous Access-Aggregation-Circuit-Id-Binary, followed by a Port Up message for the access line identified by the new Access-Aggregation-Circuit-Id-Binary.

In either case, the ANCP agent notifies the autoconfiguration daemon (autoconfd), which takes the following actions:

1. Logs out the corresponding Layer 2 wholesale session.
2. Sends a RADIUS Accounting-Stop message with the final statistics for the associated service sessions and client session.
3. Removes the dynamic VLAN logical interface.
4. Attempts to reestablish the Layer 2 wholesale session by means of a login sequence, including authentication, creation of the dynamic VLAN logical interface, activation of any services, and if successful, sending RADIUS Accounting-Start messages for the service and client sessions.

You must manually log out any PPPoE session corresponding to the access line with the previous identifiers, even if the access node sends the appropriate Port Down message when the values change.



NOTE: In the case of a change in the port VLAN ID only, autoconfd takes no action to reinitiate the session when a dynamic stacked VLAN or a Layer 2 wholesale session exists with the same access-facing physical interface and outer VLAN tag. You must manually intervene in this case, such as by issuing a `request ancp oam port-up` command to initiate the creation of the Layer 2 wholesale session.



BEST PRACTICE: Because an existing session is not automatically logged out, we recommend that the network operator disconnect the session—for example, by issuing a RADIUS Disconnect-Request message—before modifying any of the access line attributes. Depending on subsequent subscriber login and successful negotiation, a new session with the new identifier may then be created as usual.

Disconnecting PPPoE Sessions and Automatically Attempting Reconnection as Layer 2 Wholesale Sessions

You can use RADIUS-initiated disconnect messages to disconnect and log out existing PPPoE sessions and attempt to reestablish them as Layer 2 wholesale sessions. Use Access-Reject messages to prevent PPPoE subscriber access and attempt a reconnect as a Layer 2 wholesale session. Use this feature when you want to migrate sessions from PPPoE to Layer 2 wholesale. Both the RADIUS-initiated disconnect and Access-Reject message must include Acct-Terminate-Cause (RADIUS attribute 49) with a value of callback (16); callback causes the reconnect attempt. The **remove-when-no-subscribers** statement must be configured on the underlying physical interface.

1. The initial behavior for the messages is the following:
 - Access-Reject message—When a PPPoE PADI is received and a new PPPoE session is requested, RADIUS responds to the Access-Request message with an Access-Reject message. The session is rejected, fully logged out, and the underlying dynamic VLAN logical interface is removed.
 - RADIUS-initiated disconnect message—When a RADIUS-initiated disconnect message is received for an existing PPPoE session, the dynamic PPPoE session is logged out and the underlying dynamic VLAN logical interface is removed.
2. The next action is the same for both messages:
 - If an ANCP Port Up message has been received for the corresponding access line, the router attempts to authorize the access line and create a dynamic Layer 2 wholesale VLAN logical interface in place of the underlying dynamic VLAN logical interface that was removed.
 - If a Port Up message has not been received, then this action is deferred until the message is received.
 - If a PPPoE PADI is received before an ANCP Port Up message, RADIUS responds to the Access-Request for a new PPPoE session with an Access-Reject message. The session is rejected, fully logged out, and the underlying dynamic VLAN logical interface is removed.

If the RADIUS-initiated disconnect or Access-Reject message is received for a non-PPPoE session, such as DHCP, the session is disconnected, but the reconnect request is ignored. No attempt is made to establish a Layer 2 wholesale session.

If the RADIUS-initiated disconnect does not include Acct-Terminate-Cause with a value of callback, PPPoE renegotiation after the disconnect can succeed, but if an ANCP Port

Up message is received for the access line before a PPPoE session is established, then a Layer 2 wholesale session is attempted.

As an alternative to the RADIUS-initiated disconnect, you can manually log out the PPPoE session with the **clear network-access aaa subscriber** command. Specify the subscriber by either username or session ID. When you include the **reconnect** option, it attempts to reconnect the cleared session as a Layer 2 wholesale session when the subscriber session has been fully logged out.

Consequences of a State Transition in the Access-Facing Physical Interface

The following behavior results when the access-facing physical interface state transitions from Up to Down:

- Conventional in-band VLAN autosensing stops for the interface.
- ANCP-sourced Port Up messages for the interface are ignored. Action on new or unprocessed Port Up messages is deferred until the interface transitions to the Up state. If the ANCP connection is in band with the subscriber traffic on the interface, then all ANCP traffic stops; if the outage lasts long enough, the ANCP adjacency is lost.
- All Layer 2 wholesale sessions that are assigned to the interface are treated as if the ANCP agent received a Port Down message for the corresponding access line. Each session is subject to being logged out. Whether a session is logged out depends on the ANCP adjacency loss hold timer. The timer starts running when the ANCP agent detects the state transition to Down. The subscriber continues using the original session if all three of the following occur before the timer expires:
 1. The physical interface comes back up.
 2. The ANCP adjacency is restored.
 3. A Port Up message is received on the interface.

Otherwise, `autoconfd` takes the following actions:

1. Logs out the session.
2. Sends a RADIUS Accounting-Stop message with the final statistics for the associated service sessions and client session.
3. Removes the dynamic VLAN logical interface.

These sessions can be reestablished when the physical interface recovers, unless an ANCP Port Down message is received.

- The autoconfiguration daemon does not automatically delete dynamic, autosensed VLAN logical interfaces. The interfaces for the ANCP-triggered Layer 2 wholesale VLANs are maintained because the assumption is that an outage is short-lived. If the outage is not short-lived, then a subsequent Port Down message brings down the session and removes the interface.

For conventional autosensed dynamic VLANs, the interface is removed only when the **remove-when-no-subscribers** statement is configured on the access-facing physical interface and all references to the VLAN logical interface from a higher logical interface

or session are removed. This mechanism does not apply to the ANCP-triggered Layer 2 wholesale VLANs because they do not have upper session references.

The following behavior results when the access-facing physical interface state transitions from Down to Up:

1. Conventional in-band VLAN autosensing resumes for the interface. PPPoE sessions owned by the access provider that were logged out due to the transition from Up to Down can renegotiate and undergo a full login sequence.
2. Appropriate actions are taken for all ANCP Port Up messages for the interface, including messages that were deferred because of the previous Down state for the interface. If the ANCP connection is in band with the subscriber traffic, then all ANCP traffic resumes.
3. Forwarding resumes for any dynamic, autosensed VLAN logical interfaces that were not deleted when the interface went down.

Deletion of an access-facing physical interface triggers logout and removal of all upper dynamic VLAN logical interfaces and their corresponding sessions.

Consequences of a State Transition from Up to Down in the Core-Facing Physical Interface

The following behavior results when the core-facing physical interface state transitions from Up to Down:

- The core-facing physical interface is no longer eligible for assigning new or pending access lines in this routing instance as based on the original RADIUS authorization.
- All Layer 2 wholesale sessions that are assigned to the interface are treated as if the ANCP agent received a Port Down/Port Up message sequence for the corresponding access line. Each session is subject to being logged out. Whether a session is logged out depends on the ANCP adjacency loss hold timer. The timer starts running when the ANCP agent detects the state transition to Down. The subscriber continues using the original session if all three of the following occur before the timer expires:
 1. The physical interface comes back up.
 2. The ANCP adjacency is restored.
 3. A Port Up message is received on the interface.

Otherwise, autoconfd takes the following actions:

1. Logs out the session.
 2. Removes the session entry from the SDB.
 3. Sends a RADIUS Accounting-Stop message with the final statistics for the associated service sessions and client session.
 4. Removes the dynamic VLAN logical interface.
- Next, autoconfd attempts to migrate the sessions to available connections on any remaining eligible core-facing physical interfaces that are assigned to the same routing instance:

1. The original request is placed on a retry queue.
2. A login sequence is attempted for each session, including authentication, creation of dynamic VLAN logical interfaces, activation of any services, and sending RADIUS Accounting-Start messages for the service and client sessions.
 - If the login sequence is successful, then the request is removed from the retry queue.
 - If the login fails, then the session is logged out, the session entry is removed from the SDB, and the corresponding access line is set to a pending state.

When the available connections are all used—when there are no more available VLAN tags from the configured inner VLAN ID swap ranges—as a result of successful reconnections, no attempt is made to connect any remaining Layer 2 wholesale sessions. Although authentication can succeed, the creation of dynamic VLAN logical interfaces fails during profile instantiation. In this case, the session is out, the session entry is removed from the SDB, and the corresponding access line is set to a pending state.

- The pending access lines that represent these non-migrated sessions can be reestablished if the interface recovers or if additional VLAN connections become available; for example, by a configuration change that either increases the inner VLAN ID swap range for one or more remaining core-facing physical interfaces or adds new core-facing physical interfaces. However, if the ANCP agent receives a Port Down message for a pending access line, the corresponding session is not reestablished.

You can use the **show auto-configuration out-of-band pending** command to display a count of pending access lines per routing instance.



NOTE:

In addition to core-facing physical interface state transitions from Up to Down, these behaviors also apply in the following circumstances:

- A core-facing physical interface is deleted.
- More Layer 2 wholesale sessions are assigned to a routing instance than can be accommodated by the inner VLAN ID swap range configured on the interface assigned to the routing instance.



BEST PRACTICE: We recommend that you use aggregated Ethernet for the core-facing physical interfaces to provide link protection, bandwidth aggregation, or both.

Consequences of a State Transition from Down to Up in the Core-Facing Physical Interface

The following behavior results when the core-facing physical interface state transitions from Down to Up:

- The physical interface is now eligible to assign new Layer 2 wholesale subscriber sessions.
- The ANCP agent notifies the autoconfiguration daemon (autoconfd), which attempts to reestablish the Layer 2 wholesale sessions that correspond to pending access line by initiating a conventional login sequence. This sequence includes authentication, creation of dynamic VLAN logical interfaces, activation of any services, and sending RADIUS Accounting-Start messages for the service and client sessions.
- Pending sessions continue to be reestablished until none are left or an error occurs, typically due to exhaustion of inner VLAN tags from the swap ranges on the interface. In the latter case, the sessions are logged out, the session entry is removed from the SDB, and the access line is set to a pending state.

You can use the **show auto-configuration out-of-band pending** command to display a count of pending access lines per routing instance.

These behaviors also occur in the following cases:

- Additional VLAN connection resources become available, by a configuration change that either increases the inner VLAN ID swap range for one or more remaining core-facing physical interfaces or adds new core-facing physical interfaces. The newly added physical interface must be in the Up state to assume any Layer 2 wholesale sessions.
- A RADIUS-initiated disconnect is received for an existing Layer 2 wholesale session assigned to this routing instance is logged out (disconnect only). For a disconnect with a reconnect qualifier, the affected session is given preference to reconnect over pending access lines.
- You issue the **request auto-configuration reconnect-pending**, **clear ancp access-loop**, or **request ancp oam port-up** command.

Loss of ANCP TCP Adjacency

The ANCP agent can lose its TCP adjacency with a neighbor in any of the following circumstances:

- The access node renegotiates the connection; for example, as a result of losing synchronization. The renegotiation triggers the local state to change from established to not established. The state transitions back to established when the session is successfully renegotiated.
- An end-of-file (EOF) message is received on the socket indicating the adjacency is closed. This can result when the ANCP configuration is deleted on the access node.
- An adjacency keepalive failure occurs. When no response is received for three consecutive polls, the adjacency is declared to be lost.

The ANCP agent treats the loss of adjacency as if it has received a Port Down message for each access loop represented by the ANCP connection. The agent notifies autoconfd, which takes the following actions:

- Logs out all Layer 2 wholesale sessions that were triggered by this ANCP connection.
- Sends a RADIUS Accounting-Stop message with the final statistics for the associated service sessions and client session.
- Removes the dynamic VLAN logical interface.

If the assigned access-facing or core-facing physical interface is in the Down state, any pending sessions that were triggered by this ANCP connection cannot be reestablished when the interface recovers to the Up state.

Dynamic, conventionally auto-sensed VLAN logical interfaces, such as those supporting PPPoE sessions, are not affected by the TCP adjacency loss.

If the adjacency is reestablished, the expected behavior is a complete replay of Port Down and Port Up messages for all associated configured access lines. The Layer 2 wholesale sessions for which the ANCP agent receives Port Up messages are reestablished.

You can mitigate the effects of short-term adjacency losses by configuring an adjacency loss hold time. The timer starts when adjacency is lost. Even though the adjacency is lost, established sessions are maintained while the timer runs unless a Port Down message is received for the corresponding access line.

Any access line that for which the ANCP agent has not received a Port Up message by the time the timer expires is treated as though the agent has received a Port Down message for the line. The ANCP Agent notifies autoconfd, which takes the following actions:

- Logs out all Layer 2 wholesale sessions that correspond to the access line.
- Sends a RADIUS Accounting-Stop message with the final statistics for the associated service sessions and client session.
- Removes the dynamic VLAN logical interface.

Port Up messages received after the timer expires repopulate the SDB access line table and reestablish the Layer 2 wholesale sessions

The adjacency loss hold timer serves the following purposes:

- Dampens the effect of adjacency loss of short duration thereby maintaining existing Layer 2 wholesale sessions.
- Detects the removal of an access line configuration on the access node. For example, in some circumstances you may want to remove the configuration of an access line on a neighbor. You first disconnect the ANCP session between a neighbor and the BNG, remove the configuration on the neighbor, and then restore the ANCP connection with the BNG. The neighbor does not issue a Port Down message. If the adjacency-loss hold-timer is configured, the ANCP agent detects an access line for which it has not

received a Port Up or Port Down message, and consequently triggers logout and removal of the corresponding Layer 2-wholesale session.



NOTE: When you deactivate the ANCP protocol, the router does not perform a commit check to determine whether any ANCP or L2-BSA subscribers are present (active or inactive). Any subscribers that are active at the time of deactivation remain active.

Release History Table

Release	Description
16.1R4	Starting in Junos OS Release 16.1R4, you can configure the ANCP agent to trigger the creation of an autosensed VLAN when the ANCP agent receives a Port Up message where the DSL-Line-State attribute has a value of Showtime.

Related Documentation

- [Configuring Out-of-Band ANCP Messages to Trigger Dynamic VLAN Instantiation on page 169](#)
- [Configuring the ANCP Agent for ANCP-Triggered, Autosensed Dynamic VLANs on page 167](#)
- [Configuring the ANCP Agent](#)
- [ANCP and the ANCP Agent Overview](#)

Junos OS Predefined Variables

Junos OS contains many predefined variables. The dynamic profile obtains and replaces values for these variables from an incoming client data packet and configuration (local and RADIUS). These variables are predefined—you use them in the body of a dynamic profile without first having to define the variables at the **[dynamic-profiles profile-name variables]** hierarchy level. [Table 9 on page 118](#) provides a list of predefined variables, their descriptions, and where in the Junos OS hierarchy you can configure them.

Table 9: Junos OS Predefined Variables and Definitions

Variable	Definition
Access and Access-Internal Routes	
\$junos-framed-route-cost	Cost metric of an IPv4 access route. You specify this variable at the [edit dynamic-profiles profile-name routing-options access route address] hierarchy level for the metric statement.
\$junos-framed-route-distance	Distance of an IPv4 access route. You specify this variable at the [edit dynamic-profiles profile-name routing-options access route address] hierarchy level for the preference statement.

Table 9: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
<code>\$junos-framed-route-ip-address-prefix</code>	Route prefix of an IPv4 access route. You specify this variable at the [edit dynamic-profiles <i>profile-name</i> routing-options access] hierarchy level for the route statement.
<code>\$junos-framed-route-ipv6-address-prefix</code>	Route prefix of an IPv6 access route. You specify this variable at the [edit dynamic-profiles <i>profile-name</i> routing-options access] hierarchy level for the route statement.
<code>\$junos-framed-route-ipv6-cost</code>	Cost metric of an IPv6 access route. You specify this variable with the metric statement at the [edit dynamic-profiles <i>profile-name</i> routing-instances \$junos-routing-instance routing-options rib \$junos-ipv6-rib access route \$junos-framed-route-ipv6-address-prefix] hierarchy level.
<code>\$junos-framed-route-ipv6-distance</code>	Distance of an IPv6 access route. You specify this variable with the preference statement at the [edit dynamic-profiles <i>profile-name</i> routing-instances \$junos-routing-instance routing-options rib \$junos-ipv6-rib access route \$junos-framed-route-ipv6-address-prefix] hierarchy level.
<code>\$junos-framed-route-ipv6-nexthop</code>	IPv6 next-hop address of an access route. You specify this variable at the [edit dynamic-profiles <i>profile-name</i> routing-options access route <i>address</i>] hierarchy level for the next-hop statement.
<code>\$junos-framed-route-ipv6-tag</code>	Tag value of an IPv6 access route. You specify this variable with the tag statement at the [edit dynamic-profiles <i>profile-name</i> routing-instances \$junos-routing-instance routing-options rib \$junos-ipv6-rib access route \$junos-framed-route-ipv6-address-prefix] hierarchy level.
<code>\$junos-framed-route-nexthop</code>	IPv4 next-hop address of an access route. You specify this variable at the [edit dynamic-profiles <i>profile-name</i> routing-options access route <i>address</i>] hierarchy level for the next-hop statement.
<code>\$junos-framed-route-tag</code>	Tag value of an IPv4 access route. You specify this variable at the [edit dynamic-profiles <i>profile-name</i> routing-options access route <i>address</i>] hierarchy level for the tag statement.

Table 9: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
\$junos-interface-name	<p>Logical interface of an access-internal route. DHCP or PPP supplies this information when the subscriber logs in. You specify this variable at the [edit dynamic-profiles <i>profile-name</i> routing-options access-internal route address] hierarchy level for the qualified-next-hop statement.</p> <p>This variable is also used for creating dynamic IP demux interfaces.</p>
\$junos-ipv6-rib	<p>Routing table for an IPv6 access route. You specify this variable with the rib statement at the [edit dynamic-profiles <i>profile-name</i> routing-instances \$junos-routing-instance routing-options] hierarchy level.</p> <p>You can use this variable to specify a nondefault routing instance for the route.</p>
\$junos-subscriber-ip-address	<p>IP address of a subscriber identified in an access-internal route. You specify this variable at the [edit dynamic-profiles <i>profile-name</i> routing-options access-internal] hierarchy level for the route statement.</p> <p>This variable is also used for creating dynamic IP demux interfaces.</p>
\$junos-subscriber-mac-address	<p>MAC address for a subscriber identified in an access-internal route. You specify this variable at the [edit dynamic-profiles <i>profile-name</i> routing-options access-internal route address qualified-next hop underlying-interface] hierarchy level for the mac-address statement.</p>
Dynamic Protocols	
\$junos-igmp-access-group-name	Specifies the access list to use for the source (S) filter.
\$junos-igmp-access-source-group-name	Specifies the access list to use for the source-group (S,G) filter.
\$junos-igmp-enable	<p>Ensures that IGMP is not disabled on the interface by an AAA-based authentication and management method (for example, RADIUS). You specify this variable at the [dynamic-profiles <i>profile-name</i> protocols igmp] hierarchy level for the interface statement.</p>

Table 9: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
<code>\$junos-igmp-immediate-leave</code>	Enables IGMP immediate leave on the interface. You specify this variable at the [dynamic-profiles profile-name protocols igmp] hierarchy level for the interface statement.
<code>\$junos-igmp-version</code>	IGMP version configured in a client access profile. Junos OS obtains this information from the RADIUS server when a subscriber accesses the router. The version is applied to the accessing subscriber when the profile is instantiated. You specify this variable at the [dynamic-profiles profile-name protocols igmp] hierarchy level for the interface statement.
<code>\$junos-interface-name</code>	<p>Name of the dynamic interface to which the subscriber access client connects. Its use is in dynamically enabling IGMP on the subscriber interface. You specify this variable at the [dynamic-profiles profile-name protocols igmp] hierarchy level for the interface statement.</p> <p>The interface name is derived from concatenating the <code>\$junos-interface-afd-name</code> and the <code>\$junos-underlying-interface-unit</code> variables obtained when a subscriber is created dynamically at the [dynamic-profiles profile-name interfaces] hierarchy level.</p>
<code>\$junos-ipv6-ndra-prefix</code>	Prefix value for the router advertisement interface. Junos OS obtains this information from the RADIUS server when a subscriber accesses the router. The prefix value is applied to the accessing subscriber when the profile is instantiated. You specify this variable at the [dynamic-profiles profile-name protocols router-advertisement interface \$junos-interface-name] hierarchy level.
<code>\$junos-mld-access-group-name</code>	Specifies the access list to use for the group (G) filter.
<code>\$junos-mld-access-source-group-name</code>	Specifies the access list to use for the source-group (S,G) filter.
<code>\$junos-mld-enable</code>	Ensures that MLD is not disabled on the interface by an AAA-based authentication and management method (for example, RADIUS). You specify this variable at the [dynamic-profiles profile-name protocols mld] hierarchy level for the interface statement.

Table 9: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
\$junos-mld-immediate-leave	Enables MLD immediate leave on the interface. You specify this variable at the [dynamic-profiles profile-name protocols mld] hierarchy level for the interface statement.
\$junos-mld-version	MLD version configured in a client access profile. Junos OS obtains this information from the RADIUS server when a subscriber accesses the router. The version is applied to the accessing subscriber when the profile is instantiated. You specify this variable at the [dynamic-profiles profile-name protocols mld] hierarchy level for the interface statement.
Dynamic CoS — Traffic-Control Profile Parameters	
\$junos-cos-adjust-minimum	<p>Minimum adjusted shaping rate configured in a traffic-control profile in a dynamic profile. Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the adjust-minimum statement at the [edit dynamic-profiles profile-name class-of-service traffic-control-profiles profile-name] hierarchy level.</p>
\$junos-cos-byte-adjust	<p>Byte adjustment value configured in a traffic-control profile in a dynamic profile. Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the bytes option with the overhead-accounting statement at the [edit dynamic-profiles profile-name class-of-service traffic-control-profiles profile-name] hierarchy level.</p>
\$junos-cos-byte-adjust-cell	<p>Overhead bytes when downstream ATM traffic is in cell-mode.</p> <p>NOTE: Do not configure the \$junos-cos-byte-adjust-cell variable when the \$junos-cos-byte-adjust variable is configured.</p>

Table 9: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
\$junos-cos-byte-adjust-frame	<p>Overhead bytes when downstream ATM traffic is in frame-mode.</p> <p>NOTE: Do not configure the \$junos-cos-byte-adjust-frame variable when the \$junos-cos-byte-adjust variable is configured.</p>
\$junos-cos-delay-buffer-rate	<p>Delay-buffer rate configured in a traffic-control profile in a dynamic profile. Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the delay-buffer-rate statement at the [edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>] hierarchy level.</p>
\$junos-cos-excess-rate	<p>Excess rate configured in a traffic-control profile in a dynamic profile. Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the excess-rate statement at the [edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>] hierarchy level.</p>
\$junos-cos-excess-rate-high	<p>Rate configured for excess high-priority traffic in a traffic-control profile in a dynamic profile. Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the excess-rate-high statement at the [edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>] hierarchy level.</p>

Table 9: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
\$junos-cos-excess-rate-low	<p>Rate configured for excesslow-priority traffic in a traffic-control profile in a dynamic profile for subscriber access. Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the excess-rate-low statement at the [edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>] hierarchy level.</p>
\$junos-cos-guaranteed-rate	<p>Guaranteed rate configured in a traffic-control profile in a dynamic profile Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the guaranteed-rate statement at the [edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>] hierarchy level.</p>
\$junos-cos-guaranteed-rate-burst	<p>Burst size for the guaranteed rate that is configured in a traffic-control profile in a dynamic profile. Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable with the burst-size option in the guaranteed-rate statement at the [edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>] hierarchy level.</p>

Table 9: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
\$junos-cos-scheduler-map	<p>Scheduler-map name configured in a traffic-control profile in a dynamic profile. Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the scheduler-map statement at the [edit dynamic-profiles profile-name class-of-service traffic-control-profiles profile-name] hierarchy level.</p> <p>NOTE: The scheduler map can be defined dynamically (at the [edit dynamic-profiles profile-name class-of-service scheduler-maps] hierarchy level) or statically (at the [edit class-of-service scheduler-maps] hierarchy level).</p>
\$junos-cos-shaping-mode	<p>Shaping mode configured in a traffic-control profile in a dynamic profile. Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the overhead-accounting statement at the [edit dynamic-profiles profile-name class-of-service traffic-control-profiles profile-name] hierarchy level.</p>
\$junos-cos-shaping-rate	<p>Shaping rate configured in a traffic-control profile in a dynamic profile. Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the shaping-rate statement at the [edit dynamic-profiles profile-name class-of-service traffic-control-profiles profile-name] hierarchy level.</p>

Table 9: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
\$junos-cos-shaping-rate-burst	<p>Burst size for the shaping rate configured in a traffic-control profile in a dynamic profile. Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable with the burst-size option in the shaping-rate statement at the [edit dynamic-profiles <i>profile-name</i> class-of-service traffic-control-profiles <i>profile-name</i>] hierarchy level.</p>
\$junos-cos-shaping-rate-excess-high	Shaping rate configured for excess high-priority traffic in a traffic-control profile for a dynamic interface set or dynamic ACI interface set at a household level. Specifying this variable in a traffic-control profile for a dynamic subscriber interface is prohibited.
\$junos-cos-shaping-rate-excess-high-burst	Shaping rate burst size configured for excess high-priority traffic in a traffic-control profile for a dynamic interface set or dynamic ACI interface set at a household level. Specifying this variable in a traffic-control profile for a dynamic subscriber interface is prohibited.
\$junos-cos-shaping-rate-excess-low	Shaping rate configured for excess low-priority traffic in a traffic-control profile for a dynamic interface set or dynamic ACI interface set at a household level. Specifying this variable in a traffic-control profile for a dynamic subscriber interface is prohibited.
\$junos-cos-shaping-rate-excess-low-burst	Shaping rate burst size configured for excess low-priority traffic in a traffic-control profile for a dynamic interface set or dynamic ACI interface set at a household level. Specifying this variable in a traffic-control profile for a dynamic subscriber interface is prohibited.
\$junos-cos-shaping-rate-priority-high	Shaping rate configured for high-priority traffic in a traffic-control profile for a dynamic interface set or dynamic ACI interface set at a household level. Specifying this variable in a traffic-control profile for a dynamic subscriber interface is prohibited.
\$junos-cos-shaping-rate-priority-high-burst	Shaping rate burst size configured for high-priority traffic in a traffic-control profile for a dynamic interface set or dynamic ACI interface set at a household level. Specifying this variable in a traffic-control profile for a dynamic subscriber interface is prohibited.

Table 9: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
<code>\$junos-cos-shaping-rate-priority-low</code>	Shaping rate configured for low-priority traffic in a traffic-control profile for a dynamic interface set or dynamic ACI interface set at a household level. Specifying this variable in a traffic-control profile for a dynamic subscriber interface is prohibited.
<code>\$junos-cos-shaping-rate-priority-low-burst</code>	Shaping rate burst size configured for low-priority traffic in a traffic-control profile for a dynamic interface set or dynamic ACI interface set at a household level. Specifying this variable in a traffic-control profile for a dynamic subscriber interface is prohibited.
<code>\$junos-cos-shaping-rate-priority-medium</code>	Shaping rate configured for medium-priority traffic in a traffic-control profile for a dynamic interface set or dynamic ACI interface set at a household level. Specifying this variable in a traffic-control profile for a dynamic subscriber interface is prohibited.
<code>\$junos-cos-shaping-rate-priority-medium-burst</code>	Shaping rate burst size configured for medium-priority traffic in a traffic-control profile for a dynamic interface set or dynamic ACI interface set at a household level. Specifying this variable in a traffic-control profile for a dynamic subscriber interface is prohibited.
<code>\$junos-cos-traffic-control-profile</code>	<p>Traffic-control profile configured in a dynamic profile for subscriber access. The Junos OS obtains the profile information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the traffic-control-profiles statement at the [edit dynamic-profiles <i>profile-name</i> class-of-service] hierarchy level.</p>
Dynamic CoS — Scheduler Parameters	
<code>\$junos-cos-scheduler</code>	<p>Name of a scheduler configured in a dynamic profile. Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable at the [edit dynamic-profiles <i>profile-name</i> class-of-service schedulers] hierarchy level.</p>

Table 9: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
\$junos-cos-scheduler-bs	<p>Buffer size as a percentage of total buffer, specified for a scheduler configured in a dynamic profile. Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the buffer-size statement with the percent option at the [edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i>] hierarchy level.</p>
\$junos-cos-scheduler-pri	<p>Packet-scheduling priority value specified for a scheduler configured in a dynamic profile. Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the priority statement at the [edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i>] hierarchy level.</p>
\$junos-cos-scheduler-dropfile-any	<p>Name of the drop profile for random early detection (RED) for loss-priority level any specified for a scheduler configured in a dynamic profile. Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the drop-profile statement at the [edit dynamic-profiles <i>profile-name</i> class-of-service schedulers <i>scheduler-name</i> drop-profile-map loss-priority any protocol any] hierarchy level.</p> <p>NOTE: The drop profile must be configured statically (at the [edit class-of-service drop-profiles] hierarchy level).</p>

Table 9: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
\$junos-cos-scheduler-dropfile-high	<p>Name of the drop profile for random early detection (RED) for loss-priority level high specified for a scheduler configured in a dynamic profile. Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the drop-profile statement at the [edit dynamic-profiles profile-name class-of-service schedulers scheduler-name drop-profile-map loss-priority high protocol any] hierarchy level.</p> <p>NOTE: The drop profile must be configured statically (at the [edit class-of-service drop-profiles] hierarchy level).</p>
\$junos-cos-scheduler-dropfile-low	<p>Name of the drop profile for random early detection (RED) for loss-priority level low specified for a scheduler configured in a dynamic profile. Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the drop-profile statement at the [edit dynamic-profiles profile-name class-of-service schedulers scheduler-name drop-profile-map loss-priority low protocol any] hierarchy level.</p> <p>NOTE: The drop profile must be configured statically (at the [edit class-of-service drop-profiles] hierarchy level) for loss-priority low.</p>

Table 9: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
\$junos-cos-scheduler-dropfile-medium-high	<p>Name of the drop profile for random early detection (RED) for loss-priority level medium-high specified for a scheduler configured in a dynamic profile. Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the drop-profile statement at the [edit dynamic-profiles profile-name class-of-service schedulers scheduler-name drop-profile-map loss-priority medium-high protocol any] hierarchy level.</p> <p>NOTE: The drop profile must be configured statically (at the [edit class-of-service drop-profiles] hierarchy level).</p>
\$junos-cos-scheduler-dropfile-medium-low	<p>Name of the drop profile for random early detection (RED) for loss-priority level medium-low specified for a scheduler configured in a dynamic profile. Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the drop-profile statement at the [edit dynamic-profiles profile-name class-of-service schedulers scheduler-name drop-profile-map loss-priority medium-low protocol any] hierarchy level.</p> <p>NOTE: The drop profile must be configured statically (at the [edit class-of-service drop-profiles] hierarchy level).</p>
\$junos-cos-scheduler-excess-priority	<p>Priority value of the excess rate specified for a scheduler configured in a dynamic profile. Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the excess-priority statement at the [edit dynamic-profiles profile-name class-of-service schedulers scheduler-name] hierarchy level.</p>

Table 9: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
\$junos-cos-scheduler-excess-rate	<p>Value of the excess rate specified for a scheduler configured in a dynamic profile. Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the excess-rate statement at the [edit dynamic-profiles profile-name class-of-service schedulers scheduler-name] hierarchy level.</p>
\$junos-cos-scheduler-shaping-rate	<p>Value of the shaping rate specified for a scheduler configured in a dynamic profile. Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the shaping-rate statement at the [edit dynamic-profiles profile-name class-of-service schedulers scheduler-name] hierarchy level.</p>
\$junos-cos-scheduler-tx	<p>Transmit rate specified for a scheduler configured in a dynamic profile. Junos OS obtains this information from the RADIUS server when a subscriber authenticates over the static or dynamic subscriber interface to which the dynamic profile is attached.</p> <p>You reference this variable in the transmit-rate statement at the [edit dynamic-profiles profile-name class-of-service schedulers scheduler-name] hierarchy level.</p>
Dynamic Connectivity Fault Management Parameters	
\$junos-action-profile	Name of the action profile configured in a dynamic profile.
\$junos-ccm-interval	Continuity check interval time configured in a dynamic profile.
\$junos-loss-threshold	The number of continuity check messages lost before marking the remote MEP as down, configured in a dynamic profile.
\$junos-ma-name-format	Name of the maintenance association name format configured in a dynamic profile.
\$junos-md-name-format	Name of the maintenance domain format configured in a dynamic profile.

Table 9: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
\$junos-ma-name	Name of the maintenance association configured in a dynamic profile.
\$junos-md-level	Value of 'Level', configured in a dynamic profile.
\$junos-md-name	Name of the maintenance domain configured in a dynamic profile.
\$junos-mep-id	The 'MEP' value configured in the dynamic profile.
\$junos-remote-mep-id	The 'Remote MEP' value configured in the dynamic profile.
Filters — RADIUS-obtained Policies	
\$junos-input-filter	Name of an input filter to be attached; filter name is derived from RADIUS VSA 26-10 (Ingress-Policy-Name) or RADIUS attribute 11 (Filter-ID) to the interface.
\$junos-input-interface-filter	<p>Name of an input filter to be attached to a family any interface; filter name is derived from RADIUS VSA 26-191 (Input-Interface-Filter) to the interface.</p> <p>You can also specify the filter name with the <code>\$junos-input-interface-filter</code> statement at the <code>[edit dynamic-profiles profile-name interfaces interface-name unit logical-interface-number filter input]</code> hierarchy level.</p>
\$junos-input-ipv6-filter	Name of an IPv6 input filter to be attached; filter name is derived from RADIUS VSA 26-106 (IPv6-Ingress-Policy-Name) to the interface.
\$junos-output-filter	Name of an output filter to be attached; filter name is derived from RADIUS VSA 26-11 (Egress-Policy-Name) to the interface.
\$junos-output-interface-filter	<p>Name of an output filter to be attached to a family any interface; filter name is derived from RADIUS VSA 26-191 (Output-Interface-Filter) to the interface.</p> <p>You can also specify the filter name with the <code>\$junos-output-interface-filter</code> statement at the <code>[edit dynamic-profiles profile-name interfaces interface-name unit logical-interface-number filter output]</code> hierarchy level.</p>

Table 9: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
\$junos-output-ipv6-filter	Name of an IPv6 output filter to be attached; filter name is derived from RADIUS VSA 26-107 (IPv6-Egress-Policy-Name) to the interface.
Services	
\$junos-input-ipv6-service-filter	<p>Starting in Junos OS Release 17.2R1, name of an IPv6 input service filter to be attached. The filter name is derived from RADIUS-VSA 26-202 (IPv6 input service filter) to the interface.</p> <p>You specify this variable at the [edit dynamic-profile <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet6 service input service-set <i>service-set-name</i> service-filter] hierarchy level.</p>
\$junos-input-ipv6-service-set	<p>Starting in Junos OS Release 17.2R1, name of an IPv6 service set to be attached. The service set name is derived from RADIUS-VSA 26-200 (IPv6 input service set) to the interface.</p> <p>You specify this variable at the [edit dynamic-profile <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet6 service input service-set] hierarchy level.</p>
\$junos-input-service-filter	<p>Starting in Junos OS Release 17.2R1, name of an IPv4 input service filter to be attached. The filter name is derived from RADIUS-VSA 26-198 (IPv4 input service filter) to the interface.</p> <p>You specify this variable at the [edit dynamic-profile <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet service input service-set <i>service-set-name</i> service-filter] hierarchy level.</p>
\$junos-input-service-set	<p>Starting in Junos OS Release 17.2R1, name of an IPv4 input service set to be attached. The service set name is derived from RADIUS-VSA 26-196 (IPv4 input service set) to the interface.</p> <p>You specify this variable at the [edit dynamic-profile <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet service input service-set] hierarchy level.</p>

Table 9: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
\$junos-output-ipv6-service-filter	<p>Starting in Junos OS Release 17.2R1, name of an IPv6 service filter to be attached. The filter name is derived from RADIUS-VSA 26-203 (IPv6 output service filter) to the interface.</p> <p>You specify this variable at the [edit dynamic-profile <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet6 service output service-set <i>service-set-name</i> service-filter] hierarchy level.</p>
\$junos-output-ipv6-service-set	<p>Starting in Junos OS Release 17.2R1, name of an IPv6 service set to be attached. The service set name is derived from RADIUS-VSA 26-201 (IPv6 output service set) to the interface.</p> <p>You specify this variable at the [edit dynamic-profile <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet6 service output service-set] hierarchy level.</p>
\$junos-output-service-filter	<p>Starting in Junos OS Release 17.2R1, name of an IPv4 service filter to be attached. The filter name is derived from RADIUS-VSA 26-199 (IPv4 output service filter) to the interface.</p> <p>You specify this variable at the [edit dynamic-profile <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet service output service-set <i>service-set-name</i> service-filter] hierarchy level.</p>
\$junos-output-service-set	<p>Starting in Junos OS Release 17.2R1, name of an IPv4 output service set to be attached. The service set name is derived from RADIUS-VSA 26-197 (IPv4 output service set) to the interface.</p> <p>You specify this variable at the [edit dynamic-profile <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet service output service-set] hierarchy level.</p>
\$junos-pcef-profile	<p>Starting in Junos OS Release 17.2R1, name of a PCEF profile to be attached. The profile name is derived from RADIUS-VSA 26-204 (PCEF profile) to the interface.</p> <p>You specify this variable at the [edit dynamic-profile <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> service] hierarchy level.</p>

Table 9: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
\$junos-pcef-rule	<p>Starting in Junos OS Release 17.2R1, name of a PCC rule to activate. The rule name is derived from RADIUS-VSA 26-205 (PCEF rule) to the interface.</p> <p>You specify this variable at the [edit dynamic-profile <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> service pcef <i>pcef-profile-name</i> activate] hierarchy level.</p>
Subscriber Interfaces — Dynamic Demux Interfaces	
\$junos-interface-ifd-name	<p>Name of the device to which the subscriber access client connects. All interfaces are created on this device. Its primary use is in creating single or multiple subscribers on a statically created interface. You specify this variable at the [dynamic-profiles <i>profile-name</i> interfaces] hierarchy level.</p> <p>When creating a logical underlying interface for a dynamic VLAN demux interface, you must also specify this variable at the [dynamic-profiles <i>profile-name</i> interfaces <i>demux0</i> unit <i>\$junos-interface-unit</i> demux-options underlying-interface] hierarchy level.</p>
\$junos-interface-unit	<p>Creates a unit number assigned to the logical interface. The router supplies this information when the subscriber accesses the network. You specify this variable at the [dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i>] hierarchy level for the unit statement.</p>
\$junos-ipv6-address	<p>Selects the IPv6 address of the interface the subscriber uses. You specify this variable at the [edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>], [edit dynamic-profiles <i>profile-name</i> interfaces <i>demux0</i> unit <i>logical-unit-number</i> family <i>family</i>], [edit dynamic-profiles <i>profile-name</i> interfaces <i>pp0</i> unit "<i>\$junos-interface-unit</i>" family <i>family</i>], and [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>] hierarchy level for the address statement.</p>
\$junos-loopback-interface	<p>Selects the loopback interface the subscriber uses. You specify this variable at the [dynamic-profiles <i>profile-name</i> interfaces <i>demux0</i> unit "<i>\$junos-interface-unit</i>" family inet] hierarchy level for the unnumbered-address statement.</p>

Table 9: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
<code>\$junos-preferred-source-address</code>	<p>Selects the preferred IPv4 source address (family inet) associated with the loopback address used for the subscriber. You specify this variable at the <code>[dynamic profiles <i>profile-name</i> interfaces demux0 unit "\$junos-interface-unit" family inet unnumbered-address "\$junos-loopback-interface"]</code> hierarchy level for the <code>preferred-source-address</code> statement.</p> <p>NOTE: Starting in Junos OS Release 16.1, when you specify a static logical interface for the unnumbered interface in a dynamic profile that includes the <code>\$junos-routing-instance</code> predefined variable, you must not configure an IPv4 preferred source address. This constraint applies whether you use the <code>\$junos-preferred-source-address</code> predefined variable or the <code>preferred-source-address</code> statement. Configuring the preferred source address in this circumstance causes a commit failure.</p>
<code>\$junos-preferred-source-ipv6-address</code>	<p>Selects the preferred IPv6 source address (family inet6) associated with the loopback address used for the subscriber. You specify this variable at the <code>[dynamic profiles <i>profile-name</i> interfaces demux0 unit "\$junos-interface-unit" family inet6 unnumbered-address "\$junos-loopback-interface"]</code> hierarchy level for the <code>preferred-source-address</code> statement.</p> <p>NOTE: Starting in Junos OS Release 16.1, when you specify a static logical interface for the unnumbered interface in a dynamic profile that includes the <code>\$junos-routing-instance</code> predefined variable, you must not configure an IPv6 preferred source address. This constraint applies whether you use the <code>\$junos-preferred-source-ipv6-address</code> predefined variable or the <code>preferred-source-address</code> statement. Configuring the preferred source address in this circumstance causes a commit failure.</p>
<code>\$junos-subscriber-ip-address</code>	<p>IP address of the subscriber. You specify this variable at the <code>[dynamic-profiles <i>profile-name</i> interfaces <i>demux0</i> unit family <i>inet</i> demux-source]</code> hierarchy level.</p> <p>This variable is also used for creating access-internal routes.</p>

Table 9: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
\$junos-subscriber-ipv6-address	IPv6 address for subscriber. You specify this variable at the [dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet6 demux-source] hierarchy level.
\$junos-subscriber-ipv6-multi-address	<p>Expands the demux-source into multiple addresses; for example, the IPv6 prefix and /128 address for the subscriber.</p> <p>You specify this variable at the [dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet6 demux-source] hierarchy level.</p>
\$junos-underlying-interface	<p>Creates a logical underlying interface for a dynamic IP demux interface. The client logs in on this interface. You specify this variable at the [dynamic profiles <i>profile-name</i> interfaces demux0 unit "<i>\$junos-interface-unit</i>" demux-options] hierarchy level for the underlying-interface statement.</p> <p>When configured, the underlying interface is used to determine the \$junos-underlying-interface, \$junos-underlying-interface-unit, and \$junos-ifd-name variables. For example, if the receiving logical interface is ge-0/0/0.1, the \$junos-underlying-interface variable is set to ge-0/0/0 and the \$junos-underlying-interface-unit variable is set to 1.</p> <p>This variable is also used for creating access-internal routes.</p>
Subscriber Interfaces — Static VLAN Interfaces	
\$junos-interface-ifd-name	Name of the device to which the subscriber access client connects. All interfaces are created on this device. Its primary use is in creating single or multiple subscribers on a statically created interface. You specify this variable at the [dynamic-profiles <i>profile-name</i> interfaces] hierarchy level.
\$junos-underlying-interface-unit	Obtains the unit number for the underlying interface. It specifies the use of the underlying interface for the subscriber. You specify this variable at the [dynamic-profiles <i>profile-name</i> interfaces <i>\$junos-interface-ifd-name</i>] hierarchy level for the unit statement.

Table 9: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
Subscriber Interfaces — Dynamic PPPoE Interfaces	
<code>\$junos-interface-unit</code>	Specifies the logical unit number when the router dynamically creates a PPPoE logical interface. The <code>\$junos-interface-unit</code> predefined variable is dynamically replaced with the unit number supplied by the network when the PPPoE subscriber logs in. You specify this variable at the <code>[edit dynamic-profiles profile-name interfaces pp0]</code> hierarchy level for the <code>unit</code> statement.
<code>\$junos-underlying-interface</code>	Specifies the name of the underlying Ethernet interface on which the router dynamically creates the PPPoE logical interface. The <code>\$junos-underlying-interface</code> predefined variable is dynamically replaced with the name of the underlying interface supplied by the network when the PPPoE subscriber logs in. You specify this variable at the <code>[edit dynamic-profiles profile-name interfaces pp0 unit "\$junos-interface-unit" pppoe-options]</code> hierarchy level for the <code>underlying-interface</code> statement.
Subscriber Interfaces — Dynamic Interface Sets	
<code>\$junos-interface-set-name</code>	Name of an interface set configured in a dynamic profile. To represent the name of a dynamically created agent circuit identifier (ACI) interface set, use the <code>\$junos-interface-set-name</code> predefined variable in the <code>interface-set</code> statement at the <code>[edit dynamic-profiles profile-name interfaces]</code> hierarchy level.

Table 9: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
<code>\$junos-phy-ifd-interface-set-name</code>	<p>Name of an interface set associated with the underlying physical interface in a dynamic profile.</p> <p>In a heterogeneous topology where residential and business subscribers share the same physical interface, although only two levels of CoS are required for residential access, business access requires three levels. Because they share the same physical interface, three levels are configured for both, causing an unnecessary level 2 node to be consumed for each residential connection.</p> <p>Starting in Junos OS Release 16.1, you can reduce the CoS resources wasted on residential access by collecting the residential subscribers into an interface set associated with the physical interface. In this way, a level 2 node is used for the interface set rather than for each residential interface. To do so, specify the <code>\$junos-phy-ifd-interface-set-name</code> predefined variable with the <code>interface-set</code> statement at the <code>[edit dynamic-profiles profile-name interfaces]</code> hierarchy level to create the interface set based on the underlying physical interface.</p>
<code>\$junos-pon-id-interface-set-name</code>	<p>Locally generated interface set name used to associate individual customer circuits in a passive optical network (PON) to deliver CoS and other services to the set of interfaces.</p> <p>The name is extracted from the DHCPv4 (Option 82, suboption 2) or DHCPv6 (Option 37) agent remote ID string inserted by an optical line terminal (OLT) in a PON. The OLT must format the agent remote ID string with a pipe symbol () as the delimiter between substrings. The substring extracted for the interface set name consists of the characters following the last delimiter in the agent remote ID string.</p> <p>The extracted substring identifies individual customer circuits. You determine the format and contents of the substring, and configure your OLT to insert the information. Typically, the substring may include the name and port of the OLT accessed by the CPE optical network terminal (ONT).</p>
<code>\$junos-svlan-interface-set-name</code>	<p>Locally generated interface set name for use by dual-tagged VLAN interfaces based on the outer tag of the dual-tagged VLAN. The format of the generated variable is <code>physical_interface_name - outer_VLAN_tag</code>.</p>

Table 9: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
Wholesale Networking	
<code>\$junos-interface-name</code>	<p>Name of the dynamic interface to which the subscriber access client connects. Its use is in identifying the subscriber interface. You specify this variable at the <code>[dynamic-profiles <i>profile-name</i> routing-instance \$junos-routing-instance]</code> hierarchy level for the <code>interface</code> statement.</p> <p>The interface name is derived from concatenating the <code>\$junos-interface-ifd-name</code> and the <code>\$junos-underlying-interface-unit</code> variables obtained when a subscriber is created dynamically at the <code>[dynamic-profiles <i>profile-name</i> routing-instance \$junos-routing-instance interface]</code> hierarchy level.</p>
<code>\$junos-routing-instance</code>	<p>Name of the routing instance to which the subscriber is assigned. This variable triggers a return value from the RADIUS server for Virtual-Router (VSA 26-1).</p> <p>You reference this variable in the statement at the <code>[dynamic-profiles <i>profile-name</i>]</code> hierarchy level for the <code>routing-instance</code> statement.</p> <p>NOTE: Starting in Junos OS Release 16.1, when you specify a static logical interface for the unnumbered interface in a dynamic profile that includes the <code>\$junos-routing-instance</code> predefined variable, you must not configure a preferred source address. This constraint applies whether you use the <code>\$junos-preferred-source-address</code> predefined variable, the <code>\$junos-preferred-source-ipv6-address</code> predefined variable, or the <code>preferred-source-address</code> statement. Configuring the preferred source address in this circumstance causes a commit failure.</p>

Table 9: Junos OS Predefined Variables and Definitions (*continued*)

Variable	Definition
\$junos-inner-vlan-map-id	<p>Starting in Junos OS Release 16.1R4, identifier for the inner VLAN tag for Layer 2 wholesale, ANCP-triggered, autosensed dynamic VLANs. The VLAN tag is allocated from the inner VLAN ID swap ranges that are provisioned on the core-facing physical interface. The inner VLAN tag is swapped with (replaces) the outer VLAN tag when the subscriber traffic is tunneled to the NSP.</p> <p>You specify this variable with the inner-vlan-id statement at the [edit dynamic-profiles <i>profile-name</i> interfaces \$junos-interface-ifd-name unit \$junos-interface-unit input-vlan-map] hierarchy level.</p>
\$junos-vlan-map-id	<p>Identifier for a VLAN that is rewritten at the input or output interface as specified by a VLAN map.</p> <p>You specify this variable with the vlan-id statement at the [edit dynamic-profiles <i>profile-name</i> interfaces \$junos-interface-ifd-name unit \$junos-interface-unit input-vlan-map] or [edit dynamic-profiles <i>profile-name</i> interfaces \$junos-interface-ifd-name unit \$junos-interface-unit input-vlan-map] hierarchy levels.</p>

Release History Table

Release	Description
17.2R1	Starting in Junos OS Release 17.2R1, name of an IPv6 input service filter to be attached.
17.2R1	Starting in Junos OS Release 17.2R1, name of an IPv6 service set to be attached.
17.2R1	Starting in Junos OS Release 17.2R1, name of an IPv4 input service filter to be attached.
17.2R1	Starting in Junos OS Release 17.2R1, name of an IPv4 input service set to be attached.
17.2R1	Starting in Junos OS Release 17.2R1, name of an IPv6 service filter to be attached.
17.2R1	Starting in Junos OS Release 17.2R1, name of an IPv6 service set to to be attached.
17.2R1	Starting in Junos OS Release 17.2R1, name of an IPv4 service filter to be attached.
17.2R1	Starting in Junos OS Release 17.2R1, name of an IPv4 output service set to be attached.
17.2R1	Starting in Junos OS Release 17.2R1, name of a PCEF profile to be attached.
17.2R1	Starting in Junos OS Release 17.2R1, name of a PCC rule to activate.
16.1R4	Starting in Junos OS Release 16.1R4, identifier for the inner VLAN tag for Layer 2 wholesale, ANCP-triggered, autosensed dynamic VLANs.
16.1	Starting in Junos OS Release 16.1, when you specify a static logical interface for the unnumbered interface in a dynamic profile that includes the \$junos-routing-instance predefined variable, you must not configure an IPv4 preferred source address.
16.1	Starting in Junos OS Release 16.1, when you specify a static logical interface for the unnumbered interface in a dynamic profile that includes the \$junos-routing-instance predefined variable, you must not configure an IPv6 preferred source address.
16.1	Starting in Junos OS Release 16.1, you can reduce the CoS resources wasted on residential access by collecting the residential subscribers into an interface set associated with the physical interface.
16.1	Starting in Junos OS Release 16.1, when you specify a static logical interface for the unnumbered interface in a dynamic profile that includes the \$junos-routing-instance predefined variable, you must not configure a preferred source address.

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

- Junos OS Predefined Variables That Correspond to RADIUS Attributes and VSAs
- User-Defined Variables

Juniper Networks VSAs Supported by the AAA Service Framework

Table 10 on page 143 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 10: 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

Table 10: Supported Juniper Networks VSAs (*continued*)

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
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	Tunnel password in cleartext. Do not use both this VSA and the standard RADIUS attribute Tunnel-Password [69]. We recommend that you use the standard attribute because the password is encrypted when that attribute is used.	string: <i>tunnel-password</i>	No
26-10	Ingress-Policy-Name	Input policy name to apply to client interface.	string: <i>input-policy-name</i>	Yes
26-11	Egress-Policy-Name	Output policy name to apply to client interface.	string: <i>output-policy-name</i>	Yes
26-23	IGMP-Enable	Whether IGMP is enabled or disabled on a client interface.	integer: <ul style="list-style-type: none"> 0=disable 1=enable 	Yes
26-24	PPPoE-Description	Client MAC address.	string: <i>pppoe</i> <i>client-mac-address</i>	No
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	SSC service bundle.	string <i>bundle-name</i>	No

Table 10: Supported Juniper Networks VSAs (*continued*)

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
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
26-51	Disconnect-Cause	Disconnect cause when a tunneled subscriber is disconnected, and L2TP layer of the LNS initiates the termination. 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>disconnect-cause</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

Table 10: Supported Juniper Networks VSAs (*continued*)

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
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
26-60	Med-Ip-Address	<p>IP address of content destination device to which mirrored traffic is forwarded.</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 IP address	No
26-61	Med-Port-Number	<p>UDP port in the content destination device to which mirrored traffic is forwarded.</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 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>	Yes
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

Table 10: Supported Juniper Networks VSAs (*continued*)

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
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
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

Table 10: Supported Juniper Networks VSAs (*continued*)

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
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)	No
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)	No
26-94	Tunnel-Tx-Speed-Method	Method that determines the source from which the transmit speed is derived. Overrides global configuration in the CLI.	integer: 4-octet <ul style="list-style-type: none"> • 0 = none • 1 = static Layer 2 • 2 = dynamic layer 2. This method is not supported; the static Layer 2 method is used instead. • 3 = CoS. This method is not supported; the actual method is used instead. • 4 = actual • 5 = ANCP • 6 = PPPoE IA tags 	No
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

Table 10: Supported Juniper Networks VSAs (*continued*)

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-107	IPv6-Egress-Policy-Name	Output policy name to apply to a user IPv6 interface.	string: <i>policy-name</i>	Yes
26-108	CoS-Traffic-Control-Profile-Parameter-Type	<p>CoS traffic-shaping parameter type and description:</p> <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 	<p>Two parts, delimited by white space:</p> <ul style="list-style-type: none"> • Parameter type • Parameter value <p>Examples:</p> <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	No
26-111	Acc-Aggr-Cir-Id-Bin	Unique identification of the DSL line.	integer: 8-octet	No
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	No
26-113	Act-Data-Rate-Up	Actual upstream data rate of the subscriber's synchronized DSL link.	integer: 4-octet	No
26-114	Act-Data-Rate-Dn	Actual downstream data rate of the subscriber's synchronized DSL link.	integer: 4-octet	No
26-115	Min-Data-Rate-Up	Minimum upstream data rate configured for the subscriber.	integer: 4-octet	No

Table 10: Supported Juniper Networks VSAs (*continued*)

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-116	Min-Data-Rate-Dn	Minimum downstream data rate configured for the subscriber.	integer: 4-octet	No
26-117	Att-Data-Rate-Up	Maximum upstream data rate that the subscriber can attain.	integer: 4-octet	No
26-118	Att-Data-Rate-Dn	Maximum downstream data rate that the subscriber can attain.	integer: 4-octet	No
26-119	Max-Data-Rate-Up	Maximum upstream data rate configured for the subscriber.	integer: 4-octet	No
26-120	Max-Data-Rate-Dn	Maximum downstream data rate configured for the subscriber.	integer: 4-octet	No
26-121	Min-LP-Data-Rate-Up	Minimum upstream data rate in low power state configured for the subscriber.	integer: 4-octet	No
26-122	Min-LP-Data-Rate-Dn	Minimum downstream data rate in low power state configured for the subscriber.	integer: 4-octet	No
26-123	Max-Interlv-Delay-Up	Maximum one-way upstream interleaving delay configured for the subscriber.	integer: 4-octet	No
26-124	Act-Interlv-Delay-Up	Subscriber's actual one-way upstream interleaving delay..	integer: 4-octet	No
26-125	Max-Interlv-Delay-Dn	Maximum one-way downstream interleaving delay configured for the subscriber.	integer: 4-octet	No
26-126	Act-Interlv-Delay-Dn	Subscriber's actual one-way downstream interleaving delay.	integer: 4-octet	No
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 	No
26-128	DSL-Type	Encapsulation used by the subscriber associated with the DSLAM interface from which requests are initiated.	integer: 4-octet	No

Table 10: Supported Juniper Networks VSAs (*continued*)

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
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	No
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	No
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
26-146	CoS-Scheduler-Pmt-Type	<p>CoS scheduler parameter type and description:</p> <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 	<p>Three parts, delimited by white space:</p> <ul style="list-style-type: none"> Scheduler name Parameter type Parameter value <p>Examples:</p> <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

Table 10: Supported Juniper Networks VSAs (*continued*)

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
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
26-160	Vlan-Map-Id	Trunk VLAN tag corresponding to the core-facing trunk physical interface.	integer	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 transmit speed of the user's connection.	string	No
26-163	Rx-Connect-Speed	Indication of receive speed of the 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 for residential services 2 = op-script for business services 	No
26-174	Client-Profile-Name	Enables RADIUS to override an assigned client dynamic profile with the included profile.	string	No
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

Table 10: Supported Juniper Networks VSAs (*continued*)

Attribute Number	Attribute Name	Description	Value	Dynamic CoA Support
26-181	DHCPv6-Guided-Relay-Server	IPv6 addresses of DHCPv6 servers to which DHCPv6 relay agent forwards the Solicit and subsequent PDUs. Use multiple instances of the VSA to specify a list of servers.	hexadecimal string: <i>ipv6-address</i>	No
26-182	Acc-Loop-Remote-Id	Reports the ANCP Access-Loop-Remote-ID attribute.	string	No
26-183	Acc-Loop-Encap	Reports the ANCP Access-Loop-Encapsulation attribute.	hexadecimal string	No
26-184	Inner-Vlan-Map-Id	Inner VLAN tag allocated from the ranges provisioned on the core-facing physical interface, used to swap (replace) the autosensed VLAN tag on the access interface.	integer	No
26-185	Core-Facing-Interface	Name of the core-facing physical interface that forwards the Layer 2 wholesale session's downstream and upstream traffic relative to the network service provider (NSP) router.	string	No
26-187	DHCP-First-Relay-IPv4-Address	IPv4 address of the first relay link of a client/server binding.	integer: 4-byte <i>ip-address</i>	No
26-188	DHCP-First-Relay-IPv6-Address	IPv6 address of the first relay link of a client/server binding.	hexadecimal string: <i>ipv6-address</i>	No
26-191	Input-Interface-Filter	Name of an input filter to be attached to a family any interface.	string	No
26-192	Output-Interface-Filter	Name of an output filter to be attached to a family any interface.	string	No
26-194	Bulk-CoA-Transaction-Id	A common identifier or tag to associate the series of related CoA Requests as a transaction. This attribute is untagged and value 0 is reserved.	integer: 4-octet	Yes
26-195	Bulk-CoA-Identifier	A unique identifier for each CoA Request message that is part of the same transaction as specified by the Bulk-CoA-Transaction-Id VSA. This attribute is untagged and the value 0 is reserved.	integer: 4-octet	Yes

- Related Documentation**
- [AAA Access Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS on page 154](#)
 - [AAA Accounting Messages and Supported RADIUS Attributes and Juniper Networks VSAs for Junos OS on page 160](#)

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

Table 11 on page 154 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 11: 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	✓	✓	–	–	✓	–
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	–	✓	–	–	–	–

Table 11: 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
26-5	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	–	✓	–	–	–	–
26-24	PPPoE-Description	✓	–	–	–	–	–
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	✓	–	–	–	–	–
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	✓	–	–	–	–	–

Table 11: 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
26-64	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	–	✓	–	–	–	–
26-94	Tunnel-Tx-Speed-Method	–	✓	–	–	–	–
26-97	IGMP-Immediate-Leave	–	✓	–	–	–	–
26-100	MLD-Immediate-Leave	–	✓	–	–	–	–
26-106	IPv6-Ingress-Policy-Name	–	✓	–	–	–	–
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	✓	–	–	–	–	–

Table 11: 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
26-113	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	–	✓	–	–	–	–
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	–	✓	–	–	–	–

Table 11: 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
26-160	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	–	–	–	–	✓	–
26-181	DHCPv6-Guided-Relay-Server	–	✓	–	–	–	–
26-182	Acc-Loop-Remote-Id	✓	–	–	–	–	–
26-183	Acc-Loop-Encap	✓	–	–	–	–	–
26-184	Inner-Vlan-Map-Id	–	✓	–	–	–	–
26-185	Core-Facing-Interface	–	–	–	–	–	–
26-187	DHCP-First-Relay-IPv4-Address	✓	–	–	–	–	–
26-188	DHCP-First-Relay-IPv6-Address	✓	–	–	–	–	–
26-191	Input-Interface-Filter	✓	–	–	–	–	–
26-192	Output-Interface-Filter	✓	–	–	–	–	–
27	Session-Timeout	–	✓	–	✓	–	–
31	Calling-Station-ID	✓	–	–	–	✓	–
32	NAS-Identifier	✓	–	–	–	–	–
44	Acct-Session-ID	✓	–	–	–	✓	✓
61	NAS-Port-Type	✓	–	–	–	–	–
64	Tunnel-Type	✓	✓	–	–	–	–

Table 11: 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
65	Tunnel-Medium-Type	✓	✓	–	–	–	–
66	Tunnel-Client-Endpoint	✓	✓	–	–	–	–
67	Tunnel-Server-Endpoint	✓	✓	–	–	–	–
68	Acct-Tunnel-Connection-ID	✓	✓	–	–	–	–
68	Acct-Tunnel-Connection	–	✓	–	–	–	–
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 160](#)
 - [RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework](#)

- *RADIUS IETF Attributes Supported by the AAA Service Framework*
- [Juniper Networks VSAs Supported by the AAA Service Framework on page 143](#)

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

Table 12 on page 160 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 12: 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	✓	✓	✓	–	–
26-1	Virtual-Router	✓	✓	✓	–	–
26-10	Ingress-Policy-Name	✓	✓	✓	–	–
26-11	Egress-Policy-Name	✓	✓	✓	–	–
26-24	PPPoE-Description	✓	✓	✓	–	–
26-42	Input-Gigapackets	–	✓	✓	–	–
26-43	Output-Gigapackets	–	✓	✓	–	–

Table 12: 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
26-47	Ipv6-Primary-DNS	✓	✓	✓	–	–
26-48	Ipv6-Secondary-DNS	✓	✓	✓	–	–
26-51	Disconnect-Cause	–	✓	–	–	–
26-55	DHCP-Options	✓	✓	✓	–	–
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	✓	✓	✓	–	–

Table 12: 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
26-125	Max-Interlv-Delay-Dn	✓	✓	✓	–	–
26-126	Act-Interlv-Delay-Dn	✓	✓	✓	–	–
26-127	DSL-Line-State	✓	✓	✓	–	–
26-128	DSL-Type	✓	✓	✓	–	–
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	–	✓	✓	–	–
26-160	Vlan-Map-Id	✓	✓	✓	–	–
26-162	Tx-Connect-Speed	✓	✓	✓	–	–
26-163	Rx-Connect-Speed	✓	✓	✓	–	–
26-177	Cos-Shaping-Rate	✓	✓	✓	–	–
26-182	Acc-Loop-Remote-Id	✓	✓	–	–	–
26-183	Acc-Loop-Encap	✓	✓	–	–	–
26-184	Inner-Vlan-Map-Id	✓	✓	–	–	–
26-185	Core-Facing-Interface	✓	✓	–	–	–
26-187	DHCP-First-Relay-IPv4-Address	✓	✓	✓	–	–
26-188	DHCP-First-Relay-IPv6-Address	✓	✓	✓	–	–
26-191	Input-Interface-Filter	✓	✓	✓	–	–

Table 12: 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
26-192	Output-Interface-Filter	✓	✓	✓	–	–
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	–	✓	✓	–	–
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	✓	✓	✓	–	–
68	Acct-Tunnel-Connection	✓	✓	✓	–	–
82	Tunnel-Assignment-Id	✓	✓	✓	–	–

Table 12: 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
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 154](#)
- *RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework*
- *RADIUS IETF Attributes Supported by the AAA Service Framework*
- [Juniper Networks VSAs Supported by the AAA Service Framework on page 143](#)

CHAPTER 9

Configuring ANCP-Triggered Layer 2 Wholesale Services

- [Configuring ANCP Neighbors on page 165](#)
- [Configuring the ANCP Agent for ANCP-Triggered, Autosensed Dynamic VLANs on page 167](#)
- [Configuring a Username for Authentication of Out-of-Band Triggered Dynamic VLANs on page 168](#)
- [Configuring Out-of-Band ANCP Messages to Trigger Dynamic VLAN Instantiation on page 169](#)
- [Triggering ANCP OAM to Simulate ANCP Port Down and Port Up Messages on page 170](#)
- [Configuring the ANCP Agent to Dampen the Effects of Short-Term Adjacency Losses on page 172](#)
- [Reestablishing Pending Access Line Sessions for Layer 2 Wholesale on page 173](#)
- [Configuring Multiple Non-Overlapping VLAN Ranges for Core-Facing Physical Interfaces on page 173](#)
- [Clearing ANCP Access Loops on page 174](#)

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 203.0.113.234
```

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 203.0.113.234]  
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 203.0.113.234]  
user@host# set ietf-mode
```

4. (Optional) Configure the interval in seconds between ANCP adjacency messages exchanged with this neighbor.

```
[edit protocols ancp neighbor 203.0.113.234]  
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 203.0.113.234]  
user@host# set maximum-discovery-table-entries 10000
```

6. (Optional) Enable out-of-band ANCP triggering of autosensed, dynamic VLANs on the physical interface.

```
[edit protocols ancp neighbor 203.0.113.234]  
user@host# set auto-configure-trigger interface ge-1/0/0
```

7. (Optional) Configure how long the ANCP agent maintains a Layer 2 wholesale session when an adjacency loss occurs.

```
[edit protocols ancp neighbor 203.0.113.234]  
user@host# set adjacency-loss-hold-time 10
```

**Related
Documentation**

- *Configuring the ANCP Agent*
- *Configuring the ANCP Agent for Backward Compatibility*
- *Specifying the Interval Between ANCP Adjacency Messages*
- *Specifying the Maximum Number of Discovery Table Entries*
- *Configuring the ANCP Agent to Dampen the Effects of Short-Term Adjacency Losses on page 172*

Configuring the ANCP Agent for ANCP-Triggered, Autosensed Dynamic VLANs

Starting in Junos OS Release 16.1R4, you can configure the ANCP agent to associate a neighbor with an access-facing physical interface for the creation of autosensed dynamic VLANs on the interface. When the ANCP agent receives a Port Up message from the neighbor, it triggers notification to the autoconfd daemon to initiate the detection, authorization, and creation of dynamic VLANs. Receipt of an out-of-band ANCP Port Down message triggers notification to the autoconfd daemon to initiate the destruction of an existing VLAN on the interface.

This configuration assumes the following:

- The dynamic profile is configured to instantiate a dynamic VLAN when notified by the ANCP agent that it has received an out-of-band ANCP Port Up message.
- The RADIUS authentication server is properly configured to authorize the VLANs and apply services as needed.
- The ANCP agent is configured to initiate interim accounting updates (which also enables immediate interim accounting updates) in response to information received in Port Up messages.

To map a neighbor to a physical interface for autosensed dynamic VLANs:

- Specify the physical interface name.

```
[edit protocols ancp]
```

```
user@host# set auto-configure-trigger interface physical-interface-name
```

Release History Table

Release	Description
16.1R4	Starting in Junos OS Release 16.1R4, you can configure the ANCP agent to associate a neighbor with an access-facing physical interface for the creation of autosensed dynamic VLANs on the interface.

Related Documentation

- [Configuring the ANCP Agent](#)
- [Configuring ANCP Neighbors on page 165](#)
- [ANCP and the ANCP Agent Overview](#)
- [Layer 2 Wholesale with ANCP-Triggered VLANs Overview on page 99](#)
- [Configuring Out-of-Band ANCP Messages to Trigger Dynamic VLAN Instantiation on page 169](#)

Configuring a Username for Authentication of Out-of-Band Triggered Dynamic VLANs

When a subscriber logs in, the Access-Request message that is sent to the RADIUS server includes a username and optionally a password generated locally on the router to authenticate the subscriber during the VLAN authorization process. For a Layer 2 network that is wholesaled to a retailer where the dynamic VLANs are instantiated by out-of-band ANCP Port Up messages, you can configure the router to create a unique username with the value of the ANCP TLVs—Access-Loop-Circuit-ID, Access-Loop-Remote-Id, or both—as received in the ANCP Port Up message from the access node.

This configuration assumes the following:

- The ANCP agent is configured to notify AAA when it receives ANCP Port Up and Port Down messages.
- The dynamic profile is configured to instantiate a dynamic VLAN when notified by the ANCP agent that it has received an out-of-band ANCP Port Up message.
- The RADIUS authentication server is properly configured.

To include ANCP TLVs in the authentication username

1. (Optional) Specify inclusion of the Access-Loop-Circuit-ID TLV value.

```
[edit interfaces ge-0/0/0 auto-configure vlan-ranges username-include]
user@host# set circuit-id
```

2. (Optional) Specify inclusion of the Access-Loop-Remote-ID TLV value.

```
[edit interfaces ge-0/0/0 auto-configure vlan-ranges username-include]
user@host# set remote-id
```



NOTE: This ANCP information is not supported in stacked VLANs.



NOTE: You can use any of the attributes available to the `username-include` statement, except: `mac-address`, `option-18`, `option-37`, and `option-82`.

You can include other information in the username as for conventional autosensed dynamic VLANs. Alternatively, if you configure the router to convey ANCP-sourced access loop attributes as Juniper Networks VSAs—in this case `Acc-Loop-Cir-Id` (26-110) and `Acc-Loop-Remote-Id` (26-182)—the Access-Request message includes sufficient unique access line information for the RADIUS server to determine whether the access loop is wholesaled to a retailer or retained for the wholesaler.

Related Documentation

- [Configuring VLAN Interface Username Information for AAA Authentication](#)
- [Configuring Out-of-Band ANCP Messages to Trigger Dynamic VLAN Instantiation on page 169](#)

- [Configuring the ANCP Agent for ANCP-Triggered, Autosensed Dynamic VLANs on page 167](#)
- [Layer 2 Wholesale with ANCP-Triggered VLANs Overview on page 99](#)

Configuring Out-of-Band ANCP Messages to Trigger Dynamic VLAN Instantiation

The instantiation of conventional autosensed dynamic VLANs is triggered by in-band PPPoE or DHCP control packets that the Packet Forwarding Engine exceptions to the Routing Engine. A VLAN is authorized based on information extracted from specific fields and created according to a dynamic profile assigned to the VLAN range or stacked VLAN range.

Another way to instantiate an autosensed dynamic VLAN is with the processing of packets from an out-of-band protocol, ANCP. The out-of-band protocol method is useful where the traffic received might not be PPPoE or DHCP, such as in a Layer 2 wholesale scenario, where the traffic for an entire outer VLAN is wholesaled to a retailer and the VLANs are based on access line identifiers.

For this method, you configure the dynamic profile to accept packets from the out-of-band protocol. The dynamic profile is on an access-facing physical interface and is associated with a VLAN range available for the autosensed VLANs.

This configuration assumes the following:

- The dynamic profile is configured to instantiate a dynamic VLAN when notified by the ANCP agent that it has received an out-of-band ANCP Port Up message.
- The RADIUS authentication server is properly configured to authorize the VLANs and apply services as needed.
- The ANCP agent is configured to notify AAA when it receives ANCP Port Up and Port Down messages.
- The ANCP agent is configured to initiate interim accounting updates (which also enables immediate interim accounting updates) in response to information received in Port Up messages.



NOTE: Out-of-band triggering is supported only for single-tag VLANs; it is not supported for stacked VLANs.

To configure the instantiation of autosensed dynamic VLANs by out-of-band ANCP packets:

- Specify that ANCP packets are accepted.

```
[edit interfaces interface-name auto-configure vlan-ranges dynamic-profile profile-name]
user@host# set accept-out-of-band ancp
```

- Related Documentation**
- [Layer 2 Wholesale with ANCP-Triggered VLANs Overview on page 99](#)
 - [Configuring the ANCP Agent for ANCP-Triggered, Autosensed Dynamic VLANs on page 167](#)
 - [Configuring VLAN Interface Username Information for AAA Authentication](#)
 - [Configuring an Interface to Use the Dynamic Profile Configured to Create Single-Tag VLANs](#)

Triggering ANCP OAM to Simulate ANCP Port Down and Port Up Messages

You can trigger ANCP OAM to simulate the sending of an ANCP Port-Down or Port-Up message. Typically you use this feature only when troubleshooting an ANCP issue or to mitigate an error condition when ANCP is not operating normally.

When you issue either the **request ancp oam port-down** command or the **request ancp oam port-up** command from operational mode, you must specify either an IP address for an ANCP neighbor or the physical interface used for subscriber access. You must also specify all of the following; all three are required together to identify the access node:

- circuit-id *aci*—ANCP Access-Loop-Circuit-ID TLV
- remote-id *ari*—ANCP Access-Loop-Remote-ID TLV
- outer-vlan-id *vlan-id*—ANCP Access-Aggregation-Circuit-ID-Binary TLV

You can use the **request ancp oam port-up** command to trigger reauthorization and re-creation of the dynamic VLAN session and logical interface that is supporting Layer 2 wholesale after they have been removed by any of the following:

- Issuance of the **clear network-access aaa subscriber** command.
- Receipt of a RADIUS disconnect message that does not include the RADIUS Acct-Terminate-Cause attribute (49).
- Action by the ANCP agent.

The previous instance of the VLAN can be either ANCP-triggered (a wholesaled VLAN) or a conventionally autosensed dynamic VLAN (an access-provider-owned VLAN).

If no access line parameters are available from ANCP for a given access line, you can use the **request ancp oam port-up** command as a test mechanism to trigger authorization of a dynamic VLAN session and logical interface. The session and interface are created when a RADIUS Access-Accept message is subsequently received.

These commands have no effect on conventionally autosensed dynamic VLANs (for the access provider's own subscriber sessions) that have matching access loop attributes.



NOTE: Genuine ANCP Port-Down and Port-Up messages take precedence over these simulated messages. This means that when a Port-Down message has already been received, you cannot use the `request ancp oam port-up` command to initiate the Port-Up condition. When a Port-Up message has already been received, you cannot use the `request ancp oam port-down` command to initiate the Port-Down condition.

You can use the `request ancp oam port-down` command to trigger removal of the ANCP-triggered, autosensed, dynamic VLAN that corresponds to the specified attributes. The typical use for this command is to remove the VLAN created by sending a `request ancp oam port-up` command.

To simulate an ANCP Port Up message:

- Identify the loop by the neighbor's IP address or the access-facing physical interface, and the ACI, ARI, and outer VLAN ID.

```
user@host> request ancp oam port-up neighbor 192.168.32.5 circuit-id line-aci-1
remote-id line-ari-1 outer-vlan-id 126
user@host> request ancp oam port-up subscriber-interface ge-1/0/1 circuit-id line-aci-1
remote-id line-ari-1 outer-vlan-id 126
```

To simulate an ANCP Port Down message:

- Identify the loop by the neighbor's IP address or the access-facing physical interface, and the ACI, ARI, and outer VLAN ID.

```
user@host> request ancp oam port-down neighbor 192.168.32.5 circuit-id line-aci-1
remote-id line-ari-1 outer-vlan-id 126
user@host> request ancp oam port-down subscriber-interface ge-1/0/1 circuit-id
line-aci-1 remote-id line-ari-1 outer-vlan-id 126
```

To verify the operation of either request, you can enter the following commands before and after initiating the Port Down or Port Up message:

- `show subscribers client-type vlan-oob detail`—Subscriber information is displayed for the VLAN on Port UP, or disappears on Port Down.
- `show subscribers summary`—The VLAN-OOB counter reflects the creation or removal of the VLAN-OOB session by incrementing (Port Up) or decrementing (Port Down).
- `show l2-routing-instance routing-instance-name`—The VLAN counters reflect to reflect the creation or removal of the VLAN-OOB session by incrementing (Port Up) or decrementing (Port Down).

Related Documentation

- [Layer 2 Wholesale with ANCP-Triggered VLANs Overview on page 99](#)

Configuring the ANCP Agent to Dampen the Effects of Short-Term Adjacency Losses

By default, the ANCP agent treats a loss of adjacency as if it has received a Port Down message for every access loop that is represented by the adjacency. All Layer 2 wholesale sessions are logged out and cleaned up. If the associated physical interface is in the Down state, then pending sessions cannot be reestablished when the interface transitions back to the Up state.

You can configure the ANCP agent to maintain the corresponding ANCP-triggered Layer 2 wholesale sessions for a configurable period in the event that an ANCP adjacency is lost. If the adjacency is restored before the timer expires, the session continues. If the timer expires before the adjacency is restored, then the session is logged out and cleaned up. This behavior dampens the effect of unstable ANCP connections. The hold timer can also detect when an access line is unconfigured on a neighbor and trigger logout and cleanup of the related sessions.



NOTE: The default value of the timer is 0, which means that the loss of neighbor adjacency immediately triggers a logout of all corresponding Layer 2 wholesale sessions.

To configure how long the ANCP agent maintains sessions in the event of an adjacency loss for any neighbor:

- Specify the hold timer duration in seconds.

```
[edit protocols ancp]
user@host# set adjacency-loss-hold-time seconds
```

To configure how long the ANCP agent maintains sessions in the event of an adjacency loss for a specific neighbor:

- Specify the hold timer duration in seconds.

```
[edit protocols ancp neighbor ip-address]
user@host# set adjacency-loss-hold-time seconds
```

Related Documentation

- [Configuring the ANCP Agent](#)
- [Configuring ANCP Neighbors on page 165](#)
- [ANCP and the ANCP Agent Overview](#)
- [Layer 2 Wholesale with ANCP-Triggered VLANs Overview on page 99](#)

Reestablishing Pending Access Line Sessions for Layer 2 Wholesale

The access lines for ANCP-triggered, Layer 2 wholesale sessions can transition to a pending state after an ANCP adjacency loss when the inner VLAN ID swap range has been exhausted of tags and no other eligible core-facing physical interfaces are available. Typically, the sessions are reestablished when more VLAN IDs are made available, such as by extending the swap range, or more interfaces are available, such as by reconfiguration. When that does not happen, you can manually initiate the reestablishment process by issuing the **request auto-configuration reconnect-pending** command.

To manually reestablish sessions for which the corresponding access lines are in the pending state:

- Specify the routing instance with the reconnection request.

```
user@host> request auto-configuration reconnect-pending
```

Related Documentation

- [Layer 2 Wholesale with ANCP-Triggered VLANs Overview on page 99](#)

Configuring Multiple Non-Overlapping VLAN Ranges for Core-Facing Physical Interfaces

You can configure up to 32 non-overlapping inner VLAN ID swap ranges for each core-facing physical interface in a Layer 2 wholesale network with VLAN-OOB subscribers. VLAN IDs from the ranges are allocated to replace the outer VLAN tag on traffic received on the access-facing physical interfaces. The swap occurs before the subscriber traffic is forwarded to the network service provider (NSP).

You can add or remove ranges or increase or decrease the size of existing ranges even while Layer 2 wholesale sessions are assigned to the core-facing interface associated with the ranges. You cannot remove a range from which a VLAN ID has already been allocated. You cannot reduce a range if the new range excludes a VLAN ID that has already been allocated.

To configure multiple ranges per interface:

- Specify the ranges.

```
user@host# set interfaces interface-name unit logical-unit-number
inner-vlan-id-swap-ranges low-inner-tag1-high-inner-tag1
user@host# set interfaces interface-name unit logical-unit-number
inner-vlan-id-swap-ranges low-inner-tag2-high-inner-tag2
user@host# set interfaces interface-name unit logical-unit-number
inner-vlan-id-swap-ranges low-inner-tag3-high-inner-tag3
...
```

You can configure the ranges in any order. For example, one way to configure three non-overlapping ranges on interface ge-0/1/1 is the following:

```
[edit]
user@host# set interfaces ge-0/1/1 unit 0 inner-vlan-id-swap-ranges 70-80
user@host# set interfaces ge-0/1/1 unit 0 inner-vlan-id-swap-ranges 100-120
```

```
user@host# set interfaces ge-0/1/1 unit 0 inner-vlan-id-swap-ranges 10-60
```

Regardless of the order of configuration, **show** commands display the ranges in ascending order from lowest to highest:

```
user@host> show interfaces ge-0/1/1
description "ISP 1 core-facing PE1";
encapsulation ethernet-vpls;
unit 0 {
    inner-vlan-id-swap-ranges [10-60 70-80 100-120];
    ...
}
```

Related •
Documentation

Clearing ANCP Access Loops

You can force a reset of a particular Layer 2 wholesale connection while the access loop is operationally up by issuing the **clear ancp access-loop** command. The command initiates logout of an ANCP-triggered, dynamic VLAN session, which includes issuing RADIUS Accounting-Stop messages for the session, and removal of the dynamic VLAN logical interface and active services. After the session is cleaned up, the command initiates re-authorization of the dynamic VLAN session, simulating receipt of an ANCP Port Up message. The session may then be recreated.

You must identify the access loop by either the IP address of the ANCP neighbor or the name of the subscriber-facing physical interface. You must also specify one or more of the following additional identifiers for the access loop:

- **circuit-id**—The value of the ANCP Access-Loop-Circuit-ID TLV.
- **remote-id**—The value of the ANCP Access-Loop-Remote-ID TLV.
- **outer-vlan-id**—The value of the ANCP Access-Aggregation-Circuit-ID-binary TLV.



NOTE:

The **clear ancp access-loop** command has no effect in the following circumstances:

- The access line is reported to be down, as indicated by an ANCP Port Down message, when the command is issued.
 - An ANCP Port Down message is received for the access line while the dynamic VLAN logical interface and the services are being removed. In this case, re-authorization of the dynamic VLAN cannot take place until an ANCP Port Up message is received for that access line.
 - A conventionally autosensed dynamic VLAN (for the access provider's own subscriber sessions) has matching access loop attributes. In this case, the Layer 2 wholesale access line for which the command is intended is cleared, but the other VLAN, for sessions owned by the access-provider, is cleared as expected.
-

To clear an ANCP access loop:

- Identify the loop by the neighbor's IP address or the access-facing physical interface, and one or more of the ACI, ARI, and outer VLAN ID.

```
user@host> clear ancp access-loop neighbor 192.168.32.5 circuit-id line-aci-1 remote-id  
line-ari-1 outer-vlan-id 126
```

```
user@host> clear ancp access-loop subscriber-interface ge-1/0/1 circuit-id line-aci-1  
remote-id line-ari-1 outer-vlan-id 126
```

**Related
Documentation**

- [Layer 2 Wholesale with ANCP-Triggered VLANs Overview on page 99](#)

CHAPTER 10

Configuring Flat-File Accounting for Layer 2 Wholesale Services

- [Flat-File Accounting Overview on page 177](#)
- [Configuring Flat-File Accounting for Layer 2 Wholesale on page 181](#)
- [Configuring Flat-File Accounting for Extensible Subscriber Services Management on page 185](#)
- [Configuring Service Accounting in Local Flat Files on page 189](#)

Flat-File Accounting Overview

Accounting statistics can be collected from the Packet Forwarding Engine and reported in an XML flat file, which both contains and describes the data. Starting in Junos OS Release 16.1R4, you can use a flat-file profile that acts as a template to define attributes for accounting flat files.

Subscriber service accounting statistics are typically collected based on RADIUS Acct-Start and Acct-Stop messages that are sent to a RADIUS server individually or in bulk. Starting in Junos OS Release 17.1R1, you can alternatively configure service-filter-based accounting statistics to be recorded per subscriber in a local flat file that is not automatically forwarded to a RADIUS server. This configuration collects the running total service statistics per interface family. Service accounting is initiated when the service profile is attached to the interface, whether by a static configuration or a RADIUS Change of Authorization (CoA) message.

When the accounting file is created, a file header is also created if the file format is IP Detail Record (IPDR). The header is not created if the format is comma-separated variable (CSV). The file header includes the following information:

- XML namespace—Static link to the World Wide Web Consortium (W3C) organization's XML Schema Instance (XSI) definition.
- Schema version—Configurable name of the schema that defines the information conveyed in the accounting file. The schema version is associated with a specific XML format and output based on the flat-file profile configuration that is used for the business purpose. This structure enables the XML-formatted contents of the file to be correctly interpreted by the service provider's external file processor.

- NAS ID—Name of the BNG host (network access server) where the accounting statistics are collected.
- File creation timestamp—UTC time zone date and time when the accounting file was created.
- File ID—Number identifying the file. The ID is incremented when a new accounting file is created and can range from 1 through 2,147,483,647.

For example, consider the following sample header for an accounting file for Extensible Subscriber Services Manager (ESSM) business subscribers:

```
<BNGFile xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:noNamespaceSchemaLocation="BNG_IPDR_20130423.xsd" NAS-ID="host-mx480-x5"

  FileCreationTimeStamp="2015-10-09T08:25:50" FileID="29">
<IPDR>
.....
.....
</IPDR>
</BNGFile>
```

Table 13 on page 178 lists the elements and their values in the sample header.

Table 13: Value of Elements in Sample Accounting Flat File XML Header

Description	Header Element	Value
XML namespace	xmlns	:xsi="http://www.w3.org/2001/XMLSchema-instance"
schema version	xsi:noNamespaceSchemaLocation	BNG_IPDR_20130423.xsd
NAS ID	NAS-ID	host-mx480-x5
file creation timestamp	FileCreationTimeStamp	2015-10-09T08:25:50
File ID	FileID	29

You can configure the following options for flat-file accounting at the **[edit accounting-options file filename]** hierarchy level:

- Maximum size of the accounting file.
- Number of files that are saved before overwriting.
- One or more sites where the files are sent for archiving.
- Frequency at which the files are transferred to an archive site.
- Start time for file transfer.
- Compression for the transferred files.
- Local backup on the router for files when transfer fails.

- Whether accounting files are saved when a change in mastership occurs for both the new master Routing Engine and the new backup Routing Engine or for only the new master Routing Engine.
- How long files are kept before being deleted from the local backup directory.

You can also create one or more flat-file profiles at the **[edit accounting-options flat-file-profile *profile-name*]** hierarchy level that act as templates to specify the following attributes for new accounting files when they are created:

- Statistics fields that you want to collect, such as egress statistics or ingress statistics fields.
- Name and format of the accounting file.
- Frequency at which the Packet Forwarding Engine is polled for the statistics.
- Schema version.

Archive sites provide security and storage for the accounting files, which are transferred at regular intervals. When more than one archive site is configured, the router attempts to transfer the files to the first site on the list. If that fails, the router tries each of the other sites in turn until the transfer either succeeds for one site or fails for all sites. If you configure the last site in the list to be a local directory on the router rather than another remote site, then the files are backed up locally if all remote sites fail. The failed files are simply stored in the designated site. They are not automatically resubmitted to the archival sites. You must use an event script or some other means to have these files resubmitted. Any files remaining in the local directory are deleted when the **cleanup-interval** expires.

Alternatively, you can use the **backup-on-failure** statement at the **[edit accounting-options file *filename*]** hierarchy level to back up the files locally if all the remote attempts fail. If that occurs, the router compresses the accounting files and backs them up to the **/var/log/pfedBackup/** directory. Whenever any of the archive sites is reachable, the router attempts to transfer the data from **/var/log/pfedBackup/** to that site in compressed format. If the transfer of the backed-up files to the reachable site fails, the system tries to transfer the files to any other site that becomes reachable during the transfer interval. Any files that fail to transfer are compressed and kept in **/var/log/pfedBackup/** until an archival site is reachable and the files are successfully transferred. Any files that remain in that directory are deleted when the **cleanup-interval** expires.



BEST PRACTICE: Use the **backup-on-failure** feature to reliably and automatically back up files and retransmit them to archives rather than relying on a local site listed as the last archive site.

If the backup Routing Engine does not have access to the archive site—for example, when the site is not connected by means of an out-of-band interface or when the path to the site is routed through a line card—you can ensure that the backup Routing Engine's accounting files are backed up by using the **push-backup-to-master** statement at the **[edit accounting-options file *filename*]** hierarchy level. When a change in mastership

occurs, the new backup Routing Engine saves its files to the `/var/log/pfedBackup/` directory. The master Routing Engine subsequently includes these files when it sends its own accounting files to the archive site at every transfer interval.

To conserve resources during transfer of accounting files and at the archive site, use the **compress** statement at the **[edit accounting-options file *filename*]** hierarchy level to compress the files when they are transferred. This option is disabled by default.

A system logging message is generated when a transfer succeeds (**transfer-file: Transferred *filename***) or fails (**transfer-file failed to transfer**). In the event of a failure, an error message is logged to indicate the nature of the failure.

Release History Table

Release	Description
17.1R1	Starting in Junos OS Release 17.1R1, you can alternatively configure service-filter-based accounting statistics to be recorded per subscriber in a local flat file that is not automatically forwarded to a RADIUS server.
16.1R4	Starting in Junos OS Release 16.1R4, you can use a flat-file profile that acts as a template to define attributes for accounting flat files.

Related Documentation

- [Configuring Flat-File Accounting for Extensible Subscriber Services Management on page 185](#)
- [Configuring Flat-File Accounting for Layer 2 Wholesale on page 181](#)
- [Configuring Service Accounting in Local Flat Files on page 189](#)
- [Configuring Accounting-Data Log Files](#)

Configuring Flat-File Accounting for Layer 2 Wholesale

Flat-file accounting is typically used for recording accounting statistics on logical interfaces for Extensible Subscriber Services Manager (ESSM) business subscribers. However, starting in Junos OS Release 16.1R4, you can also use flat-file accounting to collect and archive various accounting statistics for your Layer 2 wholesale environment. You do this by creating a flat-file profile and applying it to a core-facing physical interface.

You can also configure a flat-file profile to monitor and report Layer 2 multicast statistics; you assign this profile to the logical interface configured on the core-facing physical interface. This approach enables you to have separate accounting files that overlap in content only in the non-statistical, general parameters. The Layer 2 multicast statistics are available only when the encapsulation on the logical interface is **ethernet-vpls**.

You can configure multiple accounting profiles with different combinations of fields for specific accounting requirements, and then assign the profiles as needed to provisioned interfaces to satisfy the accounting requirements for each interface depending on how the interface is used.

A given flat-file profile can be assigned to both use cases; for example, by specifying **all-fields** for a global or group level. In this case, the fields you configure appear in the accounting record only if they make sense in the context.



BEST PRACTICE: We recommend you use separate flat-file profiles for Layer 2 wholesale core-facing physical interfaces and ESSM business subscriber logical interfaces.

Some statistics and general parameter fields are available either only for logical interfaces or only for physical interfaces. The **accounting-type**, **line-id**, **nas-port-id**, and **vlan-id** general parameters are not available for core-facing physical interfaces. Because the core-facing physical interfaces carry Layer 2 cross-connected sessions, no useful IPv6 statistics are available. Accordingly, do not configure the **input-v6-bytes**, **input-v6-packets**, **output-v6-bytes**, or **output-v6-packets** overall packet fields.

To configure flat-file accounting for a Layer 2 wholesale network:

1. Create a flat-file profile.

```
[edit accounting-options]
user@host# edit flat-file-profile profile-name
```

2. (Optional) Configure the name of the XML schema for the accounting flat file.

```
[edit accounting-options flat-file-profile profile-name]
user@host# set schema-version schema-name
```

3. Specify the filename for the accounting file.

```
[edit accounting-options flat-file-profile profile-name]
user@host# set file accounting-filename
```

4. Specify the general, nonstatistical parameters for the accounting file that are displayed as part of the accounting record header.

```
[edit accounting-options flat-file-profile profile-name fields]  
user@host# set general-param option
```



BEST PRACTICE: We recommend that you include the general parameter **all-fields** option for both core-facing physical interfaces and, when you are collecting Layer 2 multicast statistics, on the logical interface that represents the physical interface.

5. Specify the accounting statistics that are collected and recorded in the accounting file for the core-facing physical interface.

```
[edit accounting-options flat-file-profile profile-name fields]  
user@host# set egress-stats option  
user@host# set ingress-stats option  
user@host# set overall-packet option
```



BEST PRACTICE: We recommend that you include the following statistics fields in flat-file profiles for core-facing physical interfaces:

- Egress statistics fields: all-fields
 - Ingress statistics fields: all-fields
 - Overall packet fields: input-bytes, input-discards, input-errors, input-packets, output-bytes, output-errors, output-packets
-

6. (Optional) For Layer 2 multicast statistics, specify the accounting statistics that are collected and recorded in the accounting file for the logical interface representing the core-facing physical interface.

```
[edit accounting-options flat-file-profile profile-name fields]  
user@host# set l2-stats option
```



BEST PRACTICE: We recommend that you include the following statistics fields in flat-file profiles for logical interfaces on the core-facing physical interfaces:

- Layer 2 statistics fields: all-fields
-

7. (Optional) Specify the format of the accounting file.

```
[edit accounting-options flat-file-profile profile-name]  
user@host# set format (csv | ipdr)
```

8. (Optional) Specify the interval at which the Packet Forwarding Engine associated with the interface is polled for the statistics specified in the profile.

```
[edit accounting-options flat-file-profile profile-name]
user@host# set interval minutes
```



NOTE: When you do not configure this option, the polling interval is 15 minutes.

9. Configure the maximum size of the accounting file.

```
[edit accounting-options file filename]
user@host# set size bytes
```

10. Configure one or more archive sites for the files.

```
[edit accounting-options file filename]
user@host# set archive-sites site-name
```

The **site-name** is any valid FTP or Secure FTP URL. When the file is archived, the router attempts to transfer the file to the archive site. If you have specified more than one site, it tries the first site in the list. If that fails, it tries each site in turn until a transfer succeeds. The log file is stored at the archive site with a filename of the format **router-name_log-filename_timestamp**. The last site in a list is often a local directory, in case no remote site is reachable.

11. (Optional) Configure the start time for transferring files.

```
[edit accounting-options file filename]
user@host# set start-time YYYY-MM-DD.hh:mm
```

12. (Optional) Configure how frequently the file is transferred.

```
[edit accounting-options file filename]
user@host# set transfer-interval minutes
```



NOTE: When you do not configure this option, the file is transferred every 30 minutes.

13. (Optional) Configure the maximum number of files (3 through 1000) to save.

```
[edit accounting-options file filename]
user@host# set files number
```



NOTE: When you do not configure this option, a maximum of 10 files are saved.

14. (Optional) Configure the router to save a backup copy of the accounting file to the `/var/log/pfedBackup` directory if the normal transfer of the files to the archive sites fails.

```
[edit accounting-options file filename]  
user@host# set backup-on-failure
```



NOTE: When you do not configure this option, the file is saved on failure into the local directory specified as the last site in the list of archive sites.

15. (Optional) Configure the accounting file to be compressed during transfer to an archive site.

```
[edit accounting-options file filename]  
user@host# set compress
```

16. (Optional) Configure the router's new backup Routing Engine to send its accounting file to the `/var/log/pfedBackup` directory on the new master Routing Engine when a change in mastership occurs.

```
[edit accounting-options file filename]  
user@host# set push-backup-to-master
```

17. (Optional) Configure the number of days after which accounting files are deleted from the local backup directory.

```
[edit accounting-options]  
user@host# set cleanup-interval days
```



NOTE: Files are retained for 1 day if you do not configure this option.

18. Assign the profile to the relevant interface.

For the core-facing physical interface:

```
[edit interfaces physical-interface-name]  
user@host# set accounting-profile flat-file-profile-name
```

For the logical interface representing the core-facing physical interface:

```
[edit interfaces physical-interface-name unit logical-unit-number]  
user@host# set accounting-profile flat-file-profile-name
```

Release History Table

Release	Description
16.1R4	However, starting in Junos OS Release 16.1R4, you can also use flat-file accounting to collect and archive various accounting statistics for your Layer 2 wholesale environment.

Related Documentation

- [Configuring Accounting-Data Log Files](#)
- [Flat-File Accounting Overview on page 177](#)
- [Configuring Flat-File Accounting for Extensible Subscriber Services Management on page 185](#)
- [Layer 2 Wholesale with ANCP-Triggered VLANs Overview on page 99](#)

Configuring Flat-File Accounting for Extensible Subscriber Services Management

Flat-file accounting is typically used to collect and archive various accounting statistics on logical interfaces for Extensible Subscriber Services Manager (ESSM) business subscribers. Other applications include accounting for wholesaler and retailer subscriber activity in a Layer 2 wholesale environment. Starting in Junos OS Release 16.1R4, you can create a flat-file profile to use as a template to define attributes for accounting flat files. The profile specifies the following:

- The statistics fields that are collected.
- The filename where the statistics are logged.
- The format of the file, the interval at which the statistics are collected.
- The name of the XML schema file that specifies the contents of the accounting file.

You can configure multiple accounting profiles with different combinations of fields for specific accounting requirements, and then assign the profiles as needed to provisioned interfaces to satisfy the accounting requirements for each interface depending on how it is used.

A given flat-file profile can be assigned to both use cases; for example, by specifying **all-fields** for a global or group level. In this case, the fields you configure appear in the accounting record only if they make sense in the context.



BEST PRACTICE: We recommend you use separate flat-file profiles for ESSM business subscriber logical interfaces and Layer 2 wholesale core-facing physical interfaces.

To configure flat-file accounting for ESSM business services:

1. Create a flat-file profile.
[edit accounting-options]

```
user@host# edit flat-file-profile profile-name
```

2. (Optional) Configure the name of the XML schema for the accounting flat file.

```
[edit accounting-options flat-file-profile profile-name]  
user@host# set schema-version schema-name
```

3. Specify the filename for the accounting file.

```
[edit accounting-options flat-file-profile profile-name]  
user@host# set file accounting-filename
```

4. Specify the general, nonstatistical parameters for the accounting file that are displayed as part of the accounting record header.

```
[edit accounting-options flat-file-profile profile-name fields]  
user@host# set general-param option
```



BEST PRACTICE: We recommend that you include the following general parameter fields in flat-file profiles for ESSM subscribers:

- General parameter fields: accounting-type, descr, line-id, logical-interface, nas-port-id, timestamp, and vlan-id

5. Specify the accounting statistics that are collected and recorded in the accounting file.

```
[edit accounting-options flat-file-profile profile-name fields]  
user@host# set egress-stats option  
user@host# set ingress-stats option;  
user@host# set overall-packet option;
```



BEST PRACTICE: We recommend that you include the following statistics fields in flat-file profiles for core-facing physical interfaces:

- Egress statistics fields: all-fields
- Ingress statistics fields: all-fields
- Overall packet fields: all-fields

6. (Optional) Specify the format of the accounting file.

```
[edit accounting-options flat-file-profile profile-name]  
user@host# set format (csv | ipdr)
```

7. (Optional) Specify the interval at which the Packet Forwarding Engine associated with the interface is polled for the statistics specified in the profile.

```
[edit accounting-options flat-file-profile profile-name]
```



```
user@host# set interval minutes
```



NOTE: When you do not configure this option, the polling interval is 15 minutes.

8. Configure the maximum size of the accounting file.

```
[edit accounting-options file filename]
user@host# set size bytes
```

9. Configure one or more archive sites for the files.

```
[edit accounting-options file filename]
user@host# set archive-sites site-name
```

The **site-name** is any valid FTP or Secure FTP URL. When the file is archived, the router attempts to transfer the file to the archive site. If you have specified more than one site, it tries the first site in the list. If that fails, it tries each site in turn until a transfer succeeds. The log file is stored at the archive site with a filename of the format **router-name_log-filename_timestamp**. The last site in a list is often a local directory, in case no remote site is reachable.

10. (Optional) Configure the start time for transferring the file.

```
[edit accounting-options file filename]
user@host# set start-time YYYY-MM-DD.hh:mm
```

11. (Optional) Configure how frequently the file is transferred.

```
[edit accounting-options file filename]
user@host# set transfer-interval minutes
```



NOTE: When you do not configure this option, the file is transferred every 30 minutes.

12. (Optional) Configure the maximum number of files (3 through 1000) to save.

```
[edit accounting-options file filename]
user@host# set files number
```



NOTE: When you do not configure this option, a maximum of 10 files are saved.

13. (Optional) Configure the router to save a backup copy of the accounting file to the **/var/log/pfedBackup** directory if the normal transfer of the files to the archive sites

fails. Specify whether only the current file from the master Routing Engine is saved or both that file and the file from the backup Routing Engine.

```
[edit accounting-options file filename]
user@host# set backup-on-failure (master-and-slave | master-only)
```



NOTE: When you do not configure this option, the file is saved on failure into the local directory specified as the last site in the list of archive sites.

14. (Optional) Configure the accounting file to be compressed during transfer to an archive site.

```
[edit accounting-options file filename]
user@host# set compress
```

15. (Optional) Configure the router's new backup Routing Engine to send its accounting file to the `/var/log/pfedBackup` directory on the new master Routing Engine when a change in mastership occurs.

```
[edit accounting-options file filename]
user@host# set push-backup-to-master
```

16. (Optional) Configure the number of days after which accounting files are deleted from the local backup directory.

```
[edit accounting-options]
user@host# set cleanup-interval days
```



NOTE: Files are retained for 1 day if you do not configure this option.

17. Assign the profile to an ESSM subscriber.

```
[edit system services extensible-subscriber-services]
user@host# set flat-file-profile flat-file-profile-name
```

Release History Table

Release	Description
16.1R4	Starting in Junos OS Release 16.1R4, you can create a flat-file profile to use as a template to define attributes for accounting flat files.

Related Documentation

- [Configuring Accounting-Data Log Files](#)
- [Configuring Flat-File Accounting for Layer 2 Wholesale on page 181](#)

Configuring Service Accounting in Local Flat Files

Starting in Junos OS Release 17.1R1, you can configure flat-file accounting to collect service statistics for subscribers and report those statistics to a local file. This configuration collects the running total service statistics per interface family. Because the statistics are maintained in the Routing Engine in a statistics database, they are not affected by a line-card restart, a graceful Routing Engine switchover, or a unified in-service software upgrade (ISSU). The statistics counters are reset when the router reboots.

To configure local flat-file accounting for services:

1. Configure the subscriber access profile to report service accounting records in a local flat file.

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



NOTE: When you configure `local`, the CLI checks at commit that the flat-file profile is configured under `[edit access profile profile-name local]`.

Alternatively, you can set the service accounting order to `activation-protocol` instead of `local`:

```
user@host# set service accounting-order activation-protocol
```

Use this option only when you plan to activate the service by means of the CLI configuration or a command. In this case, the CLI does not check for the flat-file profile to be configured. If the profile is not configured, no statistics are collected.



NOTE: When you configure the `local` option, both volume and time statistics are collected for the service accounting sessions. In this case, you must not configure the `volume-time` option at the `[edit access profile profile-name service accounting statistics]` hierarchy level; otherwise, an error is generated when you commit the configuration.

2. Specify the name of the flat-file profile that is used to collect the service statistics.

```
[edit access profile profile-name]
user@host# set local flat-file-profile flat-file-profile-name
```

3. Create the flat-file profile to collect the subscriber service accounting statistics and other parameters.

```
[edit accounting-options]
user@host# edit flat-file-profile profile-name
```

4. Specify the filename for the accounting file.

```
[edit accounting-options flat-file-profile profile-name]
user@host# set file accounting-filename
```

5. Specify that service accounting statistics are collected.

```
[edit accounting-options flat-file-profile profile-name fields]
user@host# set service-accounting
```

6. (Optional) Specify the general, nonstatistical parameters for the accounting file that are displayed as part of the accounting record header.

```
[edit accounting-options flat-file-profile profile-name fields]
user@host# set general-param option
```

7. (Optional) Configure the name of the XML schema for the accounting flat file.

```
[edit accounting-options flat-file-profile profile-name]
user@host# set schema-version schema-name
```

8. (Optional) Specify the format of the accounting file.

```
[edit accounting-options flat-file-profile profile-name]
user@host# set format (csv | ipdr)
```



NOTE: When you do not configure this option, the format is ipdr.

9. (Optional) Specify the interval at which the Packet Forwarding Engine associated with the interface is polled for the statistics specified in the profile.

```
[edit accounting-options flat-file-profile profile-name]
user@host# set interval minutes
```



NOTE: When you do not configure this option, the polling interval is 15 minutes.



NOTE:

The interval value configured in the flat-file profile can be overridden by other interval values:

- The service accounting update interval configured at the edit access profile *profile-name* service accounting update-interval] hierarchy level.
 - An update interval value configured in the RADIUS attribute, Service-Interim-Acct-Interval (VSA 26–140). This value also overrides the service accounting update interval.
-

10. Configure the maximum size of the accounting file.

```
[edit accounting-options file filename]
user@host# set size bytes
```

11. (Optional) Configure the maximum number of files (3 through 1000) to save.

```
[edit accounting-options file filename]
user@host# set files number
```



NOTE: When you do not configure this option, a maximum of 10 files are saved.

12. (Optional) Configure one or more archive sites for the files.

```
[edit accounting-options file filename]
user@host# set archive-sites site-name
```

The ***site-name*** is any valid FTP or Secure FTP URL. When the file is archived, the router attempts to transfer the file to the archive site. If you have specified more than one site, it tries the first site in the list. If that fails, it tries each site in turn until a transfer succeeds. The log file is stored at the archive site with a filename of the format ***router-name_log-filename_timestamp***. The last site in a list is often a local directory, in case no remote site is reachable.

13. (Optional) Configure the start time for transferring files.

```
[edit accounting-options file filename]
user@host# set start-time YYYY-MM-DD.hh:mm
```

14. (Optional) Configure how frequently the file is transferred.

```
[edit accounting-options file filename]
user@host# set transfer-interval minutes
```



NOTE: When you do not configure this option, the file is transferred every 30 minutes.

15. (Optional) Configure the router to save a backup copy of the accounting file to the ***/var/log/pfedBackup*** directory if the normal transfer of the files to the archive sites fails.

```
[edit accounting-options file filename]
user@host# set backup-on-failure
```



NOTE: When you do not configure this option, the file is saved on failure into the local directory specified as the last site in the list of archive sites.

16. (Optional) Configure the accounting file to be compressed during transfer to an archive site.

```
[edit accounting-options file filename]  
user@host# set compress
```

17. (Optional) Configure the router's new backup Routing Engine to send its accounting file to the `/var/log/pfedBackup` directory on the new master Routing Engine when a change in mastership occurs.

```
[edit accounting-options file filename]  
user@host# set push-backup-to-master
```

18. (Optional) Configure the number of days after which accounting files are deleted from the local backup directory.

```
[edit accounting-options]  
user@host# set cleanup-interval days
```



NOTE: When you do not configure this option, files are retained for only 1 day.

Release History Table

Release	Description
17.1R1	Starting in Junos OS Release 17.1R1, you can configure flat-file accounting to collect service statistics for subscribers and report those statistics to a local file.

Related Documentation

- [Configuring Accounting-Data Log Files](#)
- [Flat-File Accounting Overview on page 177](#)

PART 5

Configuration Statements and Operational Commands

- [Configuration Statements on page 195](#)
- [Operational Commands on page 419](#)

CHAPTER 11

Configuration Statements

- [accept](#) on page 199
- [accept-out-of-band](#) on page 200
- [access-profile](#) on page 201
- [access-profile \(Dynamic VLAN\)](#) on page 202
- [access-profile \(Dynamic Stacked VLAN\)](#) on page 203
- [accounting-server](#) on page 204
- [active-server-group](#) on page 205
- [address](#) on page 206
- [address-assignment \(Address-Assignment Pools\)](#) on page 209
- [adjacency-loss-hold-time \(ANCP\)](#) on page 210
- [ancp](#) on page 211
- [authentication](#) on page 213
- [authentication \(DHCP Local Server\)](#) on page 214
- [authentication \(DHCP Relay Agent\)](#) on page 215
- [authentication-order](#) on page 216
- [authentication-server](#) on page 217
- [auto-configure](#) on page 218
- [auto-configure-trigger interface \(ANCP\)](#) on page 219
- [backup-on-failure \(Accounting Options\)](#) on page 220
- [circuit-id \(VLAN Authentication Username\)](#) on page 221
- [cleanup-interval \(Accounting Options\)](#) on page 222
- [compress \(Accounting Options\)](#) on page 223
- [connectivity-type](#) on page 224
- [core-facing](#) on page 225
- [demux0 \(Dynamic Interface\)](#) on page 226
- [demux-options \(Dynamic Interface\)](#) on page 227
- [demux-source \(Dynamic IP Demux Interface\)](#) on page 228
- [demux-source \(Dynamic Underlying Interface\)](#) on page 229

- [demux-source \(Underlying Interface\)](#) on page 230
- [dhcp-attributes \(Address-Assignment Pools\)](#) on page 231
- [dhcp-local-server](#) on page 233
- [dhcp-relay](#) on page 239
- [dhcpv6 \(DHCP Local Server\)](#) on page 248
- [domain-name \(Address-Assignment Pools\)](#) on page 251
- [dynamic-profile \(DHCP Local Server\)](#) on page 252
- [dynamic-profile \(DHCP Relay Agent\)](#) on page 253
- [dynamic-profile \(Dynamic PPPoE\)](#) on page 254
- [dynamic-profile \(Stacked VLAN\)](#) on page 255
- [dynamic-profile \(VLAN\)](#) on page 256
- [dynamic-profiles](#) on page 257
- [egress-stats \(Flat-File Accounting Options\)](#) on page 266
- [encapsulation \(Dynamic Interfaces\)](#) on page 268
- [encapsulation \(Logical Interface\)](#) on page 271
- [encapsulation \(Physical Interface\)](#) on page 275
- [exclude \(RADIUS\)](#) on page 281
- [family](#) on page 286
- [family \(Address-Assignment Pools\)](#) on page 291
- [family \(Dynamic Demux Interface\)](#) on page 292
- [family \(Dynamic PPPoE\)](#) on page 293
- [family \(Dynamic Standard Interface\)](#) on page 294
- [fields \(Flat-File Accounting Options\)](#) on page 296
- [file \(Flat-File Accounting Options\)](#) on page 298
- [flat-file-profile \(Accounting Options\)](#) on page 299
- [flat-file-profile \(Extensible Subscriber Services\)](#) on page 301
- [flexible-vlan-tagging](#) on page 302
- [format \(Flat-File Accounting Options\)](#) on page 303
- [forwarding-options](#) on page 304
- [general-param \(Flat-File Accounting Options\)](#) on page 305
- [grace-period](#) on page 306
- [group \(DHCP Local Server\)](#) on page 307
- [group \(DHCP Relay Agent\)](#) on page 310
- [ingress-stats \(Flat-File Accounting Options\)](#) on page 314
- [inner-vlan-id \(Dynamic VLANs\)](#) on page 315
- [inner-vlan-id-swap-ranges](#) on page 316
- [input-vlan-map \(Dynamic Interfaces\)](#) on page 317

- [interface \(DHCP Local Server\)](#) on page 318
- [interface \(DHCP Relay Agent\)](#) on page 320
- [interface \(Dynamic Routing Instances\)](#) on page 322
- [interface \(Routing Instances\)](#) on page 323
- [interface-mac-limit \(VPLS\)](#) on page 324
- [interfaces](#) on page 325
- [interfaces \(Static and Dynamic Subscribers\)](#) on page 326
- [interval \(Flat-File Accounting Options\)](#) on page 331
- [instance-role](#) on page 332
- [instance-type](#) on page 333
- [ip-address-first](#) on page 335
- [keepalives \(Dynamic Profiles\)](#) on page 336
- [l2-stats \(Flat-File Accounting Options\)](#) on page 337
- [mac-validate \(Dynamic IP Demux Interface\)](#) on page 338
- [multicast-replication](#) on page 339
- [neighbor \(Define ANCP\)](#) on page 340
- [no-local-switching](#) on page 340
- [no-tunnel-services](#) on page 341
- [maximum-lease-time](#) on page 342
- [overall-packet \(Flat-File Accounting Options\)](#) on page 343
- [output-vlan-map \(Dynamic Interfaces\)](#) on page 344
- [pap \(Dynamic PPP\)](#) on page 345
- [pool \(Address-Assignment Pools\)](#) on page 346
- [pool-match-order](#) on page 347
- [pop \(Dynamic VLANs\)](#) on page 348
- [pppoe-options \(Dynamic PPPoE\)](#) on page 348
- [pppoe-underlying-options \(Static and Dynamic Subscribers\)](#) on page 349
- [ppp-options \(Dynamic PPP\)](#) on page 350
- [prefix \(Address-Assignment Pools\)](#) on page 351
- [profile \(Access\)](#) on page 352
- [protocols](#) on page 357
- [proxy-arp](#) on page 360
- [proxy-arp \(Dynamic Profiles\)](#) on page 361
- [push \(Dynamic VLANs\)](#) on page 361
- [push-backup-to-master \(Accounting Options\)](#) on page 362
- [radius \(Access Profile\)](#) on page 363
- [radius-server](#) on page 365

- [range \(Address-Assignment Pools\)](#) on page 366
- [ranges \(Dynamic VLAN\)](#) on page 367
- [remote-id \(VLAN Authentication Username\)](#) on page 368
- [route-distinguisher](#) on page 369
- [routing-instances \(Dynamic Profiles\)](#) on page 371
- [routing-instances \(Multiple Routing Entities\)](#) on page 373
- [schema-version \(Flat-File Accounting Options\)](#) on page 374
- [secret](#) on page 375
- [server \(Dynamic PPPoE\)](#) on page 376
- [server-group](#) on page 377
- [site \(VPLS Multihoming for FEC 128\)](#) on page 378
- [site-identifier \(VPLS\)](#) on page 379
- [site-range](#) on page 380
- [stacked-vlan-ranges](#) on page 381
- [stacked-vlan-tagging](#) on page 382
- [system](#) on page 382
- [traceoptions \(DHCP\)](#) on page 383
- [underlying-interface \(demux0\)](#) on page 385
- [underlying-interface \(Dynamic PPPoE\)](#) on page 386
- [unit](#) on page 387
- [unit \(Dynamic Demux Interface\)](#) on page 394
- [unit \(Dynamic Profiles Standard Interface\)](#) on page 396
- [unnumbered-address \(Dynamic PPPoE\)](#) on page 399
- [unnumbered-address \(Dynamic Profiles\)](#) on page 400
- [unnumbered-address \(Ethernet\)](#) on page 402
- [username-include](#) on page 403
- [user-prefix \(DHCP Local Server\)](#) on page 404
- [vlan-id \(Dynamic VLANs\)](#) on page 405
- [vlan-id \(VLAN ID to Be Bound to a Logical Interface\)](#) on page 406
- [vlan-model](#) on page 407
- [vlan-ranges](#) on page 408
- [vlan-tags](#) on page 409
- [vlan-tags \(Stacked VLAN Tags\)](#) on page 410
- [vpls \(Routing Instance\)](#) on page 412
- [vrf-export](#) on page 414
- [vrf-import](#) on page 415
- [vrf-target](#) on page 416

accept

Syntax `accept (any | dhcp-v4 | dhcp-v6 | inet | inet6 | pppoe);`

Hierarchy Level `[edit interfaces interface-name auto-configure stacked-vlan-ranges dynamic-profile profile-name],`
`[edit interfaces interface-name auto-configure vlan-ranges dynamic-profile profile-name]`

Release Information Statement introduced in Junos OS Release 9.5.
dhcp-v4 option added in Junos OS Release 10.0.
dhcp-v6, **inet6** and **pppoe** options added in Junos OS Release 10.2.
any option added in Junos OS Release 10.4.

Description Specify the type of VLAN Ethernet packet accepted by an interface that is associated with a VLAN dynamic profile or stacked VLAN dynamic profile.

Options **any**—Any packet type. Specifies that any incoming packets trigger the dynamic creation of a VLAN with properties determined by the auto-configure interface configuration stanza and associated profile attributes. This option is used when configuring wholesaling in a Layer 2 network.

dhcp-v4—IPv4 DHCP packet type. Specifies that incoming IPv4 DHCP discover packets trigger the dynamic creation of a VLAN with properties determined by the auto-configure interface configuration stanza and associated profile attributes



NOTE: The DHCP-specific **mac-address** and **option-82** options are rejected if the **accept** statement is not set to **dhcp-v4**.

dhcp-v6—IPv6 DHCP packet type. Specifies that incoming IPv6 DHCP discover packets trigger the dynamic creation of a VLAN with properties determined by the auto-configure interface configuration stanza and associated profile attributes.

inet—IPv4 Ethernet and ARP packet type.

inet6—IPv6 Ethernet packet type.

pppoe—Point-to-Point Protocol over Ethernet packet type.




NOTE: The **pppoe** VLAN Ethernet packet type option is supported only for MPC/MIC interfaces.

Required Privilege **interface**—To view this statement in the configuration.
Level **interface-control**—To add this statement to the configuration.

- Related Documentation**
- [Configuring an Interface to Use the Dynamic Profile Configured to Create Stacked VLANs](#)
 - [Configuring an Interface to Use the Dynamic Profile Configured to Create Single-Tag VLANs](#)
 - [Configuring VLAN Interfaces for the Layer 2 Wholesale Solution on page 82](#)
 - [Configuring Subscriber Packet Types to Trigger VLAN Authentication](#)

accept-out-of-band

Syntax	<code>accept-out-of-band protocol;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> auto-configure vlan-ranges dynamic-profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 16.1R4.
Description	Configure the protocol for which packets are accepted as out-of-band traffic to trigger instantiation or deletion of autosensed dynamic VLANs.
<div> NOTE: A given physical interface can support VLANs created by either conventional packet-triggering or out-of-band triggering, but not both at the same time.</div>	
Options	protocol —Out-of-band protocol. The following out-of-band protocol is supported: <ul style="list-style-type: none">• ancp—ANCP Port Up and Port Down messages trigger instantiation and deletion, respectively, of autosensed, dynamic VLAN.
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 Out-of-Band ANCP Messages to Trigger Dynamic VLAN Instantiation on page 169• Layer 2 Wholesale with ANCP-Triggered VLANs Overview on page 99

access-profile

Syntax	<code>access-profile <i>profile-name</i>;</code>
Hierarchy Level	<code>[edit],</code> <code>[edit forwarding-options dhcp-relay]</code> <code>[edit forwarding-options dhcp-relay dual-stack-group <i>dual-stack-group-name</i>],</code> <code>[edit forwarding-options dhcp-relay group <i>group-name</i>]</code> <code>[edit forwarding-options dhcp-relay dhcpv6]</code> <code>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i>]</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>]</code> <code>[edit interfaces <i>interface-name</i> auto-configure vlan-ranges],</code> <code>[edit interfaces <i>interface-name</i> auto-configure stacked-vlan-ranges],</code> <code>[edit routing-instances <i>routing-instances-name</i>]</code> <code>[edit system services dhcp-local-server]</code> <code>[edit system services dhcp-local-server group <i>group-name</i>]</code> <code>[edit system services dhcp-local-server dhcpv6]</code> <code>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i>]</code> <code>[edit system services dhcp-local-server dual-stack-group <i>dual-stack-group-name</i>]</code>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3 for ACX Series routers.</p>
Description	<p>After you have created the access profile that specifies authentication and accounting parameters, you must specify where the profile is used. Authentication and accounting will not run unless you specify the profile. You can attach access profiles globally at the [edit] hierarchy level, or you can apply them to DHCP clients or subscribers, VLANs, or to a routing instance.</p>
Options	<p><i>profile-name</i>—Name of the access profile that you configured at the [edit access profile name] hierarchy level.</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"> • Attaching Access Profiles • Attaching Access Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces • Configuring Access Components for the DHCP Layer 3 Wholesale Network Solution on page 16 • Configuring Access Components for the PPPoE Wholesale Network Solution on page 61

access-profile (Dynamic VLAN)

Syntax	<code>access-profile <i>vlan-access-profile-name</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> auto-configure vlan-ranges dynamic-profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 16.2.
Description	<p>Access profiles contain subscriber access authentication, authorization and accounting (AAA) configuration parameters. You can create an access profiles and then attach it at various configuration levels. When you attach an access profile to an interface configured for dynamic VLAN or stacked VLAN, all the VLANs and stacked VLANs use the same set of AAA parameters configured in that access profile. The different access profiles can have different authentication/authorization settings so you can, for example, have authentication on some VLAN or stacked VLAN ranges but no authentication on other ranges.</p> <p>You can assign different access profiles to different dynamic profiles on the same interface. If you assign an access profile at the global level, but a different access profile is assigned at the interface level, the access profile at the interface level authenticates all dynamic VLANs and stacked VLANs on the interface. Access profiles can be assigned at various levels, but the most specific access profile takes precedence over any other profile assignments.</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">• <i>Configuring an Interface to Use the Dynamic Profile Configured to Create Single-Tag VLANs</i>• show subscribers on page 606• <i>shmlog (Shared Memory Log)</i>

access-profile (Dynamic Stacked VLAN)

Syntax	<code>access-profile <i>svlan-access-profile-name</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> auto-configure stacked-vlan-ranges dynamic-profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 16.2.
Description	<p>Access profiles contain subscriber access authentication, authorization and accounting (AAA) configuration parameters. You can create an access profiles and then attach it at various configuration levels. When you attach an access profile to an interface configured for dynamic VLAN or stacked VLAN, all the VLANs and stacked VLANs use the same set of AAA parameters configured in that access profile. The different access profiles can have different authentication/authorization settings so you can, for example, have authentication on some VLAN and stacked VLAN ranges but no authentication on other ranges.</p> <p>You can assign different access profiles to different dynamic profiles on the same interface. If you assign an access profile at the global level, but a different access profile is assigned at the interface level, the access profile at the interface level authenticates all dynamic VLANs and stacked VLANs on the interface. Access profiles can be assigned at various levels, but the most specific access profile takes precedence over any other profile assignments..</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"> • <i>Configuring an Interface to Use the Dynamic Profile Configured to Create Stacked VLANs</i> • show subscribers on page 606 • <i>shmlog (Shared Memory Log)</i>

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">• <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i>

active-server-group

Syntax	<code>active-server-group <i>server-group-name</i>;</code>
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> 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>] </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>
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	<p><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.</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"> • <i>Extended DHCP Relay Agent Overview</i> • <i>Configuring Active Server Groups to Apply a Common DHCP Relay Agent Configuration to Named Server Groups</i> • <i>Configuring Group-Specific DHCP Relay Options</i> • dhcp-relay on page 239

address

```

Syntax  address address {
        arp ip-address (mac | multicast-mac) mac-address <publish>;
        broadcast address;
        destination address;
        destination-profile name;
        eui-64;
        master-only;
        multipoint-destination address dlcidlcid-identifier;
        multipoint-destination address {
            epd-threshold cells;
            inverse-arp;
            oam-liveness {
                up-count cells;
                down-count cells;
            }
            oam-period (disable | seconds);
            shaping {
                (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst
                 length);
                queue-length number;
            }
            vci vpi-identifier.vci-identifier;
        }
        primary;
        preferred;
        virtual-gateway-address
        (vrrp-group | vrrp-inet6-group) group-number {
            (accept-data | no-accept-data);
            advertise-interval seconds;
            authentication-type authentication;
            authentication-key key;
            fast-interval milliseconds;
            (preempt | no-preempt) {
                hold-time seconds;
            }
            priority-number number;
            track {
                priority-cost seconds;
                priority-hold-time interface-name {
                    interface priority;
                    bandwidth-threshold bits-per-second {
                        priority;
                    }
                }
            }
            route ip-address/mask routing-instance instance-name priority-cost cost;
        }
        virtual-address [ addresses ];
    }
}

```

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family *family*],

[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family *family*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 11.1 for the QFX Series.

Description Configure the interface address.

Options *address*—Address of the interface.

- In Junos OS Release 13.3 and later, when you configure an IPv6 host address and an IPv6 subnet address on an interface, the commit operation fails.
- In releases earlier than Junos OS Release 13.3, when you use the same configuration on an interface, the commit operation succeeds, but only one of the IPv6 addresses that was entered is assigned to the interface. The other address is not applied.



NOTE: If you configure the same address on multiple interfaces in the same routing instance, Junos OS uses only the first configuration, and the remaining address configurations are ignored and can leave interfaces without an address. Interfaces that do not have an assigned address cannot be used as a donor interface for an unnumbered Ethernet interface.

For example, in the following configuration the address configuration of interface xe-0/0/1.0 is ignored:

```
interfaces {
  xe-0/0/0 {
    unit 0 {
      family inet {
        address 192.168.1.1/8;
      }
    }
  }
  xe-0/0/1 {
    unit 0 {
      family inet {
        address 192.168.1.1/8;
      }
    }
  }
}
```

For more information on configuring the same address on multiple interfaces, see *Configuring the Interface Address*.

The remaining statements are explained separately. See [CLI Explorer](#).



NOTE: The edit logical-systems hierarchy is not available on QFabric systems.

Required Privilege interface—To view this statement in the configuration.
Level interface-control—To add this statement to the configuration.

Related Documentation

- *Configuring the Protocol Family*
- *Junos OS Administration Library*
- *family*
- *negotiate-address*
- [unnumbered-address \(Ethernet\) on page 402](#)

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 {
            active-drain;
            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;
                }
            }
            hold-down;
            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.

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. See [CLI Explorer](#).

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](#)
 - [Configuring Address-Assignment Pools](#)
 - [Configuring an Address-Assignment Pool for L2TP LNS with Inline Services](#)

adjacency-loss-hold-time (ANCP)

- Syntax** adjacency-loss-hold-time *seconds*;
- Hierarchy Level** [edit protocols [ancp](#)],
 [edit protocols ancp [neighbor ip-address](#)]
- Release Information** Statement introduced in Junos OS Release 16.1R4.
- Description** Configure the ANCP agent to monitor, either globally or for a specified neighbor, how long an ANCP adjacency is down and to trigger a state change for the subscriber access line if the hold timer expires before the adjacency comes back up, as indicated by a Port Up message on the access line. By default, there is no delay between detecting an adjacency loss and triggering the state change.
- Options** *seconds*—Duration of period that the ANCP agent monitors loss of adjacency.
 Default: 0 seconds
 Range: 0 through 1800 seconds
- 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 to Dampen the Effects of Short-Term Adjacency Losses on page 172](#)
 - [Configuring ANCP Neighbors on page 165](#)
 - [Configuring the ANCP Agent](#)
 - [Layer 2 Wholesale with ANCP-Triggered VLANs Overview on page 99](#)

ancp

```
Syntax  ancp {
    adjacency-loss-hold-time seconds;
    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-loss-hold-time seconds;
        adjacency-timer;
        auto-configure-trigger interface interface-name;
        ietf-mode;
        maximum-discovery-table-entries entry-number;
        pre-ietf-mode;
    }
    pre-ietf-mode;
    qos-adjust {
        adsl-bytes bytes;
        adsl2-bytes bytes;
        adsl2-plus-bytes bytes;
        other-bytes bytes;
        other-overhead-adjust percentage;
        sdsl-bytes bytes;
        sdsl-overhead-adjust percentage;
        vdsl-bytes bytes;
        vdsl-overhead-adjust percentage;
        vdsl2-bytes bytes;
        vdsl2-overhead-adjust percentage;
    }
    qos-adjust-adsl adjustment-factor;
    qos-adjust-adsl2 adjustment-factor;
    qos-adjust-adsl2-plus adjustment-factor;
    qos-adjust-other 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. See [CLI Explorer](#).



NOTE: When you deactivate the ANCP protocol, the router does not perform a commit check to determine whether any ANCP or L2-BSA subscribers are present (active or inactive). Any subscribers that are active at the time of deactivation remain active.

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*

authentication

Syntax	<pre> authentication { packet-types [<i>packet-types</i>]; password <i>password-string</i>; username-include { <i>circuit-id</i>; circuit-type; delimiter <i>delimiter-character</i>; domain-name <i>domain-name-string</i>; interface-name; mac-address; option-18; option-37; option-82 <<i>circuit-id</i>> <<i>remote-id</i>>; radius-realm <i>radius-realm-string</i>; <i>remote-id</i>; user-prefix <i>user-prefix-string</i>; } }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> auto-configure vlan-ranges], [edit interfaces <i>interface-name</i> auto-configure stacked-vlan-ranges]
Release Information	Statement introduced in Junos OS Release 10.0.
Description	<p>Specify the authentication parameters that trigger the Access-Request message to AAA for the interface.</p> <p>The remaining statements are explained separately. See CLI Explorer.</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 • Configuring the Static Subscriber Global Authentication Password • Configuring a Username for Authentication of Out-of-Band Triggered Dynamic VLANs on page 168 • Layer 2 Wholesale with ANCP-Triggered VLANs Overview on page 99


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-description (device-interface logical-interface); 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 dual-stack-group <i>dual-stack-group-name</i>], [edit system services dhcp-local-server dhcpv6], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i>], [edit system services dhcp-local-server group <i>group-name</i>], [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. See CLI Explorer.</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>Using External AAA Authentication Services with DHCP</i>

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-description (device-interface logical-interface); 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 dual-stack-group <i>dual-stack-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> <p>Support at the [edit ... dual-stack-group <i>dual-stack-group-name</i>] hierarchy level introduced in Junos OS Release 15.1.</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. See CLI Explorer.</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 239 • Using External AAA Authentication Services with DHCP

authentication-order

Syntax	authentication-order [<i>authentication-methods</i>];
Hierarchy Level	[edit access <i>profile profile-name</i>]
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> <p>none option added in Junos OS Release 11.2.</p> <p>nasreq option added in Junos OS Release 16.1.</p>
Description	<p>Set the order in which AAA tries different authentication methods when verifying that a client can access the router or switch. For each login attempt, AAA tries the authentication methods in order, from first to last.</p> <p>A given subscriber does not undergo both authentication and authorization as separate steps. When both authentication-order and authorization-order are specified, DHCP subscribers honor the configured authorization order, all other subscribers use the configured authentication-order.</p>
Options	<p>authentication-methods—Ordered list of methods to use for authentication attempts. The list includes one or more of the following methods in any combination:</p> <ul style="list-style-type: none">• nasreq—Verify the client using NASREQ authentication services.• none—No authentication is performed. 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 [edit access <i>profile profile-name client client-name</i>] hierarchy level.• radius—Verify the client using RADIUS authentication services.
<div>NOTE: Subscriber access management does not support the password option, and authentication fails when no method (none) is specified.</div>	
Default: password	
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>• <i>Specifying the Authentication and Accounting Methods for Subscriber Access</i>• <i>Configuring Access Profiles for L2TP or PPP Parameters</i>

authentication-server

Syntax	<code>authentication-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 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">• <i>Configuring RADIUS Server Parameters for Subscriber Access</i>

auto-configure

```
Syntax auto-configure {
  vlan-ranges {
    access-profile profile-name;
    authentication {
      packet-types [packet-types];
      password password-string;
      username-include {
        circuit-id;
        circuit-type;
        delimiter delimiter-character;
        domain-name domain-name-string;
        interface-name;
        mac-address;
        option-18;
        option-37;
        option-82 <circuit-id> <remote-id>;
        radius-realm radius-realm-string;
        remote-id;
        user-prefix user-prefix-string;
      }
    }
    dynamic-profile profile-name {
      accept (any | dhcp-v4 | dhcp-v6 | inet | inet6 | pppoe);
      accept-out-of-band protocol;
      ranges (any | low-tag)–(any | high-tag);
    }
    override;
  }
  stacked-vlan-ranges {
    access-profile profile-name;
    authentication {
      packet-types [packet-types];
      password password-string;
      username-include {
        circuit-type;
        delimiter delimiter-character;
        domain-name domain-name-string;
        interface-name;
        mac-address;
        option-18;
        option-37;
        option-82 <circuit-id> <remote-id>;
        radius-realm radius-realm-string;
        user-prefix user-prefix-string;
      }
    }
    dynamic-profile profile-name {
      accept (any | dhcp-v4 | dhcp-v6 | inet | inet6 | pppoe);
      ranges (any | low-tag–high-tag), (any | low-tag–high-tag);
    }
    override;
  }
}
```



```

        remove-when-no-subscribers;
    }

```

Hierarchy Level [edit [interfaces](#) *interface-name*]

Release Information Statement introduced in Junos OS Release 9.5.

Description Enable the configuration of dynamic, auto-sensed VLANs.

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 an Interface to Use the Dynamic Profile Configured to Create Stacked VLANs*
- *Configuring an Interface to Use the Dynamic Profile Configured to Create Single-Tag VLANs*

auto-configure-trigger interface (ANCP)

Syntax auto-configure-trigger interface *interface-name*;

Hierarchy Level [edit protocols anc [neighbor](#) *ip-address*]

Release Information Statement introduced in Junos OS Release 16.1R4.

Description Map an ANCP neighbor to a subscriber-facing physical interface on the router, so that ANCP Port Up and Port Down messages trigger notifications to the auto-configuration daemon (autoconfd) to initiate VLAN creation (Port Up) or removal (Port Down).

Options *interface-name*—Name of the physical interface.

Required Privilege Level routing—To view this statement in the configuration.
 routing-control—To add this statement to the configuration.


Related Documentation

- [Configuring ANCP Neighbors on page 165](#)
- *Configuring the ANCP Agent*

backup-on-failure (Accounting Options)

Syntax	backup-on-failure (master-and-slave master-only);
Hierarchy Level	[edit accounting-options <i>file filename</i>]
Release Information	Statement introduced in Junos OS Release 16.1.
Description	Configure the router to save a copy of the accounting file locally, to the <code>/var/log/pfedBackup</code> directory of the relevant Routing Engine, in the event that file transfer to the remote archive sites cannot be completed.
Options	<p>master-and-slave—Back up accounting files from both the master Routing Engine and the backup Routing Engine.</p> <p>master-only—Back up accounting files from only the master Routing Engine.</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 Accounting-Data Log Files• Configuring Flat-File Accounting for Layer 2 Wholesale on page 181• Configuring Flat-File Accounting for Extensible Subscriber Services Management on page 185• Flat-File Accounting Overview on page 177

circuit-id (VLAN Authentication Username)

Syntax	circuit-id;
Hierarchy Level	[edit interfaces <i>interface-name</i> auto-configure vlan-ranges authentication username-include]
Release Information	Statement introduced in Junos OS Release 16.1R4.
Description	Include the agent circuit identifier (ACI) in the username sent to RADIUS for authentication of the dynamic VLAN. The ACI is conveyed by the Access-Loop-Circuit-ID TLV in an out-of-band ANCP Port Up message.
<div>  NOTE: This statement is not supported for stacked VLANs. </div>	
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 a Username for Authentication of Out-of-Band Triggered Dynamic VLANs on page 168 • Configuring VLAN Interface Username Information for AAA Authentication • Layer 2 Wholesale with ANCP-Triggered VLANs Overview on page 99

cleanup-interval (Accounting Options)

Syntax	cleanup-interval <i>days</i> ;
Hierarchy Level	[edit accounting-options]
Release Information	Statement introduced in Junos OS Release 16.1.
Description	Configure the interval to delete files from the local backup directory.
Options	days —Number of days after which accounting-options files are to be deleted from the backup directory. Range: 1 through 31 days Default: 1 day
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 Accounting-Data Log Files• Configuring Flat-File Accounting for Layer 2 Wholesale on page 181• Configuring Flat-File Accounting for Extensible Subscriber Services Management on page 185• Flat-File Accounting Overview on page 177

compress (Accounting Options)

Syntax	<code>compress;</code>
Hierarchy Level	[edit accounting-options file <i>filename</i>]
Release Information	Statement introduced in Junos OS Release 16.1.
Description	Compress the accounting file during file transfer to the backup site.
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 Accounting-Data Log Files• Configuring Flat-File Accounting for Layer 2 Wholesale on page 181• Configuring Flat-File Accounting for Extensible Subscriber Services Management on page 185• Flat-File Accounting Overview on page 177

connectivity-type

Syntax	<code>connectivity-type (ce irb permanent);</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls], [edit routing-instances <i>routing-instance-name</i> protocols vpls]
Release Information	Statement introduced in Junos OS Release 9.1. irb option introduced in Junos OS Release 9.3. permanent option introduced in Junos OS Release 10.4.
Description	Specify when a VPLS connection is taken down depending on whether or not the interface for the VPLS routing instance is customer-facing or integrated routing and bridging (IRB).



NOTE: The **connectivity-type** statement is not supported for FEC 129 VPLS (also known as LDP VPLS with BGP-based autodiscovery).

Default	ce
Options	<p>ce—Require that for the VPLS connection to be up, the customer-facing interface for the VPLS routing instance must also be up. If the customer-facing interface fails, the VPLS connection is taken down.</p> <p>irb—Allow a VPLS connection to remain up so long as an IRB interface is configured for the VPLS routing instance.</p> <p>permanent—Allow a VPLS connection to remain up until specifically taken down. This option is reserved for use in configuring Layer 2 Wholesale subscriber networks. See the <i>Broadband Subscriber Management Solutions Guide</i> for details about configuring a Layer 2 Wholesale network.</p>



NOTE: To specifically take down a VPLS routing instance that is using the **permanent** option, all associated static logical interfaces must also be down.

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 VPLS Routing Instances Configuring Separate NNI Routing Instances for Layer 2 Wholesale Service Retailers on page 89

core-facing

Syntax	core-facing;
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	Specifies that the VLAN is physically connected to a core-facing ISP router and ensures that the network does not improperly treat the interface as a client interface. When specified, the interface is inserted into the core-facing default mesh group where traffic from pseudowires that belong to the default mesh group is not forwarded on the core-facing link.
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>Junos OS Broadband Subscriber Management and Services Library</i>

demux0 (Dynamic Interface)

```
Syntax  demux0 {
        unit logical-unit-number {
            demux-options {
                underlying-interface interface-name
            }
            family family {
                access-concentrator name;
                address address;
                demux-source {
                    source-prefix;
                }
                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;
                rpf-check {
                    fail-filter filter-name;
                    mode loose;
                }
                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>;
            }
            filter {
                input filter-name;
                output filter-name;
            }
            vlan-id number;
        }
    }
```

Hierarchy Level [edit [dynamic-profiles](#) *profile-name* [interfaces](#)]

Release Information Statement introduced in Junos OS Release 9.3.

Description Configure the logical demultiplexing (demux) interface in a dynamic profile.

Logical IP demux interfaces do not support IPv4 and IPv6 dual stack.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

- Related Documentation**
- *Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles*
 - *Demultiplexing Interface Overview*

demux-options (Dynamic Interface)

Syntax	<pre>demux-options { underlying-interface interface-name }</pre>
Hierarchy Level	[edit dynamic-profiles profile-name interfaces demux0 interface-name unit logical-unit-number]
Release Information	Statement introduced in Junos OS Release 9.3.
Description	<p>Configure logical demultiplexing (demux) interface options in a dynamic profile.</p> <p>The remaining statement is explained separately.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles</i> • <i>Demultiplexing Interface Overview</i>

demux-source (Dynamic IP Demux Interface)

Syntax	<code>demux-source { source-address; }</code>
Hierarchy Level	[edit dynamic-profiles profile-name interfaces demux0 unit logical-unit-number family family]
Release Information	Statement introduced in Junos OS Release 9.3.
Description	Configure a logical demultiplexing (demux) source address for a subscriber in a dynamic profile.
Options	source-address —Either the specific source address you want to assign to the subscriber interface or the source address variable. For IPv4, specify \$junos-subscriber-ip-address ; for IPv6, specify \$junos-subscriber-ipv6-address . The source address for the interface is dynamically supplied by DHCP when the subscriber accesses the router.
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">• <i>Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles</i>• <i>Demultiplexing Interface Overview</i>

demux-source (Dynamic Underlying Interface)


Syntax	<code>demux-source <i>family</i>;</code>
Hierarchy Level	[edit <code>dynamic-profiles interfaces interface-name unit logical-unit-number</code>]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Configure the logical demultiplexing (demux) source family type on the IP demux underlying interface within a dynamic profile.



NOTE: The IP demux interface feature currently supports only Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet, or aggregated Ethernet underlying interfaces.

Options	<i>family</i> —Protocol family: <ul style="list-style-type: none"> • inet—Internet Protocol version 4 suite • inet6—Internet Protocol version 6 suite
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.

demux-source (Underlying Interface)

Syntax	<code>demux-source <i>family</i>;</code>
Hierarchy Level	<code>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> interfaces</code> <code> <i>interface-name</i> unit <i>logical-unit-number</i>]</code>
Release Information	Statement introduced in Junos OS Release 9.0. Support for aggregated Ethernet added in Junos OS Release 9.4.
Description	Configure the logical demultiplexing (demux) source family type on the IP demux underlying interface.
<div> NOTE: The IP demux interface feature currently supports only Fast Ethernet, Gigabit Ethernet, 10-Gigabit Ethernet, or aggregated Ethernet underlying interfaces.</div>	
Options	<i>family</i> —Protocol family: <ul style="list-style-type: none">• inet—Internet Protocol version 4 suite• inet6—Internet Protocol version 6 suite
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">• <i>Configuring an IP Demultiplexing Interface</i>• <i>Configuring a VLAN Demultiplexing Interface</i>

dhcp-attributes (Address-Assignment Pools)

Syntax

```
dhcp-attributes {
  boot-file filename;
  boot-server (address | hostname);
  dns-server [ ipv6-address ];
  domain-name domain-name;
  exclude-prefix-len exclude-prefix-length;
  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;
  t1-renewal-time;
  t2-percentage percentage;
  t2-rebinding-time;
  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.
exclude-prefix-len statement introduced in Junos OS Release 17.3 for MX Series.

Description Configure DHCP attributes for the protocol family in a specific address pool. The attributes determine options and behaviors for the DHCP clients.

The remaining statements are explained separately.

Options **exclude-prefix-len** *exclude-prefix-length*—Specify the length of the IPv6 prefix to be excluded from the delegated prefix.
Range: 1 through 128

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>Address-Assignment Pools Overview</i>• <i>DHCP Attributes for Address-Assignment Pools</i>• <i>Configuring Address-Assignment Pools</i>• <i>Configuring DHCP Client-Specific Attributes Applied When Clients Obtain an Address</i>

dhcp-local-server

```
Syntax  dhcp-local-server {
        access-profile profile-name;
        authentication {
            password password-string;
            username-include {
                circuit-type;
                delimiter delimiter-character;
                domain-name domain-name-string;
                interface-description (device-interface | logical-interface);
                interface-name;
                logical-system-name;
                mac-address;
                option-60;
                option-82 <circuit-id> <remote-id>;
                routing-instance-name;
                user-prefix user-prefix-string;
            }
        }
        dhcpv6 {
            access-profile profile-name;
            authentication {
                ...
            }
            duplicate-clients incoming-interface;
            group group-name {
                access-profile profile-name;
                authentication {
                    ...
                }
            }
            interface interface-name {
                access-profile profile-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 {
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
        pool pool-name;
    }
    protocol-attributes attribute-set-name;
    rapid-commit;
}
service-profile dynamic-profile-name;
trace;
upto upto-interface-name;
}
overrides {
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    delegated-pool;
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
        pool pool-name;
    }
    protocol-attributes attribute-set-name;
    rapid-commit;
}
route-suppression;
server-duid-type type;
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 {
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
```



```

    delegated-pool;
    include-option-82 {
        forcerenew;
        nak;
    }
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
        pool pool-name;
    }
    protocol-attributes attribute-set-name;
    rapid-commit;
}
reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    support-option-pd-exclude;
    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 {
    asymmetric-lease-time seconds;
    client-discover-match (option60-and-option82 | incoming-interface);
    include-option-82 {
        forcerenew;
        nak;
    }
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
    protocol-attributes attribute-set-name;
}
service-profile dynamic-profile-name;
trace;
upto upto-interface-name;
}
overrides {
    asymmetric-lease-time seconds;
    client-discover-match (option60-and-option82 | incoming-interface);
    include-option-82 {
        forcerenew;
        nak;
    }
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
    protocol-attributes attribute-set-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 {
    asymmetric-lease-time seconds;
    client-discover-match <option60-and-option82 | incoming-interface>;
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
    protocol-attributes attribute-set-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;
on-demand-address-allocation;
protocol-master;
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 to 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 extended DHCP local server is incompatible with the DHCP server on J Series routers and, therefore, is not supported on J Series routers. Also, the DHCP local server and the DHCP/BOOTP relay server, which are configured under the **[edit forwarding-options helpers]** hierarchy level, cannot both be enabled on the router or switch at the same time. The extended DHCP local server is fully compatible with the extended DHCP relay feature.

The **dhcpv6** 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. See [CLI Explorer](#).

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*
- *DHCPv6 Local Server Overview*

dhcp-relay

```
Syntax  dhcp-relay {
    access-profile profile-name;
    active-server-group server-group-name;
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
            domain-name domain-name-string;
            interface-description (device-interface | logical-interface);
            interface-name;
            logical-system-name;
            mac-address;
            option-60;
            option-82 <circuit-id> <remote-id>;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
    bulk-leasequery {
        attempts number-of-attempts;
        timeout seconds;
        trigger automatic;
    }
    dhcpv6 {
        access-profile profile-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;
            interface-description (device-interface | logical-interface);
            logical-system-name;
            relay-agent-interface-id;
            relay-agent-remote-id;
            relay-agent-subscriber-id;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
    bulk-leasequery {
        attempts number-of-attempts;
        timeout seconds;
        trigger automatic;
    }
    duplicate-clients incoming-interface;
    dynamic-profile profile-name {
        aggregate-clients (merge | replace);
    }
}
```

```
    use-primary primary-profile-name;
}
forward-only {
    logical-system <current | default | logical-system-name>;
    routing-instance <current | default | routing-instance-name>;
}
forward-only-replies;
}
forward-snooped-clients (all-interfaces | configured-interfaces |
non-configured-interfaces);
group group-name {
    access-profile profile-name;
    active-server-group server-group-name;
    authentication {
        ...
    }
}
dual-stack-group dual-stack-group-name {
    access-profile profile-name;
    authentication {
        ... authentication-configuration
    }
    dynamic-profile profile-name {
        ... dynamic-profile-configuration
    }
    relay-agent-interface-id {
        ... relay-agent-interface-id-configuration
    }
    relay-agent-remote-id {
        ... relay-agent-remote-id-configuration
    }
    service-profile dynamic-profile-name;
}
dynamic-profile profile-name {
    ...
}
forward-only {
    logical-system <current | default | logical-system-name>;
    routing-instance <current | default | routing-instance-name>;
}
interface interface-name {
    access-profile profile-name;
    dynamic-profile profile-name {
        ...
    }
}
exclude;
overrides {
    allow-snooped-clients;
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-negotiation-match incoming-interface;
    delay-authentication;
    delete-binding-on-renegotiation;
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    no-allow-snooped-clients;
    no-bind-on-request;
```

```

        relay-source interface-name;
        send-release-on-delete;
    }
    service-profile dynamic-profile-name;
    trace;
    upto upto-interface-name;
}
}
lease-time-validation {
    lease-time-threshold seconds;
    violation-action action;
}
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;
        }
        route-suppression;
        service-profile dynamic-profile-name;
    }
}
overrides {
    allow-snooped-clients;
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-negotiation-match incoming-interface;
    delay-authentication;
    delete-binding-on-renegotiation;
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    no-allow-snooped-clients;
    no-bind-on-request;
    relay-source interface-name;
    send-release-on-delete;
}
relay-agent-interface-id {
    ...
}
relay-agent-remote-id {
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82 <strict>;
}

```

```
}
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;
  }
}
remote-id-mismatch action;
route-suppression;
service-profile dynamic-profile-name;
}
leasequery {
  attempts number-of-attempts;
  timeout seconds;
}
lease-time-validation {
  lease-time-threshold seconds;
  violation-action action;
}
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;
    }
    route-suppression;
    service-profile dynamic-profile-name;
  }
}
no-snoop;
overrides {
```



```

allow-snooped-clients;
asymmetric-lease-time seconds;
asymmetric-prefix-lease-time seconds;
client-negotiation-match incoming-interface;
delay-authentication;
delete-binding-on-renegotiation;
dual-stack dual-stack-group-name;
interface-client-limit number;
no-allow-snooped-clients;
no-bind-on-request;
relay-source interface-name;
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);
    use-option-82 <strict>;
}
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;
    }
}
}
relay-option-vendor-specific{
    host-name;
    location;
    remote-id-mismatch action;
    route-suppression;
    server-group {
        server-group-name {
            server-ip-address;
        }
    }
    server-response-time seconds;
    service-profile dynamic-profile-name;
}
dual-stack-group dual-stack-group-name {
    access-profile profile-name;

```

```
authentication {
    ... authentication-configuration
}
dynamic-profile profile-name {
    ... dynamic-profile-configuration
}
relay-agent-interface-id {
    ... relay-agent-interface-id-configuration
}
relay-agent-remote-id {
    ... relay-agent-remote-id-configuration
}
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-only {
    logical-system <current | default | logical-system-name>;
    routing-instance <current | default | routing-instance-name>;
}
forward-only-replies;
forward-snooped-clients (all-interfaces | configured-interfaces |
    non-configured-interfaces);
group group-name {
    access-profile profile-name;
    active-server-group server-group-name;
    authentication {
        ...
    }
    dynamic-profile profile-name {
        ...
    }
    forward-only {
        logical-system <current | default | logical-system-name>;
        routing-instance <current | default | routing-instance-name>;
    }
    forward-only {
        logical-system <current | default | logical-system-name>;
        routing-instance <current | default | routing-instance-name>;
    }
}
interface interface-name {
    access-profile profile-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;
}
leasequery {
    attempts number-of-attempts;
    timeout seconds;
}
lease-time-validation {
    lease-time-threshold seconds;
    violation-action action;
}
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;
}

```

```
    }
  }
}
no-snoop;
overrides {
  allow-no-end-option
  allow-snooped-clients;
  always-write-giaddr;
  always-write-option-82;
  asymmetric-lease-time seconds;
  asymmetric-prefix-lease-time seconds;
  client-discover-match (option60-and-option82 | incoming-interface);
  delay-authentication;
  delete-binding-on-renegotiation;
  disable-relay;
  dual-stack dual-stack-group-name;
  interface-client-limit number;
  layer2-unicast-replies;
  no-allow-snooped-clients;
  no-bind-on-request;
  proxy-mode;
  relay-source
  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-id-override
}
```

```

}
remote-id-mismatch action;
route-suppression:
  server-group {
    server-group-name {
      server-ip-address;
    }
  }
server-response-time seconds;
service-profile dynamic-profile-name;

```

Hierarchy Level	<p>[edit forwarding-options],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options]</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> <p>Statement introduced in Junos OS Release 13.2X51 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>Configure extended Dynamic Host Configuration Protocol (DHCP) relay and DHCPv6 relay options on the router or switch to 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 dhcpx-relay and dhcpxv6 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	<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"> • <i>Extended DHCP Relay Agent Overview</i> • <i>DHCPv6 Relay Agent Overview</i> • <i>DHCP Relay Proxy Overview</i> • <i>Using External AAA Authentication Services with DHCP</i>

dhcipv6 (DHCP Local Server)

```
Syntax  dhcipv6 {
    access-profile profile-name;
    authentication {
        password password-string;
        username-include {
            circuit-type;
            client-id;
            delimiter delimiter-character;
            domain-name domain-name-string;
            interface-description (device-interface | logical-interface);
            logical-system-name;
            mac-address;
            relay-agent-interface-id;
            relay-agent-remote-id;
            relay-agent-subscriber-id;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
    duplicate-clients incoming-interface;
    group group-name {
        access-profile profile-name;
        authentication {
            ...
        }
        interface interface-name {
            access-profile profile-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 {
        asymmetric-lease-time seconds;
        asymmetric-prefix-lease-time seconds;
        client-negotiation-match incoming-interface;
    }
}
```

```

        delete-binding-on-renegotiation;
        interface-client-limit number;
        multi-address-embedded-option-response;
        process-inform {
            pool pool-name;
        }
        protocol-attributes attribute-set-name;
        rapid-commit;
    }
    service-profile dynamic-profile-name;
    trace;
    upto upto-interface-name;
}
overrides {
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-negotiation-match incoming-interface;
    delegated-pool;
    delete-binding-on-renegotiation;
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
        pool pool-name;
    }
    protocol-attributes attribute-set-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 {
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-negotiation-match incoming-interface;
    delegated-pool;

```

```
delete-binding-on-renegotiation;
interface-client-limit number;
multi-address-embedded-option-response;
process-inform {
    pool pool-name;
}
protocol-attributes attribute-set-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;
    support-option-pd-exclude;
    timeout timeout-value;
    token token-value;
    trigger {
        radius-disconnect;
    }
}
}
requested-ip-network-match subnet-mask;
route-suppression;
server-duid-type type;
service-profile dynamic-profile-name;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services [dhcp-local-server](#)],
[edit logical-systems *logical-system-name* system services [dhcp-local-server](#)],
[edit routing-instances *routing-instance-name* system services [dhcp-local-server](#)],
[edit system services [dhcp-local-server](#)]

Release Information Statement introduced in Junos OS Release 9.6.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description Configure DHCPv6 local server options on the router or switch to enable the router or switch to function as a server for the DHCP protocol for 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.

The DHCPv6 local server is fully compatible with the extended DHCP local server and DHCP relay agent.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *DHCPv6 Local Server Overview*

domain-name (Address-Assignment Pools)

Syntax domain-name *domain-name*;

Hierarchy Level [edit access address-assignment pool *pool-name* family inet [dhcp-attributes](#)],
[edit access protocol-attributes *attribute-set-name*]

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 *domain-name*—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

- *Configuring Address-Assignment Pools*


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 dual-stack-group <i>dual-stack-group-name</i>], [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>profile-name—Name of the dynamic profile.</p> <p>The remaining statements are explained separately. See CLI Explorer.</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>Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces</i>• <i>Configuring a Default Subscriber Service</i>

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	<p>[edit forwarding-options dhcp-relay], [edit forwarding-options dhcp-relay dhcpv6], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> interface <i>interface-name</i>], [edit forwarding-options dhcp-relay dual-stack-group <i>dual-stack-group-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 ...]</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. Support at the [edit ... dual-stack-group <i>dual-stack-group-name</i>] hierarchy level introduced in Junos OS Release 15.1.</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. See CLI Explorer.</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 239 • <i>Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces</i> • <i>Grouping Interfaces with Common DHCP Configurations</i> • <i>Configuring a Default Subscriber Service</i>

dynamic-profile (Dynamic PPPoE)

Syntax	<code>dynamic-profile <i>profile-name</i>;</code>
Hierarchy Level	<p>[edit dynamic-profiles <i>profile-name</i> interfaces demux0 unit <i>logical-unit-number</i> family pppoe],</p> <p>[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family pppoe],</p> <p>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family pppoe],</p> <p>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> pppoe-underlying-options],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family pppoe],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> pppoe-underlying-options]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.1.</p> <p>Support for the [edit ... family pppoe] hierarchies introduced in Junos OS Release 11.2.</p>
Description	<p>Attach a PPPoE dynamic profile to an underlying Ethernet interface. This underlying interface is configured with either the encapsulation ppp-over-ether statement or the family pppoe statement; the two statements are mutually exclusive. When the router creates a dynamic PPPoE logical interface on the underlying interface, it uses the information in the dynamic profile to determine the properties of the dynamic PPPoE logical interface.</p>
<div>  <p>NOTE: The [edit ... family pppoe] hierarchies are supported only on MX Series routers with MPCs.</p> <p>Starting in Junos OS Release 17.2R1, you can configure converged services for MS-MPCs and MS-MICs. You can configure captive portal content delivery (CPCD) profiles for MS-MICs and MS-MPCs by including the service interface ms-fpc/pic/port statement at the edit service-set service set name captive-portal-content-delivery-profile <i>profile name</i> interface-service heirarchy level.</p> </div>	
Options	<p><i>profile-name</i>—Name of a previously configured PPPoE dynamic profile, up to 64 characters in length, defined at the [edit dynamic-profiles <i>profile-name</i> interfaces pp0] hierarchy level.</p>
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 an Underlying Interface for Dynamic PPPoE Subscriber Interfaces Configuring the PPPoE Family for an Underlying Interface

- *Dynamic PPPoE Subscriber Interfaces over Static Underlying Interfaces Overview*

dynamic-profile (Stacked VLAN)

Syntax	<pre>dynamic-profile <i>profile-name</i> { accept (any dhcp-v4 dhcp-v6 inet inet6 pppoe); access-profile <i>vlan-dynamic-profile-name</i>; ranges (any <i>low-tag-high-tag</i>), (any <i>low-tag-high-tag</i>); }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> auto-configure stacked-vlan-ranges]
Release Information	Statement introduced in Junos OS Release 9.5.
Description	Configure a dynamic profile for use when configuring dynamic stacked VLANs.
Options	<p><i>profile-name</i>—Name of the dynamic profile that you want to use when configuring dynamic stacked VLANs.</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"> • <i>Dynamic Profiles Overview</i> • <i>Configuring a Basic Dynamic Profile</i> • <i>Configuring an Interface to Use the Dynamic Profile Configured to Create Stacked VLANs</i>

dynamic-profile (VLAN)

Syntax	<pre>dynamic-profile <i>profile-name</i> { accept (any dhcp-v4 dhcp-v6 inet inet6 pppoe); accept-out-of-band <i>protocol</i>; access-profile <i>vlan-dynamic-profile-name</i>; ranges (any <i>low-tag</i>)–(any <i>high-tag</i>); }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> auto-configure <i>vlan-ranges</i>]
Release Information	Statement introduced in Junos OS Release 9.5.
Description	Configure a dynamic profile for use when configuring dynamic VLANs.
Options	<p><i>profile-name</i>—Name of the dynamic profile that you want to use when configuring dynamic VLANs.</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">• <i>Dynamic Profiles Overview</i>• <i>Configuring a Basic Dynamic Profile</i>• <i>Configuring an Interface to Use the Dynamic Profile Configured to Create Single-Tag VLANs</i>

dynamic-profiles

```

Syntax  dynamic-profiles {
        profile-name {
            class-of-service {
                interfaces {
                    interface-name ;
                }
                unit logical-unit-number {
                    classifiers {
                        type (classifier-name | default);
                    }
                    output-traffic-control-profile (profile-name | $junos-cos-traffic-control-profile);
                    report-ingress-shaping-rate bps;
                    rewrite-rules {
                        dscp (rewrite-name | default);
                        dscp-ipv6 (rewrite-name | default);
                        ieee-802.1 (rewrite-name | default) vlan-tag (outer | outer-and-inner);
                        inet-precedence (rewrite-name | default);
                    }
                }
            }
        }
    }
    scheduler-maps {
        map-name {
            forwarding-class class-name scheduler scheduler-name;
        }
    }
    schedulers {
        (scheduler-name) {
            buffer-size (seconds | percent percentage | remainder | temporal microseconds);
            drop-profile-map loss-priority (any | low | medium-low | medium-high | high)
                protocol (any | non-tcp | tcp) drop-profile profile-name;
            excess-priority (low | high | $junos-cos-scheduler-excess-priority);
            excess-rate (percent percentage | percent $junos-cos-scheduler-excess-rate);
            overhead-accounting (shaping-mode) <bytes (byte-value)>;
            priority priority-level;
            shaping-rate (rate | predefined-variable);
            transmit-rate (percent percentage | rate | remainder) <exact | rate-limit>;
        }
    }
    traffic-control-profiles profile-name {
        delay-buffer-rate (percent percentage | rate | $junos-cos-delay-buffer-rate);
        excess-rate (percent percentage | proportion value | percent $junos-cos-excess-rate);
        guaranteed-rate (percent percentage | rate | $junos-cos-guaranteed-rate);
        overhead-accounting (shaping-mode) <bytes (byte-value)>;
        scheduler-map map-name;
        shaping-rate (rate | predefined-variable);
    }
}
    firewall {
        family family {
            fast-update-filter filter-name {
                interface-specific;
            }
        }
    }

```

```
match-order [match-order];
term term-name {
    from {
        match-conditions;
    }
    then {
        action;
        action-modifiers;
    }
    only-at-create;
}
}
filter filter-name {
    enhanced-mode-override;
    fast-lookup-filter;
    instance-shared;
    interface-shared;
    interface-specific;
    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 uid {
    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;
    }
}
}
policer uid {
    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;
    }
}
}
three-color-policer uid {
    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;
    }
}
}
}
interfaces interface-name {
    interface-set interface-set-name {
        interface interface-name {
            unit logical unit number {
                advisory-options {
                    downstream-rate rate;
                    upstream-rate rate;

```

```

    }
  }
}
unit logical-unit-number {
  auto-configure {
    agent-circuit-identifier {
      dynamic-profile profile-name;
    }
    line-identity {
      include {
        accept-no-ids;
        circuit-id;
        remote-id;
      }
      dynamic-profile profile-name;
    }
  }
}
encapsulation (atm-ccc-cell-relay | atm-ccc-vc-mux | atm-cisco-nlpid |
  atm-tcc-vc-mux | atm-mlppp-llc | atm-nlpid | atm-ppp-llc | atm-ppp-vc-mux |
  atm-snap | atm-tcc-snap | atm-vc-mux | ether-over-atm-llc |
  ether-vpls-over-atm-llc | ether-vpls-over-fr | ether-vpls-over-ppp | ethernet |
  frame-relay-ccc | frame-relay-ppp | frame-relay-tcc | frame-relay-ether-type |
  frame-relay-ether-type-tcc | multilink-frame-relay-end-to-end | multilink-ppp |
  ppp-over-ether | ppp-over-ether-over-atm-llc | vlan-bridge | vlan-ccc | vlan-vci-ccc
  | vlan-tcc | vlan-vpls);
family family {
  address address;
  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;
    }
  }
}
rpf-check {
  fail-filter filter-name;
  mode loose;
}
service {
  input {
    service-set service-set-name {
      service-filter filter-name;
    }
    post-service-filter filter-name;
  }
}

```

```

input-vlan-map {
    inner-tag-protocol-id tpid;
    inner-vlan-id number;
    (push | swap);
    tag-protocol-id tpid;
    vlan-id number;
}
output {
    service-set service-set-name {
        service-filter filter-name;
    }
}
output-vlan-map {
    inner-tag-protocol-id tpid;
    inner-vlan-id number;
    (pop | swap);
    tag-protocol-id tpid;
    vlan-id number;
}
pcef pcef-profile-name {
    activate rule-name | activate-all;
}
}
unnumbered-address interface-name <preferred-source-address address>;
}
filter {
    input filter-name (
        shared-name filter-shared-name;
    )
    output filter-name {
        shared-name filter-shared-name;
    }
}
host-prefix-only;
ppp-options {
    chap;
    pap;
}
vlan-id number;
vlan-tags outer [tpid].vlan-id [inner [tpid].vlan-id];
}
}
interfaces {
    demux0 {...}
}
interfaces {
    pp0 {...}
}
policy-options {
    prefix-list uid {
        ip-addresses;
        dynamic-db;
    }
}
}
predefined-variable-defaults predefined-variable <variable-option> default-value;
protocols {

```

```
igmp {
  interface interface-name {
    accounting;
    disable;
    group-limit limit;
    group-policy;
    group-threshold value;
    immediate-leave;
    log-interval seconds;
    no-accounting;
    oif-map;
    passive;
    promiscuous-mode;
    ssm-map ssm-map-name;
    ssm-map-policy ssm-map-policy-name
    static {
      group group {
        source source;
      }
    }
    version version;
  }
}

mld {
  interface interface-name {
    (accounting | no-accounting);
    disable;
    group-limit limit;
    group-policy;
    group-threshold value;
    immediate-leave;
    log-interval seconds;
    oif-map;
    passive;
    ssm-map ssm-map-name;
    ssm-map-policy ssm-map-policy-name;
    static {
      group multicast-group-address {
        exclude;
        group-count number;
        group-increment increment;
        source ip-address {
          source-count number;
          source-increment increment;
        }
      }
    }
    version version;
  }
}

router-advertisement {
  interface interface-name {
    current-hop-limit number;
    default-lifetime seconds;
    (managed-configuration | no-managed-configuration);
    max-advertisement-interval seconds;
```

```

        min-advertisement-interval seconds;
        (other-stateful-configuration | no-other-stateful-configuration);
        prefix prefix;
        reachable-time milliseconds;
        retransmit-timer milliseconds;
    }
}
}
routing-instances 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;
    }
}
}
services {
    captive-portal-content-delivery {
        rule name {
            match-direction (input | input-output | output);
            term name {
                from {
                    applications application-name {
                        application-protocol type;
                        destination-port port-type;
                        protocol ip-protocol-type;
                        source-port port-type;
                    }
                    destination-address name <except>;
                    destination-address-range low minimum-value high maximum-value <except>;
                    destination-prefix-list name <except>;
                }
                then {
                    accept;
                    redirect url;
                    rewrite destination-address address <destination-port port-number>;
                    syslog;
                }
            }
        }
    }
}
variables {
    variable-name {
        default-value default-value;
        equals expression;
        mandatory;
        uid;
        uid-reference;
    }
}
}

```

Hierarchy Level [\[edit\]](#)

Release Information	Statement introduced in Junos OS Release 9.2. Support at the filter, policer, hierarchical-policer, three-color-policer, and policy options hierarchy levels introduced in Junos OS Release 11.4.
Description	Create dynamic profiles for use with DHCP or PPP client access.
Options	<i>profile-name</i> —Name of the dynamic profile; string of up to 80 alphanumeric characters. 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>Configuring a Basic Dynamic Profile</i>• <i>Configuring Dynamic VLANs Based on Agent Circuit Identifier Information</i>• <i>Dynamic Profiles Overview</i>

egress-stats (Flat-File Accounting Options)

Syntax	<pre>egress-stats { all-fields; input-bytes; input-packets; output-bytes; output-packets; queue-id; red-drop-bytes; red-drop-packets; tail-drop-packets; }</pre>
Hierarchy Level	[edit accounting-options flat-file-profile <i>profile-name</i> fields]
Release Information	Statement introduced in Junos OS Release 16.1R4.
Description	Specify egress queue statistics to be collected for the interface.
Options	<p>all-fields—Collect all egress queue statistics available for the interface context, logical or physical.</p> <p>input-bytes—Collect the number of octets queued including traffic dropped because of congestion.</p> <p>input-packets—Collect the number of packets queued including traffic dropped because of congestion.</p> <p>output-bytes—Collect the number of octets transmitted by the egress queue.</p> <p>output-packets—Collect the number of packets transmitted by the egress queue.</p> <p>queue-id—Collect the logical identifier for the egress queue; identifies the traffic class.</p> <p>red-drop-bytes—Collect the number of octets dropped on the egress queue because of random early detection.</p> <p>red-drop-packets—Collect the number of packets dropped on the egress queue because of random early detection.</p> <p>tail-drop-packets—Collect the number of packets dropped in the egress queue because of tail drop.</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 Flat-File Accounting for Layer 2 Wholesale on page 181

- [Configuring Flat-File Accounting for Extensible Subscriber Services Management on page 185](#)
- [Flat-File Accounting Overview on page 177](#)

encapsulation (Dynamic Interfaces)

Syntax	<code>encapsulation (atm-ccc-cell-relay atm-ccc-vc-mux atm-cisco-nlpid atm-tcc-vc-mux atm-mlppp-llc atm-nlpid atm-ppp-llc atm-ppp-vc-mux atm-snap atm-tcc-snap atm-vc-mux ether-over-atm-llc ether-vpls-over-atm-llc ether-vpls-over-fr ether-vpls-over-ppp ethernet frame-relay-ccc frame-relay-ppp frame-relay-tcc frame-relay-ether-type frame-relay-ether-type-tcc multilink-frame-relay-end-to-end multilink-ppp ppp-over-ether ppp-over-ether-over-atm-llc vlan-bridge vlan-ccc vlan-vci-ccc vlan-tcc vlan-vpls);</code>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	Dynamic interface configuration of the logical link-layer encapsulation type.
Options	<p>atm-ccc-cell-relay—Use ATM cell-relay encapsulation.</p> <p>atm-ccc-vc-mux—Use ATM virtual circuit (VC) multiplex encapsulation on circuit cross-connect (CCC) circuits. When you use this encapsulation type, you can configure the ccc family only.</p> <p>atm-cisco-nlpid—Use Cisco ATM network layer protocol ID (NLPID) encapsulation. When you use this encapsulation type, you can configure the inet family only.</p> <p>atm-mlppp-llc—For ATM2 IQ interfaces only, use Multilink Point-to-Point Protocol (MLPPP) over AAL5 LLC. For this encapsulation type, your router must be equipped with a link services or voice services PIC. MLPPP over ATM encapsulation is not supported on ATM2 IQ OC48 interfaces.</p> <p>atm-nlpid—Use ATM NLPID encapsulation. When you use this encapsulation type, you can configure the inet family only.</p> <p>atm-ppp-llc—For ATM2 IQ interfaces only, use PPP over AAL5 LLC encapsulation.</p> <p>atm-ppp-vc-mux—For ATM2 IQ interfaces only, use PPP over ATM AAL5 multiplex encapsulation.</p> <p>atm-snap—Use ATM subnetwork attachment point (SNAP) encapsulation.</p> <p>atm-tcc-snap—Use ATM SNAP encapsulation on translational cross-connect (TCC) circuits.</p> <p>atm-tcc-vc-mux—Use ATM VC multiplex encapsulation on TCC circuits. When you use this encapsulation type, you can configure the tcc family only.</p> <p>atm-vc-mux—Use ATM VC multiplex encapsulation. When you use this encapsulation type, you can configure the inet family only.</p>

ether-over-atm-llc—For interfaces that carry IPv4 traffic, use Ethernet over ATM LLC encapsulation. When you use this encapsulation type, you cannot configure multipoint interfaces.

ether-vpls-over-atm-llc—For ATM2 IQ interfaces only, use the Ethernet virtual private LAN service (VPLS) over ATM LLC encapsulation to bridge Ethernet interfaces and ATM interfaces over a VPLS routing instance (as described in RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*). Packets from the ATM interfaces are converted to standard ENET2/802.3 encapsulated Ethernet frames with the frame check sequence (FCS) field removed.

ether-vpls-over-fr—For E1, T1, E3, T3, and SONET interfaces only, use the Ethernet virtual private LAN service (VPLS) over Frame Relay encapsulation to support Bridged Ethernet over Frame Relay encapsulated TDM interfaces for VPLS applications, as per *Multiprotocol Interconnect over Frame Relay* (RFC 2427 [1490]).

ether-vpls-over-ppp—For E1, T1, E3, T3 and SONET interfaces only, use the Ethernet virtual private LAN service (VPLS) over PPP encapsulation to support Bridged Ethernet over PPP encapsulated TDM interfaces for VPLS applications.

ethernet—Use Ethernet II encapsulation (as described in RFC 894, *A Standard for the Transmission of IP Datagrams over Ethernet Networks*).

ethernet-vpls—Use Ethernet VPLS encapsulation on Ethernet interfaces that have VPLS enabled and that must accept packets carrying standard Tag Protocol ID (TPID) values.

extended-vlan-vpls—Use extended virtual LAN (VLAN) VPLS encapsulation on Ethernet interfaces that have VLAN 802.1Q tagging and VPLS enabled and that must accept packets carrying TPIDs 0x8100, 0x9100, and 0x9901.



NOTE: The built-in Gigabit Ethernet PIC on an M7i router does not support extended VLAN VPLS encapsulation.

frame-relay-ccc—Use Frame Relay encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only.

frame-relay-ppp—Use PPP over Frame Relay circuits. When you use this encapsulation type, you can configure the **ppp** family only.

frame-relay-tcc—Use Frame Relay encapsulation on TCC circuits for connecting unlike media. When you use this encapsulation type, you can configure the **tcc** family only.

frame-relay-ether-type—Use Frame Relay ether type encapsulation for compatibility with Cisco Frame Relay. The physical interface must be configured with **flexible-frame-relay** encapsulation.

frame-relay-ether-type-tcc—Use Frame Relay ether type TCC for Cisco-compatible Frame Relay on TCC circuits to connect unlike media. The physical interface must be configured with **flexible-frame-relay** encapsulation.

multilink-frame-relay-end-to-end—Use MLFR FRF.15 encapsulation. This encapsulation is used only on multilink, link services, and voice services interfaces and their constituent T1 or E1 interfaces, and is supported on LSQ and redundant LSQ interfaces.

multilink-ppp—Use MLPPP encapsulation. This encapsulation is used only on multilink, link services, and voice services interfaces and their constituent T1 or E1 interfaces.

ppp-over-ether—You use PPP over Ethernet encapsulation to configure an underlying Ethernet interface for a dynamic PPPoE logical interface.

vlan-bridge—Use Ethernet VLAN bridge encapsulation on Ethernet interfaces that have IEEE 802.1Q tagging, flexible ethernet services, and bridging enabled, and that must accept packets carrying TPID 0x8100 or a user-defined TPID.

vlan-ccc—Use Ethernet virtual LAN (VLAN) encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only.

vlan-vci-ccc—Use ATM-to-Ethernet interworking encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only.

vlan-tcc—Use Ethernet VLAN encapsulation on TCC circuits. When you use this encapsulation type, you can configure the **tcc** family only.

vlan-vpls—Use Ethernet VLAN encapsulation on VPLS circuits.

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 a Retail Dynamic Profile for Use in the Layer 2 Wholesale Solution on page 79• <i>Configuring PPP over ATM2 Encapsulation Overview</i>
------------------------------	---

encapsulation (Logical Interface)

Syntax	encapsulation (atm-ccc-cell-relay atm-ccc-vc-mux atm-cisco-nlpid atm-mlppp-llc atm-nlpid atm-ppp-llc atm-ppp-vc-mux atm-snap atm-tcc-snap atm-tcc-vc-mux atm-vc-mux ether-over-atm-llc ether-vpls-over-atm-llc ether-vpls-over-fr ether-vpls-over-ppp ethernet ethernet-ccc ethernet-vpls ethernet-vpls-fr frame-relay-ccc frame-relay-ether-type frame-relay-ether-type-tcc frame-relay-ppp frame-relay-tcc gre-fragmentation multilink-frame-relay-end-to-end multilink-ppp ppp-over-ether ppp-over-ether-over-atm-llc vlan-bridge vlan-ccc vlan-vci-ccc vlan-tcc vlan-vpls vxlan);
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>], [edit interfaces <i>rlsq number</i> unit <i>logical-unit-number</i>] [edit protocols evpn]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers (ethernet , vlan-ccc , and vlan-tcc options only). Statement introduced in Junos OS Release 12.2 for the ACX Series Universal Access Routers. Only the atm-ccc-cell-relay and atm-ccc-vc-mux options are supported on ACX Series routers. Statement introduced in Junos OS Release 17.3R1 for QFX10000 Series switches (ethernet-ccc and vlan-ccc options only).
Description	Configure a logical link-layer encapsulation type. Not all encapsulation types are supported on the switches. See the switch CLI.
Options	<p>atm-ccc-cell-relay—Use ATM cell-relay encapsulation.</p> <p>atm-ccc-vc-mux—Use ATM virtual circuit (VC) multiplex encapsulation on CCC circuits. When you use this encapsulation type, you can configure the ccc family only.</p> <p>atm-cisco-nlpid—Use Cisco ATM network layer protocol identifier (NLPID) encapsulation. When you use this encapsulation type, you can configure the inet family only.</p> <p>atm-mlppp-llc—For ATM2 IQ interfaces only, use Multilink Point-to-Point (MLPPP) over AAL5 LLC. For this encapsulation type, your router must be equipped with a Link Services or Voice Services PIC. MLPPP over ATM encapsulation is not supported on ATM2 IQ OC48 interfaces.</p> <p>atm-nlpid—Use ATM NLPID encapsulation. When you use this encapsulation type, you can configure the inet family only.</p> <p>atm-ppp-llc—(ATM2 IQ interfaces and MX Series routers with MPC/MIC interfaces using the ATM MIC with SFP only) Use PPP over AAL5 LLC encapsulation.</p> <p>atm-ppp-vc-mux—(ATM2 IQ interfaces and MX Series routers with MPC/MIC interfaces using the ATM MIC with SFP only) Use PPP over ATM AAL5 multiplex encapsulation.</p>

atm-snap—(All interfaces including MX Series routers with MPC/MIC interfaces using the ATM MIC with SFP) Use ATM subnetwork attachment point (SNAP) encapsulation.

atm-tcc-snap—Use ATM SNAP encapsulation on translational cross-connect (TCC) circuits.

atm-tcc-vc-mux—Use ATM VC multiplex encapsulation on TCC circuits. When you use this encapsulation type, you can configure the **tcc** family only.

atm-vc-mux—(All interfaces including MX Series routers with MPC/MIC interfaces using the ATM MIC with SFP) Use ATM VC multiplex encapsulation. When you use this encapsulation type, you can configure the **inet** family only.

ether-over-atm-llc—(All IP interfaces including MX Series routers with MPC/MIC interfaces using the ATM MIC with SFP) For interfaces that carry IP traffic, use Ethernet over ATM LLC encapsulation. When you use this encapsulation type, you cannot configure multipoint interfaces.

ether-vpls-over-atm-llc—For ATM2 IQ interfaces only, use the Ethernet virtual private LAN service (VPLS) over ATM LLC encapsulation to bridge Ethernet interfaces and ATM interfaces over a VPLS routing instance (as described in RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*). Packets from the ATM interfaces are converted to standard ENET2/802.3 encapsulated Ethernet frames with the frame check sequence (FCS) field removed.

ether-vpls-over-fr—For E1, T1, E3, T3, and SONET interfaces only, use the Ethernet virtual private LAN service (VPLS) over Frame Relay encapsulation to support Bridged Ethernet over Frame Relay encapsulated TDM interfaces for VPLS applications, per RFC 2427, *Multiprotocol Interconnect over Frame Relay*.



NOTE: The SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP, the Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP, and the DS3/E3 MIC do not support Ethernet over Frame Relay encapsulation.

ether-vpls-over-ppp—For E1, T1, E3, T3, and SONET interfaces only, use the Ethernet virtual private LAN service (VPLS) over Point-to-Point Protocol (PPP) encapsulation to support Bridged Ethernet over PPP-encapsulated TDM interfaces for VPLS applications.

ethernet—Use Ethernet II encapsulation (as described in RFC 894, *A Standard for the Transmission of IP Datagrams over Ethernet Networks*).

ethernet-ccc—Use Ethernet CCC encapsulation on Ethernet interfaces.

ethernet-vpls—Use Ethernet VPLS encapsulation on Ethernet interfaces that have VPLS enabled and that must accept packets carrying standard Tag Protocol ID (TPID) values.



NOTE: The built-in Gigabit Ethernet PIC on an M7i router does not support extended VLAN VPLS encapsulation.

ethernet-vpls-fr—Use in a VPLS setup when a CE device is connected to a PE router over a time-division multiplexing (TDM) link. This encapsulation type enables the PE router to terminate the outer layer 2 Frame Relay connection, use the 802.1p bits inside the inner Ethernet header to classify the packets, look at the MAC address from the Ethernet header, and use the MAC address to forward the packet into a given VPLS instance.

frame-relay-ccc—Use Frame Relay encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only.

frame-relay-ether-type—Use Frame Relay ether type encapsulation for compatibility with Cisco Frame Relay. The physical interface must be configured with flexible-frame-relay encapsulation.

frame-relay-ether-type-tcc—Use Frame Relay ether type TCC for Cisco-compatible Frame Relay on TCC circuits to connect different media. The physical interface must be configured with flexible-frame-relay encapsulation.

frame-relay-ppp—Use PPP over Frame Relay circuits. When you use this encapsulation type, you can configure the **ppp** family only.

frame-relay-tcc—Use Frame Relay encapsulation on TCC circuits for connecting different media. When you use this encapsulation type, you can configure the **tcc** family only.

gre-fragmentation—For adaptive services interfaces only, use GRE fragmentation encapsulation to enable fragmentation of IPv4 packets in GRE tunnels. This encapsulation clears the do not fragment (DF) bit in the packet header. If the packet's size exceeds the tunnel's maximum transmission unit (MTU) value, the packet is fragmented before encapsulation.

multilink-frame-relay-end-to-end—Use MLFR FRF.15 encapsulation. This encapsulation is used only on multilink, link services, and voice services interfaces and their constituent T1 or E1 interfaces, and is supported on LSQ and redundant LSQ interfaces.

multilink-ppp—Use MLPPP encapsulation. This encapsulation is used only on multilink, link services, and voice services interfaces and their constituent T1 or E1 interfaces.

ppp-over-ether—Use PPP over Ethernet encapsulation to configure an underlying Ethernet interface for a dynamic PPPoE logical interface on M120 and M320 routers with Intelligent Queuing 2 (IQ2) PICs, and on MX Series routers with MPCs.

ppp-over-ether-over-atm-llc—(MX Series routers with MPCs using the ATM MIC with SFP only) For underlying ATM interfaces, use PPP over Ethernet over ATM LLC encapsulation. When you use this encapsulation type, you cannot configure the interface address. Instead, configure the interface address on the PPP interface.

vlan-bridge—Use Ethernet VLAN bridge encapsulation on Ethernet interfaces that have IEEE 802.1Q tagging, flexible-ethernet-services, and bridging enabled and that must accept packets carrying TPID 0x8100 or a user-defined TPID.

vlan-ccc—Use Ethernet virtual LAN (VLAN) encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only.

vlan-vci-ccc—Use ATM-to-Ethernet interworking encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only.

vlan-tcc—Use Ethernet VLAN encapsulation on TCC circuits. When you use this encapsulation type, you can configure the **tcc** family only.

vlan-vpls—Use Ethernet VLAN encapsulation on VPLS circuits.



vxlan—Use VXLAN data plane encapsulation for EVPN.

Required Privilege Level	interface —To view this statement in the configuration. interface-control —To add this statement to the configuration.
---------------------------------	---

Related Documentation

- *Configuring Layer 2 Switching Cross-Connects Using CCC*
- *Configuring the Encapsulation for Layer 2 Switching TCCs*
- *Configuring Interface Encapsulation on Logical Interfaces*
- *Configuring MPLS LSP Tunnel Cross-Connects Using CCC*
- *Circuit and Translational Cross-Connects Overview*
- *Identifying the Access Concentrator*
- *Configuring ATM Interface Encapsulation*
- *Configuring VLAN and Extended VLAN Encapsulation*
- *Configuring ATM-to-Ethernet Interworking*
- *Configuring Interface Encapsulation on PTX Series Packet Transport Routers*
- *Configuring CCC Encapsulation for Layer 2 VPNs*
- *Configuring TCC Encapsulation for Layer 2 VPNs and Layer 2 Circuits*
- *Configuring ATM for Subscriber Access*
- *Understanding CoS on ATM IMA Pseudowire Interfaces Overview*
- *Configuring Policing on an ATM IMA Pseudowire*

encapsulation (Physical Interface)

Syntax	encapsulation (atm-ccc-cell-relay atm-pvc cisco-hdlc cisco-hdlc-ccc cisco-hdlc-tcc ethernet-bridge ethernet-ccc ethernet-over-atm ethernet-tcc ethernet-vpls ethernet-vpls-fr ether-vpls-over-atm-llc ethernet-vpls-ppp extended-frame-relay-ccc extended-frame-relay-ether-type-tcc extended-frame-relay-tcc extended-vlan-bridge extended-vlan-ccc extended-vlan-tcc extended-vlan-vpls flexible-ethernet-services flexible-frame-relay frame-relay frame-relay-ccc frame-relay-ether-type frame-relay-ether-type-tcc frame-relay-port-ccc frame-relay-tcc generic-services multilink-frame-relay-uni-nni ppp ppp-ccc ppp-tcc vlan-ccc vlan-vci-ccc vlan-vpls);
Hierarchy Level	[edit interfaces <i>interface-name</i>], [edit interfaces rlsq <i>number:number</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 11.1 for EX Series switches. Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers (flexible-ethernet-services , ethernet-ccc , and ethernet-tcc options only).
Description	Specify the physical link-layer encapsulation type.
	<div>  <p>NOTE: Not all encapsulation types are supported on the switches. See the switch CLI.</p> </div>
Default	ppp—Use serial PPP encapsulation.
Options	<div>  <p>NOTE: Frame Relay, ATM, PPP, SONET, and SATSOP options are not supported on the EX Series switches.</p> </div> <p>atm-ccc-cell-relay—Use ATM cell-relay encapsulation.</p> <p>atm-pvc—Defined in RFC 2684, <i>Multiprotocol Encapsulation over ATM Adaptation Layer 5</i>. When you configure physical ATM interfaces with ATM PVC encapsulation, an RFC 2684-compliant ATM Adaptation Layer 5 (AAL5) tunnel is set up to route the ATM cells over a Multiprotocol Label Switching (MPLS) path that is typically established between two MPLS-capable routers using the Label Distribution Protocol (LDP).</p> <p>cisco-hdlc—Use Cisco-compatible High-Level Data Link Control (HDLC) framing. E1, E3, SONET/SDH, T1, and T3 interfaces can use Cisco HDLC encapsulation. Two related versions are supported:</p>

- CCC version (**cisco-hdlc-ccc**)—The logical interface does not require an encapsulation statement. When you use this encapsulation type, you can configure the **ccc** family only.
- TCC version (**cisco-hdlc-tcc**)—Similar to CCC and has the same configuration restrictions, but used for circuits with different media on either side of the connection.

cisco-hdlc-ccc—Use Cisco-compatible HDLC framing on CCC circuits.

cisco-hdlc-tcc—Use Cisco-compatible HDLC framing on TCC circuits for connecting different media.

ethernet-bridge—Use Ethernet bridge encapsulation on Ethernet interfaces that have bridging enabled and that must accept all packets.

ethernet-ccc—Use Ethernet CCC encapsulation on Ethernet interfaces that must accept packets carrying standard Tag Protocol ID (TPID) values. For 8-port, 12-port, and 48-port Fast Ethernet PICs, CCC is not supported.

ethernet-over-atm—For interfaces that carry IPv4 traffic, use Ethernet over ATM encapsulation. When you use this encapsulation type, you cannot configure multipoint interfaces. As defined in RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*, this encapsulation type allows ATM interfaces to connect to devices that support only bridge protocol data units (BPDUs). Junos OS does not completely support bridging, but accepts BPDU packets as a default gateway. If you use the router as an edge device, then the router acts as a default gateway. It accepts Ethernet LLC/SNAP frames with IP or ARP in the payload, and drops the rest. For packets destined to the Ethernet LAN, a route lookup is done using the destination IP address. If the route lookup yields a full address match, the packet is encapsulated with an LLC/SNAP and MAC header, and the packet is forwarded to the ATM interface.

ethernet-tcc—For interfaces that carry IPv4 traffic, use Ethernet TCC encapsulation on interfaces that must accept packets carrying standard TPID values. For 8-port, 12-port, and 48-port Fast Ethernet PICs, TCC is not supported.

ethernet-vpls—Use Ethernet VPLS encapsulation on Ethernet interfaces that have VPLS enabled and that must accept packets carrying standard TPID values. On M Series routers, except the M320 router, the 4-port Fast Ethernet TX PIC and the 1-port, 2-port, and 4-port, 4-slot Gigabit Ethernet PICs can use the Ethernet VPLS encapsulation type.

ethernet-vpls-fr—Use in a VPLS setup when a CE device is connected to a PE device over a time division multiplexing (TDM) link. This encapsulation type enables the PE device to terminate the outer Layer 2 Frame Relay connection, use the 802.1p bits inside the inner Ethernet header to classify the packets, look at the MAC address from the Ethernet header, and use the MAC address to forward the packet into a given VPLS instance.

ethernet-vpls-ppp—Use in a VPLS setup when a CE device is connected to a PE device over a time division multiplexing (TDM) link. This encapsulation type enables the PE device to terminate the outer Layer 2 PPP connection, use the 802.1p bits inside the inner Ethernet header to classify the packets, look at the MAC address from the Ethernet header, and use it to forward the packet into a given VPLS instance.

ether-vpls-over-atm-llc—For ATM intelligent queuing (IQ) interfaces only, use the Ethernet virtual private LAN service (VPLS) over ATM LLC encapsulation to bridge Ethernet interfaces and ATM interfaces over a VPLS routing instance (as described in RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*). Packets from the ATM interfaces are converted to standard ENET2/802.3 encapsulated Ethernet frames with the frame check sequence (FCS) field removed.

extended-frame-relay-ccc—Use Frame Relay encapsulation on CCC circuits. This encapsulation type allows you to dedicate DLCIs 1 through 1022 to CCC. When you use this encapsulation type, you can configure the **ccc** family only.

extended-frame-relay-ether-type-tcc—Use extended Frame Relay ether type TCC for Cisco-compatible Frame Relay for DLCIs 1 through 1022. This encapsulation type is used for circuits with different media on either side of the connection.

extended-frame-relay-tcc—Use Frame Relay encapsulation on TCC circuits to connect different media. This encapsulation type allows you to dedicate DLCIs 1 through 1022 to TCC.

extended-vlan-bridge—Use extended VLAN bridge encapsulation on Ethernet interfaces that have IEEE 802.1Q VLAN tagging and bridging enabled and that must accept packets carrying TPID 0x8100 or a user-defined TPID.

extended-vlan-ccc—Use extended VLAN encapsulation on CCC circuits with Gigabit Ethernet and 4-port Fast Ethernet interfaces that must accept packets carrying 802.1Q values. Extended VLAN CCC encapsulation supports TPIDs 0x8100, 0x9100, and 0x9901. When you use this encapsulation type, you can configure the **ccc** family only. For 8-port, 12-port, and 48-port Fast Ethernet PICs, extended VLAN CCC is not supported. For 4-port Gigabit Ethernet PICs, extended VLAN CCC is not supported.

extended-vlan-tcc—For interfaces that carry IPv4 traffic, use extended VLAN encapsulation on TCC circuits with Gigabit Ethernet interfaces on which you want to use 802.1Q tagging. For 4-port Gigabit Ethernet PICs, extended VLAN TCC is not supported.

extended-vlan-vpls—Use extended VLAN VPLS encapsulation on Ethernet interfaces that have VLAN 802.1Q tagging and VPLS enabled and that must accept packets carrying TPIDs 0x8100, 0x9100, and 0x9901. On M Series routers, except the M320 router, the 4-port Fast Ethernet TX PIC and the 1-port, 2-port, and 4-port, 4-slot Gigabit Ethernet PICs can use the Ethernet VPLS encapsulation type.



NOTE: The built-in Gigabit Ethernet PIC on an M7i router does not support extended VLAN VPLS encapsulation.

flexible-ethernet-services—For Gigabit Ethernet IQ interfaces and Gigabit Ethernet PICs with small form-factor pluggable transceivers (SFPs) (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), and for Gigabit Ethernet interfaces, use flexible Ethernet services encapsulation when you want to configure multiple per-unit Ethernet encapsulations. Aggregated Ethernet bundles can use this encapsulation type. This encapsulation type allows you to configure any combination of route, TCC, CCC, Layer 2 virtual private networks (VPNs), and VPLS encapsulations on a single physical port. If you configure flexible Ethernet services encapsulation on the physical interface, VLAN IDs from 1 through 511 are no longer reserved for normal VLANs.

flexible-frame-relay—For IQ interfaces only, use flexible Frame Relay encapsulation when you want to configure multiple per-unit Frame Relay encapsulations. This encapsulation type allows you to configure any combination of TCC, CCC, and standard Frame Relay encapsulations on a single physical port. Also, each logical interface can have any DLCI value from 1 through 1022.

frame-relay—Use Frame Relay encapsulation is defined in RFC 1490, *Multiprotocol Interconnect over Frame Relay*. E1, E3, link services, SONET/SDH, T1, T3, and voice services interfaces can use Frame Relay encapsulation.

frame-relay-ccc—Use Frame Relay encapsulation on CCC circuits. This encapsulation is same as standard Frame Relay for DLCIs 0 through 511. DLCIs 512 through 1022 are dedicated to CCC. The logical interface must also have **frame-relay-ccc** encapsulation. When you use this encapsulation type, you can configure the **ccc** family only.

frame-relay-ether-type—Use Frame Relay ether type encapsulation for compatibility with the Cisco Frame Relay. IETF frame relay encapsulation identifies the payload format using NLPID and SNAP formats. Cisco-compatible Frame Relay encapsulation uses the Ethernet type to identify the type of payload.



NOTE: When the encapsulation type is set to Cisco-compatible Frame Relay encapsulation, ensure that the LMI type is set to ANSI or Q933-A.

frame-relay-ether-type-tcc—Use Frame Relay ether type TCC for Cisco-compatible Frame Relay on TCC circuits to connect different media. This encapsulation is Cisco-compatible Frame Relay for DLCIs 0 through 511. DLCIs 512 through 1022 are dedicated to TCC.

frame-relay-port-ccc—Use Frame Relay port CCC encapsulation to transparently carry all the DLCIs between two customer edge (CE) routers without explicitly configuring each DLCI on the two provider edge (PE) routers with Frame Relay transport. The connection between the two CE routers can be either user-to-network interface (UNI) or network-to-network interface (NNI); this is completely transparent to the PE routers. When you use this encapsulation type, you can configure the **ccc** family only.

frame-relay-tcc—This encapsulation is similar to Frame Relay CCC and has the same configuration restrictions, but used for circuits with different media on either side of the connection.

generic-services—Use generic services encapsulation for services with a hierarchical scheduler.

multilink-frame-relay-uni-nni—Use MLFR UNI NNI encapsulation. This encapsulation is used on link services, voice services interfaces functioning as FRF.16 bundles, and their constituent T1 or E1 interfaces, and is supported on LSQ and redundant LSQ interfaces.

ppp—Use serial PPP encapsulation. This encapsulation is defined in RFC 1661, *The Point-to-Point Protocol (PPP) for the Transmission of Multiprotocol Datagrams over Point-to-Point Links*. PPP is the default encapsulation type for physical interfaces. E1, E3, SONET/SDH, T1, and T3 interfaces can use PPP encapsulation.

ppp-ccc—Use serial PPP encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only.

ppp-tcc—Use serial PPP encapsulation on TCC circuits for connecting different media. When you use this encapsulation type, you can configure the **tcc** family only.

vlan-ccc—Use Ethernet VLAN encapsulation on CCC circuits. VLAN CCC encapsulation supports TPID 0x8100 only. When you use this encapsulation type, you can configure the **ccc** family only.

vlan-vci-ccc—Use ATM-to-Ethernet interworking encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only. All logical interfaces configured on the Ethernet interface must also have the encapsulation type set to **vlan-vci-ccc**.

vlan-vpls—Use VLAN VPLS encapsulation on Ethernet interfaces with VLAN tagging and VPLS enabled. Interfaces with VLAN VPLS encapsulation accept packets carrying standard TPID values only. On M Series routers, except the M320 router, the 4-port Fast Ethernet TX PIC and the 1-port, 2-port, and 4-port, 4-slot Gigabit Ethernet PICs can use the Ethernet VPLS encapsulation type.



NOTE:

- Label-switched interfaces (LSIs) do not support VLAN VPLS encapsulation. Therefore, you can only use VLAN VPLS encapsulation on a PE-router-to-CE-router interface and not a core-facing interface.
- Starting with Junos OS release 13.3, a commit error occurs when you configure **vlan-vpls** encapsulation on a physical interface and configure family **inet** on one of the logical units. Previously, it was possible to commit this invalid configuration.

Required Privilege interface—To view this statement in the configuration.
Level interface-control—To add this statement to the configuration.

- Related Documentation**
- *Configuring Interface Encapsulation on Physical Interfaces*
 - *Configuring CCC Encapsulation for Layer 2 VPNs*
 - *Configuring Layer 2 Switching Cross-Connects Using CCC*
 - *Configuring TCC Encapsulation for Layer 2 VPNs and Layer 2 Circuits*
 - *Configuring ATM Interface Encapsulation*
 - *Configuring ATM-to-Ethernet Interworking*
 - *Configuring VLAN and Extended VLAN Encapsulation*
 - *Configuring VLAN and Extended VLAN Encapsulation*
 - [Configuring Encapsulation for Layer 2 Wholesale VLAN Interfaces on page 83](#)
 - *Configuring Interfaces for Layer 2 Circuits*
 - *Configuring Interface Encapsulation on PTX Series Packet Transport Routers*
 - *Configuring MPLS LSP Tunnel Cross-Connects Using CCC*
 - *Configuring TCC*
 - *Configuring VPLS Interface Encapsulation*
 - *Configuring Interfaces for VPLS Routing*
 - *Defining the Encapsulation for Switching Cross-Connects*
 - *Configuring an MPLS-Based Layer 2 VPN (CLI Procedure)*

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 ];
    acc-loop-encap [ access-request | accounting-on | accounting-off | accounting-start |
        accounting-stop ];
    acc-loop-remote-id [ access-request | accounting-on | accounting-off | 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 ];
    acct-tunnel-connection [ access-request | accounting-start | accounting-stop ];
    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 ];
    chap-challenge [ access-request ];
    chargeable-user-identity [ access-request ];
    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 ];
    first-relay-ipv4-address [ access-request | accounting-start | accounting-stop ];
    first-relay-ipv6-address [ access-request | 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 ];
    l2tp-rx-connect-speed [ access-request | accounting-start | accounting-stop ];
    l2tp-tx-connect-speed [ 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 ];
pppoe-description [ access-request | accounting-start | accounting-stop ];
tunnel-assignment-id [ access-request | accounting-start | accounting-stop ];
tunnel-client-auth-id [ access-request | accounting-start | accounting-stop ];
tunnel-client-endpoint [ access-request | accounting-start | accounting-stop ];
tunnel-medium-type [ access-request | accounting-start | accounting-stop ];
tunnel-server-auth-id [ access-request | accounting-start | accounting-stop ];
tunnel-server-endpoint [ access-request | accounting-start | accounting-stop ];
tunnel-type [ access-request | accounting-start | accounting-stop ];
upstream-calculated-qos-rate [ access-request | accounting-start | accounting-stop ];
virtual-router [ 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** added in Junos OS Release 11.4.
Options **cos-shaping-rate** and **filter-id** added in Junos OS Release 13.2.
Option **pppoe-description** added in Junos OS Release 14.2.
Option **virtual-router** added in Junos OS Release 15.1.
Options **first-relay-ipv4-address** and **first-relay-ipv6-address** added in Junos OS Release 16.1.
Options **acc-loop-encap** and **acc-loop-remote-id** added in Junos OS Release 16.1R4.
Option **access-request** support for all tunnel attributes added in Junos OS Release 15.1R7, 16.1R5, 16.2R2, 17.1R2, 17.2R2, and 17.3R1 for MX Series.

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.



NOTE: If you exclude an attribute from Acct-Off messages, the attributes are then excluded from Interim-Acct 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.
- **acc-loop-encap**—Juniper Networks VSA 26-183, Acc-Loop-Encap.
- **acc-loop-remote-id**—Juniper Networks VSA 26-182, Acc-Loop-Remote-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.
- **acct-tunnel-connection**—RADIUS attribute 68, Acct-Tunnel-Connection.
- **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.
- **chargeable-user-identity**—RADIUS attribute 89, Chargeable-User-Identity.
- **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.

- **first-relay-ipv4-address**—Juniper Networks VSA 26-187, DHCP-First-Relay-IPv4-Address.
- **first-relay-ipv6-address**—Juniper Networks VSA 26-188, DHCP-First-Relay-IPv6-Address.
- **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.
- **l2tp-rx-connect-speed**—Juniper Networks VSA 26-163, Rx-Connect-Speed
- **l2tp-tx-connect-speed**—Juniper Networks VSA 26-162, Tx-Connect-Speed
- **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.
- **pppoe-description**—Juniper Networks VSA 26-24, PPPoE-Description.
- **tunnel-assignment-id**—RADIUS attribute 82, Tunnel-Assignment-ID.
- **tunnel-client-auth-id**—RADIUS attribute 90, Tunnel-Client-Auth-ID.
- **tunnel-client-endpoint**—RADIUS attribute 66, Tunnel-Client-Endpoint.
- **tunnel-medium-type**—RADIUS attribute 65, Tunnel-Medium-Type.
- **tunnel-server-auth-id**—RADIUS attribute 91, Tunnel-Server-Auth-ID.
- **tunnel-server-endpoint**—RADIUS attribute 67, Tunnel-Server-Endpoint.

- **tunnel-type**—RADIUS attribute 64, Tunnel-Type.
- **upstream-calculated-qos-rate**—Juniper Networks VSA 26-142
- **virtual-router**—Juniper Networks VSA 26-1

RADIUS message type:

- **access-request**—RADIUS Access-Request 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	<ul style="list-style-type: none">• <i>Configuring How RADIUS Attributes Are Used for Subscriber Access</i>• <i>Configuring RADIUS Server Parameters for Subscriber Access</i>
------------------------------	---

family

```

Syntax  family family {
        accounting {
            destination-class-usage;
            source-class-usage {
                (input | output | input output);
            }
        }
        access-concentrator name;
        address address {
            ... the address subhierarchy appears after the main [edit interfaces interface-name unit
                logical-unit-number family family-name] hierarchy ...
        }
        bundle interface-name;
        core-facing;
        demux-destination {
            destination-prefix;
        }
        demux-source {
            source-prefix;
        }
        direct-connect;
        duplicate-protection;
        dynamic-profile profile-name;
        filter {
            group filter-group-number;
            input filter-name;
            input-list [ filter-names ];
            output filter-name;
            output-list [ filter-names ];
        }
        interface-mode (access | trunk);
        ipsec-sa sa-name;
        keep-address-and-control;
        mac-validate (loose | strict);
        max-sessions number;
        max-sessions-vsa-ignore;
        mtu bytes;
        multicast-only;
        negotiate-address;
        no-redirects;
        policer {
            arp policer-template-name;
            input policer-template-name;
            output policer-template-name;
        }
        primary;
        protocols [inet iso mpls];
        proxy inet-address address;
        receive-options-packets;
        receive-ttl-exceeded;
        remote (inet-address address | mac-address address);
        rpf-check {

```

```

    fail-filter filter-name
    mode loose;
}
sampling {
    input;
    output;
}
service {
    input {
        post-service-filter filter-name;
        service-set service-set-name <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> <filter [aci]>;
(translate-discard-eligible | no-translate-discard-eligible);
(translate-fecn-and-becn | no-translate-fecn-and-becn);
translate-plp-control-word-de;
unnumbered-address interface-name destination address destination-profile profile-name;
vlan-id number;
vlan-id-list [number number-number];
address address {
    arp ip-address (mac | multicast-mac) mac-address <publish>;
    broadcast address;
    destination address;
    destination-profile name;
    eui-64;
    master-only;
    multipoint-destination address dlci dlci-identifier;
    multipoint-destination address {
        epd-threshold cells;
        inverse-arp;
        oam-liveness {
            up-count cells;
            down-count cells;
        }
        oam-period (disable | seconds);
        shaping {
            (cbr rate | rtvbr burst length peak rate sustained rate | vbr burst length peak rate
                sustained rate);
            queue-length number;
        }
        vci vpi-identifier.vci-identifier;
    }
    preferred;
    primary;
    vrrp-group group-id {
        (accept-data | no-accept-data);
        advertise-interval seconds;
        authentication-key key;
        authentication-type authentication;
        fast-interval milliseconds;
    }
}

```

```
(preempt | no-preempt) {  
    hold-time seconds;  
}  
priority number;  
track {  
    interface interface-name {  
        bandwidth-threshold bits-per-second priority-cost priority;  
        priority-cost priority;  
    }  
    priority-hold-time seconds;  
    route prefix routing-instance instance-name priority-cost priority;  
}  
}  
virtual-address [ addresses ];  
}  
virtual-link-local-address ipv6-address;  
}  
}
```

Hierarchy Level [edit interfaces *interface-name* **unit** *logical-unit-number*],
[edit logical-systems *logical-system-name* interfaces *interface-name* **unit** *logical-unit-number*]

Release Information Statement introduced before Junos OS Release 7.4.
Option **max-sessions-vs-a-ignore** introduced in Junos OS Release 11.4.

Description Configure protocol family information for the logical interface.



NOTE: Not all subordinate statements are available to every protocol family.

Options *family*—Protocol family:

- **any**—Protocol-independent family used for Layer 2 packet filtering



NOTE: This option is not supported on T4000 Type 5 FPCs.

- **bridge**—(M Series and T Series routers only) Configure only when the physical interface is configured with **ethernet-bridge** type encapsulation or when the logical interface is configured with **vlan-bridge** type encapsulation. You can optionally configure this protocol family for the logical interface on which you configure VPLS.
- **ethernet-switching**—(M Series and T Series routers only) Configure only when the physical interface is configured with **ethernet-bridge** type encapsulation or when the logical interface is configured with **vlan-bridge** type encapsulation
- **ccc**—Circuit cross-connect protocol suite. You can configure this protocol family for the logical interface of CCC physical interfaces. When you use this encapsulation type, you can configure the **ccc** family only.
- **inet**—Internet Protocol version 4 suite. You must configure this protocol family for the logical interface to support IP protocol traffic, including Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), Internet Control Message Protocol (ICMP), and Internet Protocol Control Protocol (IPCP).
- **inet6**—Internet Protocol version 6 suite. You must configure this protocol family for the logical interface to support IPv6 protocol traffic, including Routing Information Protocol for IPv6 (RIPng), Intermediate System-to-Intermediate System (IS-IS), BGP, and Virtual Router Redundancy Protocol for IPv6 (VRRP).
- **iso**—International Organization for Standardization Open Systems Interconnection (ISO OSI) protocol suite. You must configure this protocol family for the logical interface to support IS-IS traffic.
- **mlfr-end-to-end**—Multilink Frame Relay FRF.15. You must configure this protocol or multilink Point-to-Point Protocol (MLPPP) for the logical interface to support multilink bundling.
- **mlfr-uni-nni**—Multilink Frame Relay FRF.16. You must configure this protocol or **mlfr-end-to-end** for the logical interface to support link services and voice services bundling.
- **multilink-ppp**—Multilink Point-to-Point Protocol. You must configure this protocol (or **mlfr-end-to-end**) for the logical interface to support multilink bundling.
- **mpls**—Multiprotocol Label Switching (MPLS). You must configure this protocol family for the logical interface to participate in an MPLS path.
- **pppoe**—Point-to-Point Protocol over Ethernet
- **tcc**—Translational cross-connect protocol suite. You can configure this protocol family for the logical interface of TCC physical interfaces.

- **tnp**—Trivial Network Protocol. This protocol is used to communicate between the Routing Engine and the router's packet forwarding components. The Junos OS automatically configures this protocol family on the router's internal interfaces only, as discussed in *Understanding Internal Ethernet Interfaces*.
- **vpls**—(M Series and T Series routers only) Virtual private LAN service. You can optionally configure this protocol family for the logical interface on which you configure VPLS. VPLS provides an Ethernet-based point-to-multipoint Layer 2 VPN to connect customer edge (CE) routers across an MPLS backbone. When you configure a VPLS encapsulation type, the **family vpls** statement is assumed by default.

MX Series routers support dynamic profiles for VPLS pseudowires, VLAN identifier translation, and automatic bridge domain configuration.

For more information about VPLS, see the *Junos OS VPNs Library for Routing Devices*.

The remaining statements are explained separately. See [CLI Explorer](#).

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">• <i>Configuring the Protocol Family</i>

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. See [CLI Explorer](#).

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](#)
- [Configuring Address-Assignment Pools](#)

family (Dynamic Demux Interface)

Syntax

```
family family {
    access-concentrator name;
    address address;
    demux-source {
        source-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> <filter [aci]>;
    unnumbered-address interface-name <preferred-source-address address>;
}
```

Hierarchy Level [edit [dynamic-profiles profile-name](#) [interfaces demux0 unit logical-unit-number](#)]

Release Information Statement introduced in Junos OS Release 9.3.
pppoe option added in Junos OS Release 11.2.

Description Configure protocol family information for the logical interface.



NOTE: Not all subordinate stanzas are available to every protocol family.

Options *family*—Protocol family:

- **inet**—Internet Protocol version 4 suite
- **inet6**—Internet Protocol version 6 suite
- **pppoe**—(MX Series routers with MPCs only) Point-to-Point Protocol over Ethernet

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles*

- *Subscriber Interfaces and Demultiplexing Overview*

family (Dynamic PPPoE)

Syntax

```
family family {
  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;
    }
  }
}
```

Hierarchy Level [edit [dynamic-profiles profile-name interfaces](#) pp0 unit "\$junos-interface-unit"]

Release Information Statement introduced in Junos OS Release 10.1.

Description Configure protocol family information for the logical interface.

Options *family*—Protocol family:

- **inet**—Internet Protocol version 4 suite
- **inet6**—Internet Protocol version 6 suite

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Configuring a PPPoE Dynamic Profile*
- *Dynamic PPPoE Subscriber Interfaces over Static Underlying Interfaces Overview*

family (Dynamic Standard Interface)

Syntax 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*;
 }
 }
 mac-validate (loose | strict);
 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> <filter [*aci*]>;
 unnumbered-address *interface-name* <preferred-source-address *address*>;
 }

Hierarchy Level [edit [dynamic-profiles](#) *profile-name* [interfaces](#) *interface-name* [unit](#) *logical-unit-number*]

Release Information Statement introduced in Junos OS Release 9.2.
pppoe option added in Junos OS Release 11.2.

Description Configure protocol family information for the logical interface.



NOTE: Not all subordinate stanzas are available to every protocol family.

Options *family*—Protocol family:

- **inet**—IP version 4 suite
- **inet6**—IP version 6 suite
- **pppoe**—(MX Series routers with MPCs only) Point-to-Point Protocol over Ethernet
- **vpls**—Virtual private LAN service

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege interface—To view this statement in the configuration.
Level interface-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring Static Routing on Logical Systems*
- *Configuring the Protocol Family*

fields (Flat-File Accounting Options)

```
Syntax  fields {
        all-fields;
        egress-stats {
            all-fields;
            input-bytes;
            input-packets;
            output-bytes;
            output-packets;
            queue-id;
            red-drop-bytes;
            red-drop-packets;
            tail-drop-packets;
        }
        general-param {
            all-fields;
            accounting-type;
            descr;
            line-id;
            logical-interface;
            nas-port-id;
            physical-interface;
            routing-instance;
            timestamp;
            user-name;
            vlan-id;
        }
        ingress-stats {
            all-fields;
            drop-packets;
            input-bytes;
            input-packets;
            output-bytes;
            output-packets;
            queue-id;
        }
        l2-stats {
            all-fields;
            input-mcast-bytes;
            input-mcast-packets;
        }
        overall-packet {
            all-fields;
            input-bytes;
            input-discards;
            input-errors;
            input-packets;
            inputv6-bytes;
            inputv6-packets;
            output-bytes;
            output-errors;
            output-packets;
            outputv6-bytes;
```

```

        outputv6-packets;
    }
    service-accounting;
}

```

Hierarchy Level [edit accounting-options [flat-file-profile](#) *profile-name*]

Release Information Statement introduced in Junos OS Release 16.1R4.

Description Specify the accounting statistics and the nonstatistical information to be collected for an interface and recorded in the accounting flat file created by the profile.

Options **all-fields**—Include all available statistical fields in the accounting file. Many fields are available for both logical interfaces and physical interfaces, but some fields are available only for one or the other interface type.

service-accounting—Include the filter counts in bytes for the inet input filter, inet output filter, inet6 input filter, and inet6 output filter in the service accounting flat file. Statistics reported are the running total values.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [Configuring Flat-File Accounting for Layer 2 Wholesale on page 181](#)
- [Configuring Flat-File Accounting for Extensible Subscriber Services Management on page 185](#)
- [Configuring Service Accounting in Local Flat Files on page 189](#)
- [Flat-File Accounting Overview on page 177](#)

file (Flat-File Accounting Options)

Syntax	file <i>filename</i> ;
Hierarchy Level	[edit accounting-options flat-file-profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 16.1R4.
Description	Specify the name of the accounting file created by a flat-file profile. By default, the filename becomes the name of the local directory where the accounting file is backed up: <code>/var/log/pfedBackup/<i>filename</i></code> .
Options	<i>filename</i> —Name of the accounting file. The complete output filename is in the format <i>filename.hostname.file-number_timestamp.gz</i> .
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 Flat-File Accounting for Layer 2 Wholesale on page 181• Configuring Flat-File Accounting for Extensible Subscriber Services Management on page 185• Flat-File Accounting Overview on page 177

flat-file-profile (Accounting Options)

```
Syntax flat-file-profile profile-name{
    fields {
        all-fields;
        egress-stats {
            all-fields;
            input-bytes;
            input-packets;
            output-bytes;
            output-packets;
            queue-id;
            red-drop-bytes;
            red-drop-packets;
            tail-drop-packets;
        }
        general-param {
            all-fields;
            accounting-type;
            descr;
            line-id;
            logical-interface;
            nas-port-id;
            physical-interface;
            routing-instance;
            timestamp;
            user-name;
            vlan-id;
        }
        ingress-stats {
            all-fields;
            drop-packets;
            input-bytes;
            input-packets;
            output-bytes;
            output-packets;
            queue-id;
        }
        l2-stats {
            all-fields;
            input-mcast-bytes;
            input-mcast-packets;
        }
        overall-packet {
            all-fields;
            input-bytes;
            input-discards;
            input-errors;
            input-packets;
            inputv6-bytes;
            inputv6-packets;
            output-bytes;
            output-errors;
            output-packets;
        }
    }
}
```

```
        outputv6-bytes;  
        outputv6-packets;  
    }  
    service-accounting;  
}  
file filename;  
format (csv | ipdr)  
interval minutes;  
schema-version schema-name;  
}
```

Hierarchy Level [edit *accounting-options*]

Release Information Statement introduced in Junos OS Release 16.1R4.
service-accounting option added in Junos OS Release 17.1.

Description Configure a flat-file accounting profile that defines the contents of a flat file that records accounting statistics collected from the Packet Forwarding Engine for an interface at regular intervals. To be used, the profile is associated with a subscriber interface. The accounting flat file is archived by the accounting-options archiving mechanism.

Options ***profile-name***—Name of the flat-file profile.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [Configuring Accounting-Data Log Files](#)
- [Configuring Flat-File Accounting for Layer 2 Wholesale on page 181](#)
- [Configuring Flat-File Accounting for Extensible Subscriber Services Management on page 185](#)
- [Configuring Service Accounting in Local Flat Files on page 189](#)
- [Flat-File Accounting Overview on page 177](#)
- [show extensible-subscriber-services accounting](#)

flat-file-profile (Extensible Subscriber Services)

Syntax	<code>flat-file-profile <i>profile-name</i></code>
Hierarchy Level	<code>[edit system services extensible-subscriber-services]</code>
Release Information	Statement introduced in Junos OS Release 16.1.
Description	Specify the name of an accounting flat file profile that applies to an ESSM subscriber.
Options	<i>profile name</i> —Name of an accounting flat file profile configured at the <code>[edit accounting-options]</code> hierarchy level.
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 Flat-File Accounting for Extensible Subscriber Services Management on page 185

flexible-vlan-tagging

Syntax	flexible-vlan-tagging;
Hierarchy Level	[edit interfaces <i>aex</i>], [edit interfaces <i>ge-fpc/pic/port</i>], [edit interfaces <i>et-fpc/pic/port</i>], [edit interfaces <i>ps0</i>], [edit interfaces <i>xe-fpc/pic/port</i>]
Release Information	Statement introduced in Junos OS Release 8.1. Support for aggregated Ethernet added in Junos OS Release 9.0. Statement introduced in Junos OS Release 12.1x48 for PTX Series Packet Transport Routers. Statement introduced in Junos OS Release 13.2X50-D15 for EX Series switches. Statement introduced in Junos OS Release 13.2X51-D20 for the QFX Series.
Description	<p>Support simultaneous transmission of 802.1Q VLAN single-tag and dual-tag frames on logical interfaces on the same Ethernet port, and on pseudowire logical interfaces.</p> <p>This statement is supported on M Series and T Series routers, for Fast Ethernet and Gigabit Ethernet interfaces only on Gigabit Ethernet IQ2 and IQ2-E, IQ, and IQE PICs, and for aggregated Ethernet interfaces with member links in IQ2, IQ2-E, and IQ PICs or in MX Series DPCs, or on Ethernet interfaces for PTX Series Packet Transport Routers or 100-Gigabit Ethernet Type 5 PIC with CFP.</p> <p>This statement is supported on Gigabit Ethernet, 10-Gigabit Ethernet, 40-Gigabit Ethernet, and aggregated Ethernet interfaces on EX Series and QFX Series switches.</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">• <i>Configuring Mixed Tagging</i>• <i>Configuring Flexible VLAN Tagging on PTX Series Packet Transport Routers</i>• <i>Configuring Double-Tagged VLANs on Layer 3 Logical Interfaces</i>

format (Flat-File Accounting Options)

Syntax	format (csv ipdr);
Hierarchy Level	[edit accounting-options flat-file-profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 16.1R4.
Description	Specify the format for logging the flat-file accounting statistics.
Options	csv —Comma-separated values (CSV) format. ipdr —IP Detail Record (IPDR) format. Default: ipdr
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 Flat-File Accounting for Layer 2 Wholesale on page 181• Configuring Flat-File Accounting for Extensible Subscriber Services Management on page 185• Flat-File Accounting Overview on page 177

forwarding-options

Syntax	forwarding-options { ... }
Hierarchy Level	[edit] [edit routing-instance <i>routing-instance-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure traffic forwarding. The statements that apply to services interfaces are explained separately. For other statements, see the <i>Routing Policies, Firewall Filters, and Traffic Policers Feature Guide</i> .



NOTE: The next-hop-group statement is present in the forwarding-options stanza for a routing instance, but the next-hop-group statement is not allowed in a routing instance. In other words, in a routing instance, [edit routing-instances *routing-instance-name* forwarding-options next-hop-group] is not supported. You will get an error message if you try to commit this type of configuration.

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">• <i>Configuring Flow Monitoring</i>• <i>Configuring Traffic Sampling</i>

general-param (Flat-File Accounting Options)

Syntax	<pre> general-param { all-fields; accounting-type; descr; line-id; logical-interface; nas-port-id; physical-interface; routing-instance; timestamp; user-name; vlan-id; } </pre>
Hierarchy Level	[edit accounting-options flat-file-profile <i>profile-name</i> fields]
Release Information	Statement introduced in Junos OS Release 16.1R4. user-name option added in Junos OS Release 17.1.
Description	Specify general, nonstatistical interface parameters that are displayed as part of the header for the accounting file.
Options	<p>all-fields—Display all available nonstatistical fields. Many fields are available for both logical interfaces and physical interfaces, but some fields are available for only one interface type.</p> <p>accounting-type—(Logical interfaces only) Display the accounting status type.</p> <p>descr—Display the description of the interface as configured.</p> <p>line-id—(Logical interfaces only) Display the access line identifier.</p> <p>logical-interface—(Logical interfaces only) Display the name of the logical interface.</p> <p>nas-port-id—(Logical interfaces only) Display the NAS port ID.</p> <p>physical-interface—(Physical interfaces only) Display the name of the physical interface.</p> <p>routing-instance—Display the name of the routing instance to which the interface belongs.</p> <p>timestamp—Display the timestamp of the accounting record.</p> <p>user-name—Display the name of the subscriber.</p> <p>vlan-id—(Logical interfaces only) Display the VLAN identifier.</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**
- [Configuring Flat-File Accounting for Layer 2 Wholesale on page 181](#)
 - [Configuring Flat-File Accounting for Extensible Subscriber Services Management on page 185](#)
 - [Configuring Service Accounting in Local Flat Files on page 189](#)
 - [Flat-File Accounting Overview on page 177](#)

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], [edit access protocol-attributes <i>attribute-set-name</i>]
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	seconds —Number of seconds the lease is retained. Range: 0 through 4,294,967,295 seconds Default: 0 (no grace period)
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

group (DHCP Local Server)

```
Syntax  group group-name {
        access-profile profile-name;
        authentication {
            password password-string;
            username-include {
                circuit-type;
                client-id;
                delimiter delimiter-character;
                domain-name domain-name-string;
                interface-description (device-interface | logical-interface);
                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 {
            access-profile profile-name;
            exclude;
            overrides {
                asymmetric-lease-time seconds;
                asymmetric-prefix-lease-time seconds;
                client-discover-match <option60-and-option82>;
                client-negotiation-match 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 {
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-discover-match <option60-and-option82>;
    client-negotiation-match incoming-interface;
    delegated-pool;
    delete-binding-on-renegotiation;
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
    protocol-attributes attribute-set-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 [edit system services [dhcp-local-server](#)],
[edit system services [dhcp-local-server dhcpv6](#)],
[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 12.1 for EX Series switches.

Description Configure a group of interfaces that have a common configuration, such as authentication parameters. A group must contain at least one interface.

Options *group-name*—Name of the group.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege system—To view this statement in the configuration.
Level system-control—To add this statement to the configuration.

Related Documentation

- *Extended DHCP Local Server Overview*
- *Grouping Interfaces with Common DHCP Configurations*
- *Using External AAA Authentication Services with DHCP*
- *Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*

group (DHCP Relay Agent)

```
Syntax  group group-name {
        access-profile profile-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;
                interface-description (device-interface | logical-interface);
                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;
        }
        forward-only {
            logical-system <current | default | logical-system-name>;
            routing-instance <current | default | routing-instance-name>;
        }
        interface interface-name {
            access-profile profile-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;
  asymmetric-lease-time seconds;
  asymmetric-prefix-lease-time seconds;
  client-discover-match <option60-and-option82>;
  client-negotiation-match incoming-interface;
  disable-relay;
  dual-stack dual-stack-group-name;
  interface-client-limit number;
  layer2-unicast-replies;
  no-allow-snooped-clients;
  no-bind-on-request;
  proxy-mode;
  relay-source
  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);
  use-option-82 <strict>;
}
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);  
    }  
    server-id-override  
}  
route-suppression;  
service-profile dynamic-profile-name;  
}
```

Hierarchy Level [edit forwarding-options [dhcp-relay](#)],
[edit forwarding-options dhcp-relay dhcpv6],
[edit logical-systems *logical-system-name* forwarding-options [dhcp-relay](#) ...],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name*
forwarding-options [dhcp-relay](#) ...],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay ...]

Release Information Statement introduced in Junos OS Release 8.3.
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 *group-name*—Name of a group of interfaces that have a common DHCP or DHCPv6 relay agent configuration.

The remaining statements are explained separately. See [CLI Explorer](#).

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 239](#)
 - *Extended DHCP Relay Agent Overview*
 - *Understanding the Extended DHCP Relay Agent for EX Series Switches*
 - *Configuring an Extended DHCP Relay Server on EX Series Switches (CLI Procedure)*
 - *Configuring Group-Specific DHCP Relay Options*
 - *Grouping Interfaces with Common DHCP Configurations*
 - *Using External AAA Authentication Services with DHCP*
 - *Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*

ingress-stats (Flat-File Accounting Options)

Syntax	<pre>ingress-stats { all-fields; drop-packets; input-bytes; input-packets; output-bytes; output-packets; queue-id; }</pre>
Hierarchy Level	[edit accounting-options flat-file-profile <i>profile-name</i> fields]
Release Information	Statement introduced in Junos OS Release 16.1R4.
Description	Specify ingress queue statistics to be collected for the interface.
Options	<p>all-fields—Collect all ingress queue statistics available for the interface context, logical or physical.</p> <p>drop-packets—Collect the number of received packets dropped on the Ingress queue.</p> <p>input-bytes—Collect the number of octets received on the queue for the traffic class indicated by the queue identifier.</p> <p>input-packets—Collect the number of packets received on the queue for the traffic class indicated by the queue identifier.</p> <p>output-bytes—Collect the number of octets forwarded for the traffic class indicated by the queue identifier. Same value as input-bytes unless oversubscription is present at the ingress.</p> <p>output-packets—Collect the number of packets forwarded for the traffic class indicated by the queue identifier. Same value as input-packets unless oversubscription is present at the ingress.</p> <p>queue-id—Collect the logical identifier for the ingress queue; identifies the traffic class.</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 Flat-File Accounting for Layer 2 Wholesale on page 181• Configuring Flat-File Accounting for Extensible Subscriber Services Management on page 185• Flat-File Accounting Overview on page 177

inner-vlan-id (Dynamic VLANs)

Syntax	<code>inner-vlan-id <i>number</i>;</code>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map], [edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	<p>For dynamic VLAN interfaces, specify the VLAN ID to rewrite for the inner tag of the final packet.</p> <p>You cannot include the <code>inner-vlan-id</code> statement with the <code>swap</code> statement, <code>swap-push</code> statement, <code>push-push</code> statement, or <code>push-swap</code> statement and the <code>inner-vlan-id</code> statement at the [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map] hierarchy level. If you include any of those statements in the output VLAN map, the VLAN ID in the outgoing frame is rewritten to the <code>inner-vlan-id</code> statement you include at the [edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>] hierarchy level.</p>
Options	<p><i>number</i>—VLAN ID number. When used for input VLAN maps, you can specify the <code>\$junos-inner-vlan-map-id</code> predefined variable to dynamically obtain the VLAN identifier.</p> <p>Range: 0 through 4094</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 Inner and Outer TPIDs and VLAN IDs

inner-vlan-id-swap-ranges

Syntax	<code>inner-vlan-id-swap-ranges <i>low-inner-tag</i>–<i>high-inner-tag</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]
Release Information	Statement introduced in Junos OS Release 17.2R1.
Description	<p>Define core-facing VLAN ID ranges from which an inner VLAN ID tag can be allocated to replace the outer VLAN tag that was appended by the access node on the upstream packets to the BNG in a Layer 2 wholesale network. The tag swap occurs before the subscriber traffic is forwarded to the network service provider (NSP). You can configure up to 32 non-overlapping inner VLAN ID ranges per core-facing physical interface for VLAN-OOB subscribers.</p> <p>You can add or remove ranges or increase or decrease the size of existing ranges even while Layer 2 wholesale sessions are assigned to the core-facing interface associated with the ranges. You cannot remove a range from which a VLAN ID has already been allocated. You cannot reduce a range if the new range excludes a VLAN ID that has already been allocated.</p>
Options	<p><i>low-inner-tag</i>—Inner (core-facing) VLAN ID tag representing the lower limit of the swap range. Range: 1 through 4094.</p> <p><i>high-inner-tag</i>—Inner (core-facing) VLAN ID tag representing the upper limit of the swap range. Range: 1 through 4094.</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 Multiple Non-Overlapping VLAN Ranges for Core-Facing Physical Interfaces on page 173• Layer 2 Wholesale with ANCP-Triggered VLANs Overview on page 99

input-vlan-map (Dynamic Interfaces)

Syntax	<pre>input-vlan-map { inner-tag-protocol-id <i>tpid</i>; inner-vlan-id <i>number</i>; (push swap); tag-protocol-id <i>tpid</i>; vlan-id <i>number</i>; }</pre>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	<p>For dynamic interfaces, define the rewrite profile to be applied to incoming frames on this logical interface.</p> <p>The remaining statements are explained separately. See CLI Explorer.</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"> • Stacking and Rewriting VLAN Tags for the Layer 2 Wholesale Solution on page 80

interface (DHCP Local Server)

Syntax `interface interface-name {
 access-profile profile-name;
 exclude;
 overrides {
 asymmetric-lease-time seconds;
 asymmetric-prefix-lease-time seconds;
 client-discover-match <option60-and-option82 | incoming-interface>;
 client-negotiation-match 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 supports only static DHCP configurations.

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. See [CLI Explorer](#).

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">• <i>Extended DHCP Local Server Overview</i>• <i>Grouping Interfaces with Common DHCP Configurations</i>• <i>Using External AAA Authentication Services with DHCP</i>
------------------------------	---

interface (DHCP Relay Agent)

Syntax	<pre>interface <i>dhcp-interface-name</i> { <i>access-profile profile-name</i>; exclude; overrides { allow-no-end-option allow-snooped-clients; always-write-giaddr; always-write-option-82; asymmetric-lease-time <i>seconds</i>; asymmetric-prefix-lease-time <i>seconds</i>; client-discover-match <option60-and-option82 incoming-interface>; client-negotiation-match incoming-interface; disable-relay; dual-stack <i>dual-stack-group-name</i>; interface-client-limit <i>number</i>; layer2-unicast-replies; no-allow-snooped-clients; proxy-mode; relay-source 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 <i>group group-name</i>], [edit forwarding-options dhcp-relay <i>group group-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options <i>dhcp-relay ...</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options <i>dhcp-relay ...</i>], [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. .

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. See [CLI Explorer](#).

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*
- *Grouping Interfaces with Common DHCP Configurations*
- *Using External AAA Authentication Services with DHCP*

interface (Dynamic Routing Instances)

Syntax	<code>interface <i>interface-name</i>;</code>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> routing-instances <i>routing-instance-name</i>]
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Assign the specified interface to the dynamically created routing instance.
Options	<i>interface-name</i> —The interface name variable (<i>\$junos-interface-name</i>). The interface name variable is dynamically replaced with the interface the accessing client uses when connecting to the router.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	

interface (Routing Instances)

Syntax	<pre>interface <i>interface-name</i> { description <i>text</i>; }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>], [edit routing-instances <i>routing-instance-name</i>]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.2 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 12.3 for ACX Series routers.</p> <p>Statement introduced in Junos OS Release 13.2 for MX 3D Series routers.</p>
Description	Specify the interface over which the VPN traffic travels between the PE device and CE device. You configure the interface on the PE device. If the value vrf is specified for the instance-type statement included in the routing instance configuration, this statement is required.
Options	<p><i>interface-name</i>—Name of the interface.</p> <p>The remaining statement is explained separately. See CLI Explorer.</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>Configuring Routing Instances on PE Routers in VPNs</i> • <i>Configuring EVPN Routing Instances</i> • <i>Configuring EVPN Routing Instances on EX9200 Switches</i> • <i>interface (VPLS Routing Instances)</i>

interface-mac-limit (VPLS)

Syntax	<code>interface-mac-limit <i>limit</i> { packet-action drop; }</code>
Hierarchy Level	<code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls site <i>site-name</i> interfaces <i>interface-name</i>],</code> <code>[edit routing-instances <i>routing-instance-name</i> protocols evpn],</code> <code>[edit routing-instances <i>routing-instance-name</i> protocols evpn interface <i>interface-name</i>],</code> <code>[edit routing-instances <i>routing-instance-name</i> protocols vpls site <i>site-name</i> interfaces <i>interface-name</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4. Support for EVPNs introduced in Junos OS Release 13.2 on MX 3D Series routers. Support for EVPNs introduced in Junos OS Release 14.2 on EX Series switches.
Description	<p>Specify the maximum number of media access control (MAC) addresses that can be learned by the EVPN or VPLS routing instance. You can configure the same limit for all interfaces configured for a routing instance. You can also configure a limit for a specific interface.</p> <p>Starting with Junos OS Release 12.3R4, if you do not configure the parameter to limit the number of MAC addresses to be learned by a VPLS instance, the default value is not effective. Instead, if you do not include the interface-mac-limit option at the <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls site <i>site-name</i> interfaces <i>interface-name</i>]</code>, hierarchy level, this setting is not present in the configuration with the default value of 1024 addresses. If you upgrade a router running a Junos OS release earlier than Release 12.3R4 to Release 12.3R4 or later, you must configure the interface-mac-limit option with a valid value for it to be saved in the configuration.</p>
Options	<p>limit—Number of MAC addresses that can be learned from each interface.</p> <p>Range: 16 through 65,536 MAC addresses</p> <p>Default: 1024 addresses</p> <p>The remaining statement is explained separately. See CLI Explorer.</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>Configuring EVPN Routing Instances</i>• <i>Configuring EVPN Routing Instances on EX9200 Switches</i>• <i>Configuring VPLS Routing Instances</i>• <i>interface</i>

- *mac-table-size*

interfaces

Syntax	<code>interfaces { ... }</code>
Hierarchy Level	[edit]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure interfaces on the router or switch.
Default	The management and internal Ethernet interfaces are automatically configured. You must configure all other interfaces.
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"> • <i>Physical Interface Configuration Statements Overview</i> • <i>Configuring Aggregated Ethernet Link Protection</i>

interfaces (Static and Dynamic Subscribers)

```
Syntax  interfaces {
        interface-name {
            unit logical-unit-number {
                auto-configure {
                    agent-circuit-identifier {
                        dynamic-profile profile-name;
                    }
                    line-identity {
                        include {
                            accept-no-ids;
                            circuit-id;
                            remote-id;
                        }
                        dynamic-profile profile-name;
                    }
                }
            }
            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 {
                    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>;
}
filter {
    input filter-name {
        precedence precedence;
        shared-name filter-shared-name;
    }
    output filter-name {
        precedence precedence;
        shared-name filter-shared-name;
    }
}
host-prefix-only;
ppp-options {
    chap;
    pap;
}
proxy-arp;
service {
    pcef pcef-profile-name {
        activate rule-name | activate-all;
    }
}
vlan-id;
vlan-tags outer [tpid].vlan-id [inner [tpid].vlan-id];
}
vlan-tagging;
}
interface-set interface-set-name {
    interface interface-name {
        unit logical unit number {
            advisory-options {
                downstream-rate rate;
                upstream-rate rate;
            }
        }
    }
}
pppoe-underlying-options {
    max-sessions number;
}
}
demux0 {
    unit logical-unit-number {
        demux-options {
            underlying-interface interface-name
        }
        family family {
            access-concentrator name;
        }
    }
}

```

```
address address;
direct-connect;
duplicate-protection;
dynamic-profile profile-name;
demux-source {
    source-prefix;
}
filter {
    input filter-name (
        precedence precedence;
        shared-name filter-shared-name;
    )
    output filter-name {
        precedence precedence;
        shared-name filter-shared-name;
    }
}
mac-validate (loose | strict):
max-sessions number;
max-sessions-vsa-ignore;
rpf-check {
    fail-filter filter-name;
    mode loose;
}
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>;
}
filter {
    input filter-name;
    output filter-name;
}
vlan-id number;
vlan-tags outer [tpid].vlan-id [inner [tpid].vlan-id];
}
}
pp0 {
    unit logical-unit-number {
        keepalives interval seconds;
        no-keepalives;
        pppoe-options {
            underlying-interface interface-name;
            server;
        }
        ppp-options {
            aaa-options aaa-options-name;
            authentication [ authentication-protocols ];
            chap {
                challenge-length minimum minimum-length maximum maximum-length;
            }
            initiate-ncp (ip | ipv6 | dual-stack-passive)
            ipcp-suggest-dns-option;
            mru size;
            mtu (size | use-lower-layer);
            on-demand-ip-address;
```

```

pap;
peer-ip-address-optional;
}
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;
    shared-name filter-shared-name;
  }
  output filter-name {
    precedence precedence;
    shared-name filter-shared-name;
  }
}
}
}
}
}
}

```

Hierarchy Level [edit [dynamic-profiles](#) *profile-name*]

Release Information Statement introduced in Junos OS Release 9.2.

Description Define interfaces for dynamic profiles.

Options *interface-name*—The interface variable (`$junos-interface-ifd-name`). The interface variable is dynamically replaced with the interface the DHCP client accesses when connecting to the router.



NOTE: Though we do not recommend it, you can also enter the specific name of the interface you want to assign to the dynamic profile.


The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.


Related Documentation

- *Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles*
- *Configuring Dynamic PPPoE Subscriber Interfaces*
- *Configuring Dynamic VLANs Based on Agent Circuit Identifier Information*
- *DHCP Subscriber Interface Overview*
- *Configuring Subscribers over Static Interfaces*
- *Demultiplexing Interface Overview*

interval (Flat-File Accounting Options)

Syntax	<code>interval <i>minutes</i>;</code>
Hierarchy Level	[edit accounting-options flat-file-profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 16.1R4.
Description	Specify the interval in minutes at which the Packet Forwarding Engine associated with the interface is polled to collect the statistics specified in the flat-file accounting profile. These interim accounting results are recorded in the flat file.
	<div>  <p>NOTE: The value configured with this statement is superseded by the value configured with the <i>update-interval</i> statement at the [edit access profile <i>profile-name</i> service accounting] hierarchy level. That access profile interval value is in turn superseded by an update interval value configured in the RADIUS attribute, Service-Interim-Acct-Interval (VSA 26–140).</p> </div>
Options	<p><i>minutes</i>—Polling interval.</p> <p>Range: 1 through 2880 minutes</p> <p>Default: 15 minutes</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 Flat-File Accounting for Layer 2 Wholesale on page 181 • Configuring Flat-File Accounting for Extensible Subscriber Services Management on page 185 • Configuring Service Accounting in Local Flat Files on page 189 • Flat-File Accounting Overview on page 177

instance-role

Syntax	instance-role (access nni);
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>], [edit routing-instances <i>routing-instance-name</i>]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	Define the role of the routing instance in a Layer 2 Wholesale network.
Options	<p>access—Defines the connectivity role of the routing instance in a Layer 2 Wholesale network as an access routing instance. When defined for this role, the same process occurs as in a Layer 3 Wholesale network—when the first packet is received from a given client, authentication for the client initiates with an external entity (for example, RADIUS). If authentication is successful, a logical interface is created with the appropriate outer and inner VLAN tags for that client.</p> <p>nni—Defines the connectivity role of the routing instance in a Layer 2 Wholesale network as a network to network interface (NNI) routing instance. When defined for this role, only outer VLAN tags are learned. In addition, when the NNI routing instance receives a response from the ISP, the packets are forwarded to the appropriate client, provided the packet has the same two tags that were verified during authentication.</p>
<div> NOTE: If you connect an access node or MSAN device to a router participating in the Layer 2 Wholesale network in an NNI role, you must create a new routing instance of type l2backhaul-vpn with an instance role of type access for that connection.</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 Separate Access Routing Instances for Layer 2 Wholesale Service Retailers on page 86• Configuring Separate NNI Routing Instances for Layer 2 Wholesale Service Retailers on page 89• Subscriber Management Overview

instance-type

Syntax	<code>instance-type type;</code>
Hierarchy Level	<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>
Release Information	Statement introduced before Junos OS Release 7.4. virtual-switch and layer2-control options introduced in Junos OS Release 8.4. Statement introduced in Junos OS Release 9.2 for EX Series switches. Statement introduced in Junos OS Release 11.3 for the QFX Series. Statement introduced in Junos OS Release 12.3 for ACX Series routers. mpls-internet-multicast option introduced in Junos OS Release 11.1 for the EX Series, M Series, MX Series, and T Series. evpn option introduced in Junos OS Release 13.2 for MX 3D Series routers. forwarding option introduced in Junos OS Release 14.2 for the PTX Series. mpls-forwarding option introduced in Junos OS Release 16.1 for the MX Series. evpn-vpws option introduced in Junos OS Release 17.1 for MX Series routers.
Description	Define the type of routing instance.

Options



NOTE: On ACX Series routers, you can configure only the forwarding, virtual router, and VRF routing instances.

type—Can be one of the following:

- **evpn**—(MX 3D Series routers and QFX switches only) Enable an Ethernet VPN (EVPN) on the routing instance.
You cannot configure the **evpn** option under the `[edit logical-systems logical-system-name routing-instances routing-instance-name instance-type]` hierarchy level.
- **evpn-vpws**—Enable an Ethernet VPN (EVPN) Virtual Private Wire Service (VPWS) on the routing instance.
- **forwarding**—Provide support for filter-based forwarding, where interfaces are not associated with instances. All interfaces belong to the default instance. Other instances are used for populating RPD learned routes. For this instance type, there is no one-to-one mapping between an interface and a routing instance. All interfaces belong to the default instance inet.0.
- **l2backhaul-vpn**—Provide support for Layer 2 wholesale VLAN packets with no existing corresponding logical interface. When using this instance, the router learns both the outer tag and inner tag of the incoming packets, when the **instance-role** statement is defined as **access**, or the outer VLAN tag only, when the **instance-role** statement is defined as **nni**.

- **l2vpn**—Enable a Layer 2 VPN on the routing instance. You must configure the **interface**, **route-distinguisher**, **vrf-import**, and **vrf-export** statements for this type of routing instance.
- **layer2-control**—(MX Series routers only) Provide support for RSTP or MSTP in customer edge interfaces of a VPLS routing instance. This instance type cannot be used if the customer edge interface is multihomed to two provider edge interfaces. If the customer edge interface is multihomed to two provider edge interfaces, use the default BPDU tunneling.
- **mpls-forwarding**—(MX Series routers only) Allow filtering and translation of route distinguisher (RD) values in IPv4 and IPv6 VPN address families on both routes received and routes sent for selected BGP sessions. In particular, for Inter-AS VPN Option-B networks, this option can prevent the malicious injection of VPN labels from one peer AS boundary router to another.
- **mpls-internet-multicast**—(EX Series, M Series, MX Series, and T Series routers only) Provide support for ingress replication provider tunnels to carry IP multicast data between routers through an MPLS cloud, using MBGP or next-generation MVPN.
- **no-forwarding**—This is the default routing instance. Do not create a corresponding forwarding instance. Use this routing instance type when a separation of routing table information is required. There is no corresponding forwarding table. All routes are installed into the default forwarding table. IS-IS instances are strictly nonforwarding instance types.
- **virtual-router**—Enable a virtual router routing instance. This instance type is similar to a VPN routing and forwarding instance type, but used for non-VPN-related applications. You must configure the **interface** statement for this type of routing instance. You do not need to configure the **route-distinguisher**, **vrf-import**, and **vrf-export** statements.
- **virtual-switch**—(MX Series routers, EX9200 switches, and QFX switches only) Provide support for Layer 2 bridging. Use this routing instance type to isolate a LAN segment with its Spanning Tree Protocol (STP) instance and to separate its VLAN identifier space.
- **vpls**—Enable VPLS on the routing instance. Use this routing instance type for point-to-multipoint LAN implementations between a set of sites in a VPN. You must configure the **interface**, **route-distinguisher**, **vrf-import**, and **vrf-export** statements for this type of routing instance.
- **vrf**—VPN routing and forwarding (VRF) instance. Provides support for Layer 3 VPNs, where interface routes for each instance go into the corresponding forwarding table only. Required to create a Layer 3 VPN. Create a VRF table (**instance-name.inet.0**) that contains the routes originating from and destined for a particular Layer 3 VPN. For this instance type, there is a one-to-one mapping between an interface and a routing instance. Each VRF instance corresponds with a forwarding table. Routes on an interface go into the corresponding forwarding table. You must configure the **interface**, **route-distinguisher**, **vrf-import**, and **vrf-export** statements for this type of routing instance.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Configuring Routing Instances on PE Routers in VPNs*
- *Configuring EVPN Routing Instances*
- *Configuring EVPN Routing Instances on EX9200 Switches*
- *Configuring Virtual Router Routing Instances*
- *Example: Configuring Filter-Based Forwarding on the Source Address*
- *Example: Configuring Filter-Based Forwarding on Logical Systems*
- *vpws-service-id*

ip-address-first

Syntax ip-address-first;

Hierarchy Level [edit logical-systems *logical-system-name* system services dhcp-local-server [pool-match-order](#)],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server [pool-match-order](#)],
[edit routing-instances *routing-instance-name* 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 9.0.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description Configure the extended DHCP local server to use the IP address method to determine which address-assignment pool to use. The local server uses the IP address in the 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.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use*
- *Extended DHCP Local Server Overview*
- *Address-Assignment Pools Overview*

keepalives (Dynamic Profiles)

Syntax	keepalives { interval <i>seconds</i> ; }
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit <i>logical-unit-number</i>] [edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit"] [edit dynamic-profiles <i>profile-name</i> interfaces "\$junos-interface-ifd-name" unit "\$junos-interface-unit"]
Release Information	Statement introduced in Junos OS Release 9.5. Support at the [edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit"] hierarchy level introduced in Junos OS Release 10.1. Support at the [edit dynamic-profiles <i>profile-name</i> interfaces "\$junos-interface-ifd-name" unit "\$junos-interface-unit"] hierarchy level introduced in Junos OS Release 12.2.
Description	Specify the keepalive interval in a PPP dynamic profile.
Default	Sending of keepalives is enabled by default.
Options	interval <i>seconds</i> —The time in seconds between successive keepalive requests. Range: 1 through 32767 seconds Default: 30 seconds for LNS-based PPP sessions. 10 seconds for all other PPP sessions.
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">• <i>Dynamic Profiles Overview</i>• <i>Configuring Dynamic Authentication for PPP Subscribers</i>• <i>Applying PPP Attributes to L2TP LNS Subscribers per Inline Service Interface</i>

l2-stats (Flat-File Accounting Options)

Syntax	<pre>l2-stats { all-fields; input-mcast-bytes; input-mcast-packets; }</pre>
Hierarchy Level	[edit accounting-options flat-file-profile <i>profile-name</i> fields]
Release Information	Statement introduced in Junos OS Release 16.1R4.
Description	Specify the statistics to collect for the named flat-file-profile field.
Options	<p>all-fields—Collect all Layer 2 statistics for the named flat-file profile.</p> <p>input-mcast-bytes—Collect multicast bytes from the input side for the named flat-file profile.</p> <p>input-mcast-packets—Collect multicast packets from the input side for the named flat-file profile.</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 Flat-File Accounting for Layer 2 Wholesale on page 181 • Configuring Flat-File Accounting for Extensible Subscriber Services Management on page 185 • Flat-File Accounting Overview on page 177

mac-validate (Dynamic IP Demux Interface)

Syntax	mac-validate (loose strict);
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> interfaces demux0 unit <i>logical-unit-number</i> family inet]
Release Information	Statement introduced in Junos OS Release 9.3.
Description	Enable IP and MAC address validation for dynamic IP demux interfaces in a dynamic profile.
Options	<p>loose—Forwards incoming packets when both the IP source address and the MAC source address match one of the trusted address tuples. Drops packets when the IP source address matches one of the trusted tuples, but the MAC address does not match the MAC address of the tuple. Continues to forward incoming packets when the source address of the incoming packet does not match any of the trusted IP addresses.</p> <p>strict—Forwards incoming packets when both the IP source address and the MAC source address match one of the trusted address tuples. Drops packets when the MAC address does not match the tuple's MAC source address, or when IP source address of the incoming packet does not match any of the trusted IP addresses.</p>
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring MAC Address Validation for Subscriber Interfaces</i>

multicast-replication

Syntax multicast-replication {
 ingress;
 local-latency-fairness;
 }

Hierarchy Level [edit forwarding-options]

Release Information Statement introduced in Junos OS Release 15.1 for MX Series routers.

Description Configure the mode of multicast replication that helps to optimize multicast latency.



NOTE: The `multicast-replication` statement is supported only on platforms with the enhanced-ip mode enabled.

Default This statement is disabled by default.

Options **ingress**—Complete ingress replication of the multicast data packets where all the egress Packet Forwarding Engines receive packets from the ingress Packet Forwarding Engines directly.

local-latency-fairness—Complete parallel replication of the multicast data packets.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Documentation • [forwarding-options on page 304](#)



neighbor (Define ANCP)

Syntax	<pre>neighbor <i>ip-address</i> { adjacency-loss-hold-time <i>seconds</i>; adjacency-timer; auto-configure-trigger interface <i>interface-name</i>; ietf-mode; maximum-discovery-table-entries <i>entry-number</i>; pre-ietf-mode; }</pre>
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	<p><i>ip-address</i>—IP address of the ANCP neighbor.</p> <p>The remaining statements are explained separately. See CLI Explorer.</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• Configuring ANCP Neighbors on page 165

no-local-switching

Syntax	<pre>no-local-switching</pre>
Hierarchy Level	[edit vlans <i>vlan-name</i>]
Release Information	Statement introduced in Junos OS Release 9.3 for EX Series switches.
Description	Specify that access ports in this VLAN domain do not forward packets to each other. You use this statement with primary VLANs and isolated secondary VLANs.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

no-tunnel-services

Syntax	no-tunnel-services;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> protocols vpls static-vpls], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls], [edit protocols vpls static-vpls], [edit routing-instances <i>routing-instance-name</i> protocols vpls]
Release Information	Statement introduced in Junos OS Release 7.6. Support for static VPLS added in Junos OS Release 10.2.
Description	Configure VPLS on a router without a Tunnel Services PIC. Configuring the no-tunnel-services statement creates a label-switched interface (LSI) to provide VPLS functionality. An LSI MPLS label is used as the inner label for VPLS. This label maps to a VPLS routing instance. On the PE router, the LSI label is stripped and then mapped to a logical LSI interface. The Layer 2 Ethernet frame is then forwarded using the LSI interface to the correct VPLS routing instance.
<div>  <p>NOTE: In VPLS documentation, the word <i>Router</i> in terms such as <i>PR Router</i> is used to refer to any device that provides routing functions.</p> </div>	
<p>Label-switched interfaces configured with the no-tunnel-services statement are not supported with GRE tunnels.</p>	
<div>  <p>NOTE: Although visible in the CLI, the no-tunnel-services statement is not supported on DPC cards at the [edit logical-systems <i>logical-system-name</i> protocols vpls static-vpls] and the [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls] hierarchy levels.</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"> • <i>Configuring VPLS Without a Tunnel Services PIC</i> • <i>Configuring Static Pseudowires for VPLS</i> • <i>Configuring EXP-Based Traffic Classification for VPLS</i>

maximum-lease-time

Syntax	<code>maximum-lease-time seconds;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family (inet inet6) dhcp-attributes], [edit access protocol-attributes <i>attribute-set-name</i>]
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">• <i>Configuring Address-Assignment Pools</i>• <i>DHCP Attributes for Address-Assignment Pools</i>• <i>preferred-lifetime (Address-Assignment Pools)</i>• <i>valid-lifetime (Address-Assignment Pools)</i>

overall-packet (Flat-File Accounting Options)

Syntax	<pre> overall-packet { all-fields; input-bytes; input-discards; input-errors; input-packets; inputv6-bytes; inputv6-packets; output-bytes; output-errors; output-packets; outputv6-bytes; outputv6-packets; } </pre>
Hierarchy Level	[edit accounting-options flat-file-profile <i>profile-name</i> fields]
Release Information	Statement introduced in Junos OS Release 16.1R4.
Description	Specify overall packet statistics to be collected for the interface.
Options	<p>all-fields—Collect all overall packet statistics available for the interface context, logical or physical.</p> <p>input-bytes—Collect the number of octets received on the interface.</p> <p>input-discards—(Physical interfaces only) Collect the number of received packets that were discarded on the interface.</p> <p>input-errors—(Physical interfaces only) Collect the number of frames with errors received on the interface.</p> <p>input-packets—Collect the number of packets received on the interface.</p> <p>input-v6-bytes—Collect the number of IPv6 octets received on the interface.</p> <p>input-v6-packets—Collect the number of IPv6 packets received on the interface.</p> <p>output-bytes—Collect the number of octets transmitted on the interface.</p> <p>output-errors—(Physical interfaces only) Collect the number of frames that could not be transmitted on the interface because of errors.</p> <p>output-packets—Collect the number of packets transmitted on the interface.</p> <p>output-v6-bytes—Collect the number of IPv6 octets transmitted on the interface.</p> <p>output-v6-packets—Collect the number of IPv6 packets transmitted on the interface.</p>

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- [Configuring Flat-File Accounting for Layer 2 Wholesale on page 181](#)
- [Configuring Flat-File Accounting for Extensible Subscriber Services Management on page 185](#)
- [Flat-File Accounting Overview on page 177](#)

output-vlan-map (Dynamic Interfaces)

Syntax

```
output-vlan-map {  
    inner-tag-protocol-id tpid;  
    inner-vlan-id number;  
    (pop | swap);  
    tag-protocol-id tpid;  
    vlan-id number;  
}
```

Hierarchy Level [edit [dynamic-profiles](#) *profile-name* [interfaces](#) *interface-name* [unit](#) *logical-unit-number*]

Release Information Statement introduced in Junos OS Release 10.4.

Description For dynamic interfaces, define the rewrite profile to be applied to outgoing frames on this logical interface.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- [Stacking and Rewriting VLAN Tags for the Layer 2 Wholesale Solution on page 80](#)

pap (Dynamic PPP)

Syntax	<code>pap;</code>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" ppp-options], [edit dynamic-profiles <i>profile-name</i> interfaces "\$junos-interface-ifd-name" unit "\$junos-interface-unit" ppp-options]
Release Information	Statement introduced in Junos OS Release 9.5. Support at the [edit dynamic-profiles <i>profile-name</i> interfaces "\$junos-interface-ifd-name" unit "\$junos-interface-unit" ppp-options] hierarchy level introduced in Junos OS Release 12.2.
Description	Specify PAP authentication in a PPP dynamic profile.
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"> • <i>Dynamic Profiles Overview</i> • <i>Configuring Dynamic Authentication for PPP Subscribers</i> • <i>Attaching Dynamic Profiles to Static PPP Subscriber Interfaces</i> • <i>Applying PPP Attributes to L2TP LNS Subscribers per Inline Service Interface</i>

pool (Address-Assignment Pools)

Syntax `pool pool-name {
 active-drain;
 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;
 }
 }
 hold-down;
 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. See [CLI Explorer](#).

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*
- *Configuring Address-Assignment Pools*

pool-match-order

Syntax	<pre>pool-match-order { external-authority; ip-address-first; option-82; }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server],</p> <p>[edit system services dhcp-local-server]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.0.</p> <p>Statement introduced in Junos OS Release 12.1.</p>
Description	<p>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.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Default	DHCP local server uses the ip-address-first method to determine which address pool to use.
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 How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use</i> • <i>Extended DHCP Local Server Overview</i>

pop (Dynamic VLANs)

Syntax	pop;
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	For dynamic VLAN interfaces, specify the VLAN rewrite operation to remove a VLAN tag from the top of the VLAN tag stack. The outer VLAN tag of the frame is removed.
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">• <i>Removing a VLAN Tag</i>• Stacking and Rewriting VLAN Tags for the Layer 2 Wholesale Solution on page 80

pppoe-options (Dynamic PPPoE)

Syntax	pppoe-options { underlying-interface <i>interface-name</i> ; server ; }
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit “\$junos-interface-unit”]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	Configure the underlying interface and PPPoE server mode for a dynamic PPPoE logical interface in a dynamic profile. The remaining statements are explained separately. See CLI Explorer .
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">• <i>Configuring a PPPoE Dynamic Profile</i>• <i>Configuring Dynamic PPPoE Subscriber Interfaces</i>

pppoe-underlying-options (Static and Dynamic Subscribers)

Syntax	<pre>pppoe-underlying-options { access-concentrator <i>name</i>; dynamic-profile <i>profile-name</i>; direct-connect duplicate-protection; max-sessions <i>number</i>; max-sessions-vsa-ignore; service-name-table <i>table-name</i>; short-cycle-protection <lockout-time-min <i>minimum-seconds</i>> <lockout-time-max <i>maximum-seconds</i>> <filter [<i>aci</i>]>; }</pre>
Hierarchy Level	<p>[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]</p>
Release Information	Statement introduced in Junos OS Release 10.0.
Description	<p>Configure PPPoE-specific interface properties for the underlying interface on which the router creates a static or dynamic PPPoE logical interface. The underlying interface must be configured with PPPoE (ppp-over-ether) encapsulation.</p> <p>The remaining statements are explained separately. See CLI Explorer.</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"> • <i>Configuring PPPoE</i> (for static interfaces) • <i>Configuring an Underlying Interface for Dynamic PPPoE Subscriber Interfaces</i> • <i>Assigning a Service Name Table to a PPPoE Underlying Interface</i>

ppp-options (Dynamic PPP)

Syntax	<pre>ppp-options { aaa-options <i>aaa-options-name</i>; authentication [<i>authentication-protocols</i>]; mru <i>size</i>; mtu (<i>size</i> use-lower-layer); chap { challenge-length minimum <i>minimum-length</i> maximum <i>maximum-length</i>; } initiate-ncp (ip ipv6 dual-stack-passive) ipcp-suggest-dns-option; mru <i>size</i>; mtu (<i>size</i> use-lower-layer); on-demand-ip-address; pap; peer-ip-address-optional; }</pre>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit"], [edit dynamic-profiles <i>profile-name</i> interfaces "\$junos-interface-ifd-name" unit "\$junos-interface-unit"]
Release Information	Statement introduced in Junos OS Release 9.5. Support at the [edit dynamic-profiles <i>profile-name</i> interfaces "\$junos-interface-ifd-name" unit "\$junos-interface-unit"] hierarchy level introduced in Junos OS Release 12.2.
Description	Configure PPP-specific interface properties in a dynamic profile. The remaining statements are explained separately. See CLI Explorer .
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">• <i>Dynamic Profiles Overview</i>• <i>Configuring Dynamic Authentication for PPP Subscribers</i>• <i>Attaching Dynamic Profiles to Static PPP Subscriber Interfaces</i>• <i>Applying PPP Attributes to L2TP LNS Subscribers per Inline Service Interface</i>

prefix (Address-Assignment Pools)

Syntax	<code>prefix <i>ipv6-prefix</i>;</code>
Hierarchy Level	[edit access address-assignment pool <i>pool-name</i> family inet6]
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">• <i>Address-Assignment Pools Overview</i>• <i>Configuring Address-Assignment Pools</i>

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-filter;`
 `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;`
 `}`
 `accounting-order (radius | [accounting-order-data-list]);`
 `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 number;`
 `maximum-sessions-per-tunnel number;`
 `multilink {`
 `drop-timeout milliseconds;`
 `fragment-threshold bytes;`
 `}`
 `override-result-code session-out-of-resource;`
 `ppp-authentication (chap | pap);`
 `ppp-profile profile-name;`
 `sessions-limit-group limit-group-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;
local {
  flat-file-profile profile-name;
}
preauthentication-order preauthentication-method;
provisioning-order (gx-plus | jsr | pcrf);
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;
    interface-text-description;
    mac-address;
    nas-identifier;
    stacked-vlan;
    vlan;
  }
  chap-challenge-in-request-authenticator;
  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-channel;
    exclude-sub-interface;
  }
  juniper-dsl-attributes;
  nas-identifier identifier-value;
  nas-port-extended-format {
    adapter-width width;
    ae-width width;
    port-width width;
    pw-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;
    interface-text-description;
    nas-identifier;
    order {
      agent-circuit-id;
      agent-remote-id;
      interface-description;
      interface-text-description;
      nas-identifier;
      postpend-vlan-tags;
    }
    postpend-vlan-tags;
  }
  nas-port-type {
    ethernet {
      port-type;
    }
  }
  revert-interval interval;
  service-activation {
    dynamic-profile (optional-at-login | required-at-login);
    extensible-service (optional-at-login | required-at-login);
  }
  vlan-nas-port-stacked-format;
}
preauthentication-server ip-address;
}
radius-server server-address {
  accounting-port port-number;
  accounting-retry number;
```



```

accounting-timeout seconds;
dynamic-request-port
port port-number;
preauthentication-port port-number;
preauthentication-secret password;
retry attempts;
routing-instance routing-instance-name;
secret password;
max-outstanding-requests value;
source-address source-address;
timeout seconds;
}
service {
  accounting {
    statistics (time | volume-time);
    update-interval minutes;
  }
  accounting-order (activation-protocol | local | radius);
}
session-options {
  client-idle-timeout minutes;
  client-idle-timeout-ingress-only;
  client-session-timeout minutes;
  strip-user-name {
    delimiter [ delimiter ];
    parse-direction (left-to-right | right-to-left);
  }
}
}

```

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. See [CLI Explorer](#).

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

**Related
Documentation**

- *Configuring the PPP Authentication Protocol*
- *Configuring Access Profiles for L2TP or PPP Parameters*
- *Configuring L2TP Properties for a Client-Specific Profile*
- *Configuring an L2TP LNS with Inline Service Interfaces*
- *Configuring PPP Properties for a Client-Specific Profile*
- *Configuring Service Accounting with JSRC*
- [Configuring Service Accounting in Local Flat Files on page 189](#)
- *AAA Service Framework Overview*
- [show network-access aaa statistics on page 578](#)
- *clear network-access aaa statistics*

protocols

```

Syntax protocols {
    bgp {
        ... bgp-configuration ...
    }
    isis {
        ... isis-configuration ...
    }
    ldp {
        ... ldp-configuration ...
    }
    mpls {
        ... mpls-configuration ...
    }
    msdp {
        ... msdp-configuration ...
    }
    mstp {
        ... mstp-configuration ...
    }
    ospf {
        domain-id domain-id;
        domain-vpn-tag number;
        route-type-community (iana | vendor);
        traffic-engineering {
            <advertise-unnumbered-interfaces>;
            <credibility-protocol-preference>;
            ignore-lsp-metrics;
            multicast-rpf-routes;
            no-topology;
            shortcuts {
                lsp-metric-into-summary;
            }
        }
        ... ospf-configuration ...
    }
    ospf3 {
        domain-id domain-id;
        domain-vpn-tag number;
        route-type-community (iana | vendor);
        traffic-engineering {
            <advertise-unnumbered-interfaces>;
            <credibility-protocol-preference>;
            ignore-lsp-metrics;
            multicast-rpf-routes;
            no-topology;
            shortcuts {
                lsp-metric-into-summary;
            }
        }
        ... ospf3-configuration ...
    }
    pim {

```

```
    ... pim-configuration ...  
  }  
  rip {  
    ... rip-configuration ...  
  }  
  ripng {  
    ... ripng-configuration ...  
  }  
  rstp {  
    rstp-configuration;  
  }  
  rsvp {  
    ... rsvp-configuration ...  
  }  
  vstp {  
    vstp configuration;  
  }  
  vpls {  
    vpls configuration;  
  }  
}
```

Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>], [edit routing-instances <i>routing-instance-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Support for RIPng introduced in Junos OS Release 9.0. Statement introduced in Junos OS Release 11.1 for EX Series switches. Statement introduced in Junos OS Release 11.3 for the QFX Series. mpls and rsvp options added in Junos OS Release 15.1. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Specify the protocol for a routing instance. You can configure multiple instances of many protocol types. Not all protocols are supported on the switches. See the switch CLI.

- Options**
- bgp**—Specify BGP as the protocol for a routing instance.
 - isis**—Specify IS-IS as the protocol for a routing instance.
 - ldp**—Specify LDP as the protocol for a routing instance or for a virtual router instance.
 - l2vpn**—Specify Layer 2 VPN as the protocol for a routing instance.
 - mpls**—Specify MPLS as the protocol for a routing instance.
 - msdp**—Specify the Multicast Source Discovery Protocol (MSDP) for a routing instance.
 - mstp**—Specify the Multiple Spanning Tree Protocol (MSTP) for a virtual switch routing instance.
 - ospf**—Specify OSPF as the protocol for a routing instance.
 - ospf3**—Specify OSPF version 3 (OSPFv3) as the protocol for a routing instance.



NOTE: OSPFv3 supports the **no-forwarding**, **virtual-router**, and **vrf** routing instance types only.

- pim**—Specify the Protocol Independent Multicast (PIM) protocol for a routing instance.
- rip**—Specify RIP as the protocol for a routing instance.
- ripng**—Specify RIP next generation (RIPng) as the protocol for a routing instance.
- rstp**—Specify the Rapid Spanning Tree Protocol (RSTP) for a virtual switch routing instance.
- rsvp**—Specify the RSVP for a routing instance.
- vstp**—Specify the VLAN Spanning Tree Protocol (VSTP) for a virtual switch routing instance.
- vpls**—Specify VPLS as the protocol for a routing instance.


Required Privilege Level

- routing—To view this statement in the configuration.
- routing-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring Multiple Routing Instances of OSPF*

proxy-arp

Syntax	proxy-arp (restricted unrestricted);
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.6 for EX Series switches. restricted added in Junos OS Release 10.0 for EX Series switches. Statement introduced in Junos OS Release 12.2 for the QFX Series.
Description	For Ethernet interfaces only, configure the router or switch to respond to any ARP request, as long as the router or switch has an active route to the ARP request's target address.
<div> NOTE: You must configure the IP address and the inet family for the interface when you enable proxy ARP.</div>	
Default	Proxy ARP is not enabled. The router or switch responds to an ARP request only if the destination IP address is its own.
Options	<ul style="list-style-type: none">• none—The router or switch responds to any ARP request for a local or remote address if the router or switch has a route to the target IP address.• restricted—(Optional) The router or switch responds to ARP requests in which the physical networks of the source and target are different and does not respond if the source and target IP addresses are in the same subnet. The router or switch must also have a route to the target IP address.• unrestricted—(Optional) The router or switch responds to any ARP request for a local or remote address if the router or switch has a route to the target IP address. <p>Default: unrestricted</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">• <i>Configuring Restricted and Unrestricted Proxy ARP</i>• <i>Configuring Proxy ARP (CLI Procedure)</i>• <i>Example: Configuring Proxy ARP on an EX Series Switch</i>• <i>Configuring Gratuitous ARP</i>


proxy-arp (Dynamic Profiles)

Syntax	proxy-arp;
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]
Release Information	Statement introduced in Junos OS Release 9.5.
Description	For Ethernet interfaces only, configure the router to respond to any ARP request, as long as the router has an active route to the target address of the ARP request.
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"> • <i>Configuring Restricted and Unrestricted Proxy ARP</i> • <i>Configuring Gratuitous ARP</i>

push (Dynamic VLANs)

Syntax	push;
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> input-vlan-map]
Release Information	Statement introduced in Junos OS Release 10.4.
Description	For dynamic VLAN interfaces, specify the VLAN rewrite operation to add a new VLAN tag to the top of the VLAN stack. An outer VLAN tag is pushed in front of the existing VLAN tag. If you include the push statement in the configuration, you must also include the <i>pop</i> statement at the [edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> output-vlan-map] hierarchy level.
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"> • <i>Stacking and Rewriting VLAN Tags for the Layer 2 Wholesale Solution on page 80</i>

push-backup-to-master (Accounting Options)

Syntax	<code>push-backup-to-master;</code>
Hierarchy Level	<code>[edit accounting-options <i>file filename</i>]</code>
Release Information	Statement introduced in Junos OS Release 16.1R4.
Description	<p>Configure the router to save the accounting files from the new backup Routing Engine to the new master Routing Engine when a change in mastership occurs. The files are saved to the <code>/var/log/pfedBackup</code> directory on the router. The master Routing Engine includes these accounting files with its own current accounting files when it transfers the files from the backup directory to the archive site at the next transfer interval. Use this statement when the new backup Routing Engine is not able to connect to the archive site; for example, when site is not connected by means of an out-of-band interface or the path to the site is routed through a line card.</p> <div> NOTE: The backup Routing Engine's files on the master Routing Engine are sent at each interval even though the files remain the same. If this is more activity than you want, consider using the <code>backup-on-failure master-and-slave</code> statement instead.</div>
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 Accounting-Data Log Files• Configuring Flat-File Accounting for Layer 2 Wholesale on page 181• Configuring Flat-File Accounting for Extensible Subscriber Services Management on page 185• Flat-File Accounting Overview on page 177

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;
    }
    chap-challenge-in-request-authenticator;
    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-channel;
        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;
  interface-text-description;
  nas-identifier;
  order {
    agent-circuit-id;
    agent-remote-id;
    interface-description;
    interface-text-description;
    nas-identifier;
    postpend-vlan-tags;
  }
  postpend-vlan-tags;
}
nas-port-type {
  ethernet {
    port-type;
  }
}
revert-interval interval;
service-activation {
  dynamic-profile (optional-at-login | required-at-login);
  extensible-service (optional-at-login | required-at-login);
}
vlan-nas-port-stacked-format;
}
preauthentication-server ip-address;
}
```

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.
Description	Configure the RADIUS parameters that the router uses for AAA authentication and accounting for subscribers. The remaining statements are explained separately. See CLI Explorer .
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>Configuring RADIUS Server Parameters for Subscriber Access</i>• <i>RADIUS Server Options for Subscriber Access</i>

radius-server

Syntax	<pre>radius-server server-address { accounting-port port-number; accounting-retry number; accounting-timeout seconds; dynamic-request-port max-outstanding-requests value; port port-number; preauthentication-port port-number; preauthentication-secret password; retry attempts; routing-instance routing-instance-name; secret password; 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> <p>dynamic-request-port option added in Junos OS Release 14.2 for MX Series routers.</p> <p>preauthentication-port and preauthentication-secret options added in Junos OS Release 15.1 for MX Series routers.</p> <p>Support for IPv6 server-address introduced in Junos OS Release 16.1.</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—IPv4 or IPv6 address of the RADIUS server.</p> <p>The remaining statements are explained separately. See CLI Explorer.</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 Router or Switch Interaction with RADIUS Servers</i> • <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i> • show network-access aaa statistics on page 578

- *clear network-access aaa statistics*


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>range-name—Name assigned to the range of IPv4 addresses or IPv6 prefixes.</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">• <i>Address-Assignment Pools Overview</i>• <i>Configuring Address-Assignment Pools</i>

ranges (Dynamic VLAN)

Syntax	<code>ranges (any <i>low-tag</i>)-(any <i>high-tag</i>);</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> auto-configure vlan-ranges dynamic-profile <i>profile-name</i>]
Release Information	Statement introduced in Junos OS Release 9.5.
Description	Configure VLAN ranges for dynamic, auto-sensed VLANs.
Options	<p>any—The entire VLAN range.</p> <p><i>low-tag</i>—The lower limit of the VLAN range.</p> <p><i>high-tag</i>—The upper limit of the VLAN range.</p> <p>Range: 1 through 4094</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"> • <i>Configuring an Interface to Use the Dynamic Profile Configured to Create Single-Tag VLANs</i>

remote-id (VLAN Authentication Username)

Syntax	remote-id;
Hierarchy Level	[edit interfaces <i>interface-name</i> auto-configure vlan-ranges authentication username-include]
Release Information	Statement introduced in Junos OS Release 16.1R4.
Description	Include the agent remote identifier (ARI) in the username sent to RADIUS for authentication of the dynamic VLAN. The ARI is conveyed by the Access-Loop-Remote-ID TLV in an out-of-band ANCP Port Up message.
<div> NOTE: This statement is not supported for stacked VLANs.</div>	
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 a Username for Authentication of Out-of-Band Triggered Dynamic VLANs on page 168• <i>Configuring VLAN Interface Username Information for AAA Authentication</i>• Layer 2 Wholesale with ANCP-Triggered VLANs Overview on page 99

route-distinguisher

Syntax	<code>route-distinguisher (as-number:id ip-address:id);</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn mesh-group <i>mesh-group-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i>], [edit routing-instances <i>routing-instance-name</i>], [edit routing-instances <i>routing-instance-name</i> protocols l2vpn mesh-group <i>mesh-group-name</i>], [edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i>]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 11.1 for EX Series switches.</p> <p>Support at [edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i>] hierarchy level introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 12.3 for ACX Series routers.</p> <p>Support at [edit routing-instances <i>routing-instance-name</i> protocols l2vpn mesh-group <i>mesh-group-name</i>] hierarchy level introduced in Junos OS Release 13.2.</p> <p>Statement introduced in Junos OS Release 14.1X53-D30 for QFX Series switches.</p>
Description	<p>Specify an identifier attached to a route, enabling you to distinguish to which VPN or virtual private LAN service (VPLS) the route belongs. Each routing instance must have a unique route distinguisher (RD) associated with it. The RD is used to place bounds around a VPN so that the same IP address prefixes can be used in different VPNs without having them overlap. If the instance type is vrf, the route-distinguisher statement is required.</p> <p>For Layer 2 VPNs and VPLS, if you configure the l2vpn-use-bgp-rules statement, you must configure a unique RD for each PE router participating in the routing instance.</p> <p>For other types of VPNs, we recommend that you use a unique RD for each provider edge (PE) router participating in specific routing instance. Although you can use the same RD on all PE routers for the same VPN routing instance, if you use a unique RD, you can determine the customer edge (CE) router from which a route originated within the VPN.</p> <p>For Layer 2 VPNs and VPLSs, if you configure mesh groups, the RD in each mesh group must be unique.</p>



CAUTION: We strongly recommend that if you change an RD that has already been configured, make the change during a maintenance window, as follows:

1. Deactivate the routing instance.
2. Change the RD.
3. Activate the routing instance.

This is not required if you are configuring the RD for the first time.

Options *as-number:number—***as-number** is an assigned AS number, and **number** is any 2-byte or 4-byte value. The AS number can be from 1 through 4,294,967,295. If the AS number is a 2-byte value, the administrative number is a 4-byte value. If the AS number is a 4-byte value, the administrative number is a 2-byte value. An RD consisting of a 4-byte AS number and a 2-byte administrative number is defined as a type 2 RD in RFC 4364 *BGP/MPLS IP VPNs*.



NOTE: In Junos OS Release 9.1 and later, the numeric range for AS numbers is extended to provide BGP support for 4-byte AS numbers, as defined in RFC 4893, *BGP Support for Four-octet AS Number Space*. All releases of Junos OS support 2-byte AS numbers. To configure an RD that includes a 4-byte AS number, append the letter “L” to the end of the AS number. For example, an RD with the 4-byte AS number 7,765,000 and an administrative number of 1,000 is represented as 77765000L:1000.

In Junos OS Release 9.2 and later, you can also configure a 4-byte AS number using the AS dot notation format of two integer values joined by a period: *<16-bit high-order value in decimal>.<16-bit low-order value in decimal>*. For example, the 4-byte AS number of 65,546 in the plain-number format is represented as 1.10 in AS dot notation format.

ip-address:id—IP address (*ip-address* is a 4-byte value) within your assigned prefix range and a 2-byte value for the *id*. The IP address can be any globally unique unicast address.

Range: 0 through 4,294,967,295 ($2^{32} - 1$). If the router you are configuring is a BGP peer of a router that does not support 4-byte AS numbers, you need to configure a local AS number. For more information, see *Using 4-Byte Autonomous System Numbers in BGP Networks Technology Overview*.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring BGP Route Target Filtering for VPNs*
- *Example: Configuring FEC 129 BGP Autodiscovery for VPWS*
- *Configuring EVPN Routing Instances*
- *Configuring Routing Instances on PE Routers in VPNs*
- *Configuring an MPLS-Based Layer 2 VPN (CLI Procedure)*
- *Configuring an MPLS-Based Layer 3 VPN (CLI Procedure)*
- *l2vpn-use-bgp-rules*

routing-instances (Dynamic Profiles)

```
Syntax  routing-instances routing-instance-name {
        interface interface-name;
        multicast-snooping-options {
        }
        routing-options {
            access {
                route prefix {
                    metric route-cost;
                    next-hop next-hop;
                    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 {
                    metric route-cost;
                    next-hop next-hop;
                    preference route-distance;
                    tag route-tag;
                }
            }
            access-internal {
                route subscriber-ip-address {
                    qualified-next-hop underlying-interface {
                        mac-address address;
                    }
                }
            }
        }
    }
```

Hierarchy Level [edit [dynamic-profiles](#)]
 [edit logical-systems *logical-system-name*]

Release Information Statement introduced in Junos OS Release 9.6.
 Support at the **logical-systems** hierarchy level was introduced in Junos OS Release 14.2.

Description	Dynamically configure an additional routing entity for a router.
Options	<p><i>routing-instance-name</i>—The routing instance variable (<i>\$junos-routing-instance</i>). The routing instance variable is dynamically replaced with the routing instance the accessing client uses when connecting to the router.</p> <p>The remaining statements are explained separately. See CLI Explorer.</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 a Dynamic Profile for use by a Retailer in the DHCPv4 Solution on page 20

routing-instances (Multiple Routing Entities)

Syntax	<code>routing-instances <i>routing-instance-name</i> { ... }</code>
Hierarchy Level	<code>[edit],</code> <code>[edit logical-systems <i>logical-system-name</i>]</code>
Release Information	Statement introduced before Junos OS Release 7.4.
Description	<p>Configure an additional routing entity for a router. You can create multiple instances of BGP, IS-IS, OSPF, OSPFv3, and RIP for a router. You can also create multiple routing instances for separating routing tables, routing policies, and interfaces for individual wholesale subscribers (retailers) in a Layer 3 wholesale network.</p> <p>Each routing instance consist of the following:</p> <ul style="list-style-type: none"> • A set of routing tables • A set of interfaces that belong to these routing tables • A set of routing option configurations <p>Each routing instance has a unique name and a corresponding IP unicast table. For example, if you configure a routing instance with the name my-instance, its corresponding IP unicast table is <code>my-instance.inet.0</code>. All routes for my-instance are installed into <code>my-instance.inet.0</code>.</p> <p>Routes are installed into the default routing instance <code>inet.0</code> by default, unless a routing instance is specified.</p> <p>In Junos OS Release 9.0 and later, you can no longer specify a routing-instance name of <i>master</i>, <i>default</i>, or <i>bgp</i> or include special characters within the name of a routing instance.</p> <p>In Junos OS Release 9.6 and later, you can include a slash (/) in a routing-instance name only if a logical system is not configured. That is, you cannot include the slash character in a routing-instance name if a logical system other than the default is explicitly configured. Routing-instance names, further, are restricted from having the form <code>__.*__</code> (beginning and ending with underscores). The colon : character cannot be used when multiprotocol routing (MTR) is enabled.</p>
Default	Routing instances are disabled for the router.
Options	<i>routing-instance-name</i> —Name of the routing instance. This must be a non-reserved string of not more than 128 characters.
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**
- *Example: Configuring Interprovider Layer 3 VPN Option A*
 - *Example: Configuring Interprovider Layer 3 VPN Option B*
 - *Example: Configuring Interprovider Layer 3 VPN Option C*

schema-version (Flat-File Accounting Options)

- Syntax** `schema-version schema-name;`
- Hierarchy Level** [edit accounting-options **flat-file-profile** *profile-name*]
- Release Information** Statement introduced in Junos OS Release 16.1R4.
- Description** Specify the name of the XML schema that defines the contents and format of the accounting file, and appears in the accounting record header.
- Options** ***schema-name***—Name of the schema.
- Required Privilege Level** system—To view this statement in the configuration.
system-control—To add this statement to the configuration.
- Related Documentation**
- [Configuring Flat-File Accounting for Layer 2 Wholesale on page 181](#)
 - [Configuring Flat-File Accounting for Extensible Subscriber Services Management on page 185](#)
 - [Flat-File Accounting Overview on page 177](#)

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"> • <i>Configuring Authentication and Accounting Parameters for Subscriber Access</i> • <i>Configuring Router or Switch Interaction with RADIUS Servers</i> • <i>Example: Configuring CHAP Authentication with RADIUS</i> • <i>Configuring RADIUS Authentication for L2TP</i> • <i>Configuring the RADIUS Disconnect Server for L2TP</i>

server (Dynamic PPPoE)

Syntax	server;
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" pppoe-options]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	In a dynamic profile, configure the router to act as a PPPoE server, also known as a remote access concentrator, when a PPPoE logical interface is dynamically created.
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">• <i>Configuring a PPPoE Dynamic Profile</i>• <i>Subscriber Interfaces and PPPoE Overview</i>

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>server-group-name—Name of the group of DHCP or DHCPv6 server addresses.</p> <p>server-ip-address—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 239 • <i>Extended DHCP Relay Agent Overview</i> • <i>Configuring Named Server Groups</i>

site (VPLS Multihoming for FEC 128)

Syntax	<pre>site <i>site-name</i> { mac-pinning; active-interface (any primary <i>interface-name</i>); best-site; interface <i>interface-name</i> { interface-mac-limit <i>limit</i>; } mesh-group <i>mesh-group-name</i>; multi-homing; site-identifier <i>identifier</i>; site-preference <i>preference-value</i>; }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls], [edit routing-instances <i>routing-instance-name</i> protocols vpls]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the site name and site identifier for a site. Allows you to configure a remote site ID for remote sites.
Options	<p><i>site-name</i>—Name of the site.</p> <p>The remaining statements are explained separately. See CLI Explorer.</p>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.

site-identifier (VPLS)

Syntax	site-identifier <i>identifier</i> ;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls site <i>site-name</i>], [edit routing-instances <i>routing-instance-name</i> protocols vpls site <i>site-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify the numerical identifier for the local VPLS site.
Options	<i>identifier</i> —Specify the numerical identifier for the local VPLS site. The identifier must be an unsigned 16-bit number greater than zero.
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>Configuring VPLS Routing Instances</i>

site-range

Syntax	<code>site-range <i>number</i>;</code>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls], [edit routing-instances <i>routing-instance-name</i> protocols vpls]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Specify an upper limit on the maximum site identifier that can be accepted to allow a pseudowire to be brought up. Pseudowires cannot be established to sites with site identifiers greater than the configured site range. If you issue the show vpls connections command, such sites are displayed as OR (out of range).
Options	<i>number</i> —Maximum number of site identifiers. We recommend using the default value. Range: 1 through 65,534 Default: 65,534
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>Configuring VPLS Routing Instances</i>

stacked-vlan-ranges

```
Syntax  stacked-vlan-ranges {
        access-profile profile-name;
        authentication {
            packet-types [packet-types];
            password password-string;
            username-include {
                circuit-type;
                delimiter delimiter-character;
                domain-name domain-name-string;
                interface-name;
                mac-address;
                option-18
                option-37
                option-82;
                radius-realm radius-realm-string;
                user-prefix user-prefix-string;
            }
        }
        dynamic-profile profile-name {
            accept (any | dhcp-v4 | inet);
            access-profile vlan-dynamic-profile-name;
            ranges (any | low-tag-high-tag), (any | low-tag-high-tag);
        }
        override;
    }
```

Hierarchy Level [edit interfaces *interface-name* **auto-configure**]

Release Information Statement introduced in Junos OS Release 9.5.

Description Configure multiple VLANs. Each VLAN is assigned a VLAN ID number from the range.

The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Configuring an Interface to Use the Dynamic Profile Configured to Create Stacked VLANs*
- *Configuring Interfaces to Support Both Single and Stacked VLANs*

stacked-vlan-tagging

Syntax	stacked-vlan-tagging;
Hierarchy Level	[edit interfaces <i>interface-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.2 for ACX Series Universal Access Routers.
Description	<p>For Gigabit Ethernet IQ interfaces, Gigabit Ethernet, 10-Gigabit Ethernet LAN/WAN PIC, and 100-Gigabit Ethernet Type 5 PIC with CFP, enable stacked VLAN tagging for all logical interfaces on the physical interface.</p> <p>For pseudowire subscriber interfaces, enable stacked VLAN tagging for logical interfaces on the pseudowire service.</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">• <i>Stacking and Rewriting Gigabit Ethernet VLAN Tags Overview</i>• vlan-tags (Stacked VLAN Tags) on page 410

system

Syntax	system { ... }
Hierarchy Level	[edit]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure system management properties.
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>System Management Configuration Statements</i>

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	<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>Define global tracing operations for extended DHCP local server and extended DHCP relay agent processes.</p> <p>This statement replaces the 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 Level trace—To view this statement in the configuration.
 trace-control—To add this statement to the configuration.

Related Documentation • *Tracing Extended DHCP Operations*

underlying-interface (demux0)

Syntax `underlying-interface underlying-interface-name;`

Hierarchy Level [edit [dynamic-profiles](#) *profile-name* [interfaces](#) [demux0](#) *interface-name* [unit](#) *unit logical-unit-number* [demux-options](#)]

Release Information Statement introduced in Junos OS Release 9.3.
 Support for aggregated Ethernet introduced in Junos OS Release 9.4.

Description Configure the underlying interface on which the demultiplexing (demux) interface is running.

Options *underlying-interface-name*—Either the specific name of the interface on which the DHCP discover packet arrives or one of the following interface variables:

- `$junos-underlying-interface` when configuring dynamic IP demux interfaces.
- `$junos-interface-ifd-name` when configuring dynamic VLAN demux interfaces.

The variable is used to specify the underlying interface when a new demux interface is dynamically created. The variable is dynamically replaced with the underlying interface that DHCP supplies when the subscriber logs in.



NOTE: Logical demux interfaces are currently supported on Gigabit Ethernet, Fast Ethernet, 10-Gigabit Ethernet, or aggregated Ethernet interfaces.

Required Privilege Level interface—To view this statement in the configuration.
 interface-control—To add this statement to the configuration.

Related Documentation • *Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles*
 • *Configuring Dynamic Subscriber Interfaces Using VLAN Demux Interfaces in Dynamic Profiles*
 • *Dynamic PPPoE Subscriber Interfaces over Static Underlying Interfaces Overview*
 • For information about static underlying interfaces, see the *Junos OS Network Interfaces Library for Routing Devices*

underlying-interface (Dynamic PPPoE)

Syntax	<code>underlying-interface <i>interface-name</i>;</code>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" ppoe-options]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	In a dynamic profile, configure the underlying interface on which the router creates the dynamic PPPoE logical interface.
Options	<i>interface-name</i> —Variable used to specify the name of the underlying interface on which the PPPoE logical interface is dynamically created. In the underlying-interface <i>interface-name</i> statement for dynamic PPPoE logical interfaces, you must use the predefined variable \$junos-underlying-interface in place of <i>interface-name</i> . When the router creates the dynamic PPPoE interface, the \$junos-underlying-interface predefined variable is dynamically replaced with the name of the underlying interface supplied by the network when the subscriber logs in.
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">• <i>Configuring a PPPoE Dynamic Profile</i>• <i>Dynamic PPPoE Subscriber Interfaces over Static Underlying Interfaces Overview</i>

unit

```

Syntax  unit logical-unit-number {
        accept-source-mac {
            mac-address mac-address {
                policer {
                    input cos-policer-name;
                    output cos-policer-name;
                }
            }
        }
        accounting-profile name;
        advisory-options {
            downstream-rate rate;
            upstream-rate rate;
        }
        allow-any-vci;
        atm-scheduler-map (map-name | default);
        auto-configure {
            agent-circuit-identifier {
                dynamic-profile profile-name;
            }
            line-identity {
                include {
                    accept-no-ids;
                    circuit-id;
                    remote-id;
                }
                dynamic-profile profile-name;
            }
        }
        backup-options {
            interface interface-name;
        }
        bandwidth rate;
        cell-bundle-size cells;
        clear-dont-fragment-bit;
        compression {
            rtp {
                maximum-contexts number <force>;
                f-max-period number;
                queues [queue-numbers];
                port {
                    minimum port-number;
                    maximum port-number;
                }
            }
        }
        compression-device interface-name;
        copy-tos-to-outer-ip-header;
        demux-destination family;
        demux-source family;
        demux-options {
            underlying-interface interface-name;

```

```

}
description text;
etree-ac-role (leaf | root);
interface {
    l2tp-interface-id name;
    (dedicated | shared);
}
dialer-options {
    activation-delay seconds;
    callback;
    callback-wait-period time;
    deactivation-delay seconds;
    dial-string [dial-string-numbers];
    idle-timeout seconds;
    incoming-map {
        caller caller-id | accept-all;
        initial-route-check seconds;
        load-interval seconds;
        load-threshold percent;
        pool pool-name;
        redial-delay time;
        watch-list {
            [routes];
        }
    }
}
disable;
disable-mlppp-inner-ppp-pfc;
dlci dlci-identifier;
drop-timeout milliseconds;
dynamic-call-admission-control {
    activation-priority priority;
    bearer-bandwidth-limit kilobits-per-second;
}
encapsulation type;
epd-threshold cells plp1 cells;
family family-name {
    ... the family subhierarchy appears after the main [edit interfaces interface-name unit
        logical-unit-number] hierarchy ...
}
fragment-threshold bytes;
host-prefix-only;
inner-vlan-id-range start start-id end end-id;
input-vlan-map {
    (pop | pop-pop | pop-swap | push | push-push | swap |
    swap-push | swap-swap);
    inner-tag-protocol-id tpid;
    inner-vlan-id number;
    tag-protocol-id tpid;
    vlan-id number;
}
interleave-fragments;
inverse-arp;
layer2-policer {
    input-policer policer-name;
    input-three-color policer-name;
}

```

```

    output-policer policer-name;
    output-three-color policer-name;
}
link-layer-overhead percent;
minimum-links number;
mrru bytes;
multicast-dlci dlci-identifier;
multicast-vci vpi-identifier.vci-identifier;
multilink-max-classes number;
multipoint;
oam-liveness {
    up-count cells;
    down-count cells;
}
oam-period (disable | seconds);
output-vlan-map {
    (pop | pop-pop | pop-swap | push | push-push | swap |
    swap-push | swap-swap);
    inner-tag-protocol-id tpid;
    inner-vlan-id number;
    tag-protocol-id tpid;
    vlan-id number;
}
passive-monitor-mode;
peer-unit unit-number;
plp-to-clp;
point-to-point;
ppp-options {
    mru size;
    mtu (size | use-lower-layer);
    chap {
        access-profile name;
        default-chap-secret name;
        local-name name;
        passive;
    }
    compression {
        acfc;
        pfc;
    }
    dynamic-profile profile-name;
    ipcp-suggest-dns-option;
    lcp-restart-timer milliseconds;
    loopback-clear-timer seconds;
    ncp-restart-timer milliseconds;
    pap {
        access-profile name;
        default-pap-password password;
        local-name name;
        local-password password;
        passive;
    }
}
}
pppoe-options {
    access-concentrator name;
    auto-reconnect seconds;

```

```
(client | server);
service-name name;
underlying-interface interface-name;
}
pppoe-underlying-options {
    access-concentrator name;
    direct-connect;
    dynamic-profile profile-name;
    max-sessions number;
}
proxy-arp;
service-domain (inside | outside);
shaping {
    (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst
    length);
    queue-length number;
}
short-sequence;
targeted-distribution;
transmit-weight number;
(traps | no-traps);
trunk-bandwidth rate;
trunk-id number;
tunnel {
    backup-destination address;
    destination address;
    key number;
    routing-instance {
        destination routing-instance-name;
    }
    source source-address;
    ttl number;
}
vci vpi-identifier.vci-identifier;
vci-range start start-vci end end-vci;
vpi vpi-identifier;
vlan-id number;
vlan-id-range number-number;
vlan-tags inner tpid.vlan-id outer tpid.vlan-id;
family family {
    accounting {
        destination-class-usage;
        source-class-usage {
            (input | output | input output);
        }
    }
}
access-concentrator name;
address address {
    ... the address subhierarchy appears after the main [edit interfaces interface-name unit
    logical-unit-number family family-name] hierarchy ...
}
bundle interface-name;
core-facing;
demux-destination {
    destination-prefix;
}
```

```

demux-source {
    source-prefix;
}
direct-connect;
duplicate-protection;
dynamic-profile profile-name;
filter {
    group filter-group-number;
    input filter-name;
    input-list [filter-names];
    output filter-name;
    output-list [filter-names];
}
interface-mode (access | trunk);
ipsec-sa sa-name;
keep-address-and-control;
mac-validate (loose | strict);
max-sessions number;
mtu bytes;
multicast-only;
no-redirects;
policer {
    arp policer-template-name;
    input policer-template-name;
    output policer-template-name;
}
primary;
protocols [inet iso mpls];
proxy inet-address address;
receive-options-packets;
receive-ttl-exceeded;
remote (inet-address address | mac-address address);
rpf-check {
    fail-filter filter-name
    mode loose;
}
sampling {
    input;
    output;
}
service {
    input {
        post-service-filter filter-name;
        service-set service-set-name <service-filter filter-name>;
    }
    output {
        service-set service-set-name <service-filter filter-name>;
    }
}
service-name-table table-name
(translate-discard-eligible | no-translate-discard-eligible);
(translate-fecn-and-becn | no-translate-fecn-and-becn);
translate-plp-control-word-de;
unnumbered-address interface-name destination address destination-profile profile-name;
vlan-id number;
vlan-id-list [number number-number];

```

```

address address {
  arp ip-address (mac | multicast-mac) mac-address <publish>;
  broadcast address;
  destination address;
  destination-profile name;
  eui-64;
  master-only;
  multipoint-destination address {
    dlcid dlcid-identifier;
    epd-threshold cells <plp1 cells>;
    inverse-arp;
    oam-liveness {
      up-count cells;
      down-count cells;
    }
    oam-period (disable | seconds);
    shaping {
      (cbr rate | rtvbr burst length peak rate sustained rate | vbr burst length peak rate
        sustained rate);
      queue-length number;
    }
    vci vpi-identifier.vci-identifier;
  }
  preferred;
  primary;
  (vrrp-group | vrrp-inet6-group) group-number {
    (accept-data | no-accept-data);
    advertise-interval seconds;
    authentication-type authentication;
    authentication-key key;
    fast-interval milliseconds;
    (preempt | no-preempt) {
      hold-time seconds;
    }
    priority number;
    track {
      interface interface-name {
        bandwidth-threshold bits-per-second priority-cost number;
      }
      priority-hold-time seconds;
      route ip-address/prefix-length routing-instance instance-name priority-cost cost;
    }
    virtual-address [addresses];
    virtual-link-local-address ipv6-address;
    vrrp-inherit-from {
      active-interface interface-name;
      active-group group-number;
    }
  }
}
}
}

```

Hierarchy Level	[edit interfaces <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i>], [edit interfaces interface-set <i>interface-set-name</i> interface <i>interface-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.
Options	<p><i>logical-unit-number</i>—Number of the logical unit.</p> <p>Range: 0 through 1,073,741,823 for demux and PPPoE static interfaces. 0 through 16,385 for all other static interface types.</p> <p>etree-ac-role (leaf root)—To configure an interface as either leaf or root.</p> <p>The remaining statements are explained separately. See CLI Explorer.</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">• <i>Configuring Logical Interface Properties</i>• <i>Example: Configuring E-LINE and E-LAN Services for a PBB Network on MX Series Routers</i>• <i>Junos OS Services Interfaces Library for Routing Devices</i>

unit (Dynamic Demux Interface)

Syntax `unit logical-unit-number {
 demux-options {
 underlying-interface interface-name
 }
 family family {
 access-concentrator name;
 address address;
 demux-source {
 source-address;
 }
 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;
 rpf-check {
 fail-filter filter-name;
 mode loose;
 }
 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>;
 }
 filter {
 input filter-name;
 output filter-name;
 }
}
vlan-id number;`

Hierarchy Level [edit [dynamic-profiles profile-name interfaces demux0](#)]

Release Information Statement introduced in Junos OS Release 9.3.

Description Configure a dynamic logical interface on the physical device. You must configure a logical interface to be able to use the physical device.

Options *logical-unit-number*—Either the specific unit number of the interface or the unit number variable (*\$junos-interface-unit*). The variable is used to specify the unit of the interface when a new demux interface is dynamically created. The static unit number variable is dynamically replaced with the unit number that DHCP supplies when the subscriber logs in.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege interface—To view this statement in the configuration.

Level interface-control—To add this statement to the configuration.

Related Documentation

- *Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles*

unit (Dynamic Profiles Standard Interface)

```

Syntax  unit logical-unit-number {
        auto-configure {
            agent-circuit-identifier {
                dynamic-profile profile-name;
            }
            line-identity {
                include {
                    accept-no-ids;
                    circuit-id;
                    remote-id;
                }
                dynamic-profile profile-name;
            }
        }
        dial-options {
            ipsec-interface-id name;
            l2tp-interface-id name;
            (shared | dedicated);
        }
        encapsulation (atm-ccc-cell-relay | atm-ccc-vc-mux | atm-cisco-nlpid | atm-tcc-vc-mux
            | atm-mlppp-llc | atm-nlpid | atm-ppp-llc | atm-ppp-vc-mux | atm-snap | atm-tcc-snap
            | atm-vc-mux | ether-over-atm-llc | ether-vpls-over-atm-llc | ether-vpls-over-fr |
            ether-vpls-over-ppp | ethernet | frame-relay-ccc | frame-relay-ppp | frame-relay-tcc |
            frame-relay-ether-type | frame-relay-ether-type-tcc | multilink-frame-relay-end-to-end
            | multilink-ppp | ppp-over-ether | ppp-over-ether-over-atm-llc | vlan-bridge | vlan-ccc |
            vlan-vci-ccc | vlan-tcc | vlan-vpls);
        family family {
            access-concentrator name;
            address address;
            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-vsa-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;
  }
  input-vlan-map {
    inner-tag-protocol-id tpid;
    inner-vlan-id number;
    (push | swap);
    tag-protocol-id tpid;
    vlan-id number;
  }
  output {
    service-set service-set-name {
      service-filter filter-name;
    }
  }
  output-vlan-map {
    inner-tag-protocol-id tpid;
    inner-vlan-id number;
    (pop | swap);
    tag-protocol-id tpid;
    vlan-id number;
  }
}
service-name-table table-name
short-cycle-protection <lockout-time-min minimum-seconds lockout-time-max
maximum-seconds>;
unnumbered-address interface-name <preferred-source-address address>;
keepalives {
  interval seconds;
}
ppp-options {
  chap;
  pap;
}
vlan-id number;
vlan-tags outer [tpid].vlan-id [inner [tpid].vlan-id];
}
filter {
  input filter-name {
    shared-name filter-shared-name;
  }
  output filter-name {
    shared-name filter-shared-name;
  }
}
host-prefix-only;
service {
  pcef pcef-profile-name {
    activate rule-name | activate-all;
  }
}

```

```
    }  
  }  
}
```

Hierarchy Level [edit [dynamic-profiles](#) *profile-name* [interfaces](#) *interface-name*]

Release Information Statement introduced in Junos OS Release 9.2.

Description Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.

Options *logical-unit-number*—The specific unit number of the interface you want to assign to the dynamic profile, or one of the following predefined variables:

- **\$junos-underlying-interface-unit**—For static VLANs, the unit number variable. The static unit number variable is dynamically replaced with the client unit number when the client session begins. The client unit number is specified by the DHCP when it accesses the subscriber network.
- **\$junos-interface-unit**—The unit number variable on a dynamic underlying VLAN interface for which you want to enable the creation of dynamic VLAN subscriber interfaces based on the ACL.

The remaining statements are explained separately. See [CLI Explorer](#).

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Configuring Dynamic Underlying VLAN Interfaces to Use Agent Circuit Identifier Information*
- *Configuring Static Underlying VLAN Interfaces to Use Agent Circuit Identifier Information*
- *Agent Circuit Identifier-Based Dynamic VLANs Overview*

unnumbered-address (Dynamic PPPoE)

Syntax	<code>unnumbered-address <i>interface-name</i>;</code>
Hierarchy Level	[edit dynamic-profiles <i>profile-name</i> interfaces pp0 unit "\$junos-interface-unit" family inet]
Release Information	Statement introduced in Junos OS Release 10.1.
Description	For dynamic PPPoE interfaces, enable the local address to be derived from the specified interface. Configuring unnumbered Ethernet interfaces enables IP processing on the interface without assigning an explicit IP address to the interface.
Options	<i>interface-name</i> —Interface from which the local address is derived. The interface name must include a logical unit number and must have a configured address.
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"> • <i>Configuring a PPPoE Dynamic Profile</i> • <i>Dynamic PPPoE Subscriber Interfaces over Static Underlying Interfaces Overview</i>

unnumbered-address (Dynamic Profiles)

Syntax	<code>unnumbered-address interface-name <preferred-source-address address>;</code>
Hierarchy Level	<p>[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family <i>family</i>],</p> <p>[edit dynamic-profiles <i>profile-name</i> interfaces demux0 unit <i>logical-unit-number</i> family <i>family</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.2.</p> <p>Support for the \$junos-preferred-source-address and \$junos-preferred-source-ipv6-address predefined variables introduced in Junos OS Release 9.6.</p> <p>Support for the \$junos-loopback-interface predefined variable introduced in Junos OS Release 9.6.</p>
Description	<p>For Ethernet interfaces, enable the local address to be derived from the specified interface. Configuring unnumbered Ethernet interfaces enables IP processing on the interface without assigning an explicit IP address to the interface. To configure unnumbered address dynamically, include the \$junos-loopback-interface-address predefined variable.</p> <p>You can configure unnumbered address support on Ethernet interfaces for IPv4 and IPv6 address families.</p>
Options	<p>interface-name—Name of the interface from which the local address is derived. The specified interface must have a logical unit number, a configured IP address, and must not be an unnumbered interface. This value can be a specific interface name or the \$junos-loopback-interface predefined variable.</p> <p>When defining the unnumbered-address statement using a static interface, keep the following in mind:</p> <ul style="list-style-type: none"> If you choose to include the routing-instance statement at the [edit dynamic-profiles] hierarchy level, that statement must be configured with a dynamic value by using the \$junos-routing-instance predefined variable. In addition, whatever static unnumbered interface you specify must belong to that routing instance; otherwise, the profile instantiation fails. If you choose to not include the routing-instance statement at the [edit dynamic-profiles] hierarchy level, the unnumbered-address statement uses the default routing instance. The use of the default routing instance requires that the unnumbered interface be configured statically and that it reside in the default routing instance.



NOTE: When you specify a static logical interface for the unnumbered interface in a dynamic profile that includes the **\$junos-routing-instance** predefined variable, you must not configure a preferred source address, whether with the **\$junos-preferred-source-address** predefined variable, the **\$junos-preferred-source-ipv6-address** predefined variable, or the

preferred-source-address statement. Configuring the preferred source address in this circumstance causes a commit failure.

When defining the **unnumbered-address** statement using the **\$junos-loopback-interface** predefined variable, keep the following in mind:

- To use the **\$junos-loopback-interface** predefined variable, the dynamic profile must also contain the **routing-instance** statement configured with the **\$junos-routing-instance** predefined variable at the [edit dynamic-profiles] hierarchy level.
- The applied loopback interface is based on the dynamically obtained routing instance of the subscriber.

address—(Optional) Secondary IP address of the donor interface. Configuring the preferred source address enables you to use an IP address other than the primary IP address on some of the unnumbered Ethernet interfaces in your network. This value can be a static IP address, the **\$junos-preferred-source-address** predefined variable for the inet family, or the **\$junos-preferred-source-ipv6-address** predefined variable for the inet6 family.

When defining the **preferred-source-address** value using a static IP address, keep the following in mind:

- The unnumbered interface must be statically configured.
- The IP address specified as the **preferred-source-address** must be configured in the specified unnumbered interface.

When defining the **preferred-source-address** value using the **\$junos-preferred-source-address** or the **\$junos-preferred-source-ipv6-address** predefined variables, keep the following in mind:

- You must configure the **unnumbered-address** statement using the **\$junos-loopback-interface** predefined variable.
- You must configure the **routing-instance** statement using the **\$junos-routing-instance** predefined variable at the [edit dynamic-profiles] hierarchy level.
- The preferred source address chosen is based on the dynamically applied loopback address which is in turn derived from the dynamically obtained routing instance of the subscriber. The configured loopback address with the closest network match to the user IP address is selected as the preferred source address.

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"> • <i>Dynamic Profiles Overview</i>
------------------------------	--

unnumbered-address (Ethernet)

Syntax	<code>unnumbered-address interface-name <preferred-source-address address>;</code>
Hierarchy Level	[edit interfaces interface-name unit logical-unit-number family family], [edit logical-systems <i>logical-system-name</i> interfaces interface-name unit logical-unit-number family family]
Release Information	Statement introduced in Junos OS Release 8.2. preferred-source-address option introduced in Junos OS Release 9.0.
Description	For Ethernet interfaces, enable the local address to be derived from the specified interface. Configuring an unnumbered Ethernet interface enables IP processing on the interface without assigning an explicit IP address to the interface.
Options	interface-name —Name of the interface from which the local address is derived. The specified interface must have a logical unit number and a configured IP address, and must not be an unnumbered interface. The preferred-source-address statement is explained separately.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring an Unnumbered Interface</i>• address on page 206• <i>Junos System Basics Configuration Guide</i>

username-include

Syntax	<pre>username-include { circuit-id; circuit-type; delimiter <i>delimiter-character</i>; domain-name <i>domain-name-string</i>; interface-name; mac-address; option-18; option-37; option-82 <circuit-id> <remote-id>; radius-realm <i>radius-realm-string</i>; remote-id; user-prefix <i>user-prefix-string</i>; }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> auto-configure vlan-ranges authentication], [edit interfaces <i>interface-name</i> auto-configure stacked-vlan-ranges authentication]
Release Information	Statement introduced in Junos OS Release 10.0.
Description	<p>Configure the username that the router passes to the external AAA server. You must include at least one of the optional statements for the username to be valid. If you do not configure a username, the router accesses the local authentication service only and does not use external authentication services, such as RADIUS.</p> <p>The username takes the format <i>user-prefix mac-address circuit-type circuit-id remote-id option-82 interface-name domain-name radius-realm</i>. By default, each component is separated by a period (.), but you can specify a different delimiter with the delimiter statement.</p> <p>The remaining statements are explained separately. See CLI Explorer.</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"> • <i>Configuring VLAN Interface Username Information for AAA Authentication</i> • <i>Using DHCP Option 82 Suboptions in Authentication Usernames for Autosense VLANs</i> • <i>Using DHCP Option 18 and Option 37 in Authentication Usernames for DHCPv6 Autosense VLANs</i> • Configuring a Username for Authentication of Out-of-Band Triggered Dynamic VLANs on page 168

user-prefix (DHCP Local Server)

Syntax `user-prefix user-prefix-string;`

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services **dhcp-local-server authentication** username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server **dhcpv6 authentication** username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group group-name authentication** username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server **group group-name authentication** username-include],
 [edit logical-systems *logical-system-name* system services **dhcp-local-server authentication** username-include],
 [edit logical-systems *logical-system-name* system services dhcp-local-server **dhcpv6 authentication** username-include],
 [edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 **group group-name authentication** username-include],
 [edit logical-systems *logical-system-name* system services dhcp-local-server **group group-name authentication** username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services **dhcp-local-server authentication** username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server **dhcpv6 authentication** username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group group-name authentication** username-include],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server **group group-name authentication** username-include],
 [edit routing-instances *routing-instance-name* system services **dhcp-local-server authentication** username-include],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server **dhcpv6 authentication** username-include],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group group-name authentication** username-include],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server **group group-name authentication** username-include],
 [edit system services **dhcp-local-server authentication** username-include],
 [edit system services dhcp-local-server **dhcpv6 authentication** username-include],
 [edit system services dhcp-local-server dhcpv6 **group group-name authentication** username-include],
 [edit system services dhcp-local-server **group group-name 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 the user prefix that is concatenated with the username during the subscriber authentication or DHCP client authentication process.

Options `user-prefix-string`—User prefix string.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Using External AAA Authentication Services with DHCP*

vlan-id (Dynamic VLANs)

Syntax `vlan-id number;`

Hierarchy Level [edit [dynamic-profiles profile-name interfaces interface-name unit logical-unit-number input-vlan-map](#)],
[edit [dynamic-profiles profile-name interfaces interface-name unit logical-unit-number output-vlan-map](#)]

Release Information Statement introduced in Junos OS Release 10.4.

Description For dynamic VLAN interfaces, specify the line VLAN identifiers to be rewritten at the input or output interface.

You cannot include the `vlan-id` statement with the `swap` statement, `swap-push` statement, `push-push` statement, or `push-swap` statement at the [edit [dynamic-profiles profile-name interfaces interface-name unit logical-unit-number output-vlan-map](#)] hierarchy level. If you include any of those statements in the output VLAN map, the VLAN ID in the outgoing frame is rewritten to the `vlan-id` statement that you include at the [edit [dynamic-profiles profile-name interfaces interface-name unit logical-unit-number](#)] hierarchy level.

Options *number*—A valid VLAN identifier. When used for input VLAN maps, you can specify the `$junos-vlan-map-id` predefined variable to dynamically obtain the VLAN identifier.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Rewriting the VLAN Tag on Tagged Frames*
- *Binding VLAN IDs to Logical Interfaces*

vlan-id (VLAN ID to Be Bound to a Logical Interface)

Syntax	<code>vlan-id <i>number</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]
Release Information	Statement introduced before Junos OS Release 7.4.
Description	For Fast Ethernet, Gigabit Ethernet, and Aggregated Ethernet interfaces only, bind a 802.1Q VLAN tag ID to a logical interface.
Options	<p><i>number</i>—A valid VLAN identifier.</p> <p>Range: For aggregated Ethernet, 4-port, 8-port, and 12-port Fast Ethernet PICs, and for management and internal Ethernet interfaces, 1 through 1023.</p> <p>For 48-port Fast Ethernet and Gigabit Ethernet PICs, 1 through 4094.</p> <p>VLAN ID 0 is reserved for tagging the priority of frames.</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">• <i>Configuring Mixed Tagging</i>

vlan-model

Syntax	vlan-model one-to-one;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>], [edit routing-instances <i>routing-instance-name</i>]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	Define the network VLAN model.
Options	one-to-one —Specify that any received, dual-tagged VLAN packet triggers the provisioning process in a Layer 2 Wholesale network. Using this option, the router learns VLAN tags for each individual client. The router learns both the outer tag and inner tag of the incoming packets, when the instance-role statement is defined as access , or the outer VLAN tag only, when the instance-role statement is defined as nni .
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 Separate Access Routing Instances for Layer 2 Wholesale Service Retailers on page 86• Configuring Separate NNI Routing Instances for Layer 2 Wholesale Service Retailers on page 89

vlan-ranges

Syntax `vlan-ranges {
 access-profile profile-name;
 authentication {
 packet-types [packet-types];
 password password-string;
 username-include {
 circuit-type;
 circuit-id;
 delimiter delimiter-character;
 domain-name domain-name-string;
 interface-name;
 mac-address;
 option-18;
 option-37;
 option-82 <circuit-id> <remote-id>;
 radius-realm radius-realm-string;
 remote-id;
 user-prefix user-prefix-string;
 }
 }
 dynamic-profile profile-name {
 accept (any | dhcp-v4 | inet);
 accept-out-of-band protocol;
 access-profile vlan-dynamic-profile-name;
 ranges (any | low-tag)–(any | high-tag);
 }
 override;
 }`

Hierarchy Level [edit interfaces *interface-name* **auto-configure**]

Release Information Statement introduced in Junos OS Release 9.5.

Description Configure multiple VLANs. Each VLAN is assigned a VLAN ID number from the range.



The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
 routing-control—To add this statement to the configuration.

Related Documentation

- *Configuring an Interface to Use the Dynamic Profile Configured to Create Single-Tag VLANs*
- *Configuring Interfaces to Support Both Single and Stacked VLANs*

vlan-tags

Syntax	<code>vlan-tags outer [<i>tpid</i>].<i>vlan-id</i> [inner [<i>tpid</i>].<i>vlan-id</i>];</code>
Hierarchy Level	<code>[edit dynamic-profiles <i>profile-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]</code>
Release Information	Statement introduced in Junos OS Release 9.5. VLAN demux interface support introduced in Junos OS Release 10.2.
Description	For Gigabit Ethernet IQ and IQE interfaces only, binds TPIDs and 802.1Q VLAN tag IDs to a logical interface. You must include the stacked-vlan-tagging statement at the <code>[edit interfaces <i>interface-name</i>]</code> hierarchy level.
<div>  NOTE: The inner-range <i>vid1–vid2</i> option is supported on IQE PICs only. </div>	
Options	inner [<i>tpid</i>].<i>vlan-id</i> —A TPID (optional) and a valid VLAN identifier in the format <i>tpid.vlan-id</i> . When used in the dynamic-profiles hierarchy, specify the <code>\$junos-vlan-id</code> predefined variable to dynamically obtain the VLAN ID.
<div>  NOTE: On the network-to-network (NNI) or egress interfaces of provider edge (PE) routers, you cannot configure the inner-range <i>tpid. vid1–vid2</i> option with the vlan-tags statement for ISP-facing interfaces. </div>	
Range: For VLAN ID, 1 through 4094. VLAN ID 0 is reserved for tagging the priority of frames.	
outer [<i>tpid</i>].<i>vlan-id</i> —A TPID (optional) and a valid VLAN identifier in the format <i>tpid.vlan-id</i> . When used in the dynamic-profiles hierarchy, specify the <code>\$junos-stacked-vlan-id</code> predefined variable.	
Range: For VLAN ID, 1 through 511 for normal interfaces, and 512 through 4094 for VLAN CCC interfaces. VLAN ID 0 is reserved for tagging the priority of frames.	
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 Dual VLAN Tags • stacked-vlan-tagging on page 382

vlan-tags (Stacked VLAN Tags)

Syntax	<code>vlan-tags inner <i>tpid.vlan-id</i> inner-list <i>value</i> inner-range <i>vid1—vid2</i> outer <i>tpid.vlan-id</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>], [edit logical-systems <i>logical-system-name</i> interfaces <i>interface-name</i> unit <i>logical-unit-number</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers.
Description	For Gigabit Ethernet IQ and IQE interfaces only, bind TPIDs and 802.1Q VLAN tag IDs to a logical interface.
Options	inner <i>tpid.vlan-id</i> —A TPID and a valid VLAN identifier. Range: (most routers) For VLAN ID, 1 through 4094. VLAN ID 0 is reserved for tagging the priority of frames. For PTX Series, VLAN ID 0 is not supported. inner-list <i>value</i> — List or a set of VLAN identifiers.



NOTE: This is supported on MX Series routers with Trio-based FPCs.

inner-range *tpid. vid1—vid2*—Specify a TPID and a range of VLAN IDs where vid1 is the start of the range and vid2 is the end of the range.



NOTE: On the network-to-network (NNI) or egress interfaces of provider edge (PE) routers, you cannot configure the inner-range *tpid. vid1—vid2* option with the `vlan-tags` statement for ISP-facing interfaces.

Range: For VLAN ID, 1 through 4094. VLAN ID 0 is reserved for tagging the priority of frames.

outer *tpid.vlan-id*—A TPID and a valid VLAN identifier.

Range: (most routers) For VLAN ID, 1 through 511 for normal interfaces, and 512 through 4094 for VLAN CCC interfaces. VLAN ID 0 is reserved for tagging the priority of frames. For PTX Series, VLAN ID 0 is not supported.



NOTE: Configuring inner-range with the entire vlan-id range consumes system resources and is not a best practice. The inner-range must be used only when a subset of VLAN IDs of inner tag (not the entire range) needs to be associated with a logical interface. If you specify the entire range (1 through 4094), it

has the same result as not specifying a range; however, it consumes Packet Forwarding Engine resources such as VLAN lookup table entries, and so on.

The following examples illustrate this further:

```
[edit interfaces interface-name]
stacked-vlan-tagging;
unit number {
    vlan-tags outer vid inner-range 1-4094;
}

[edit interfaces interface-name]
vlan-tagging;
unit number {
    vlan-id vid;
}
```

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"> • <i>Configuring Dual VLAN Tags</i> • <i>Configuring Flexible VLAN Tagging on PTX Series Packet Transport Routers</i> • stacked-vlan-tagging on page 382
------------------------------	--

vpls (Routing Instance)

```
Syntax  vpls {
        mac-pinning;
        active-interface {
            any;
            primary interface-name;
        }
        community COMM;
        connectivity-type (ce | irb);
        control-word;
        encapsulation-type ethernet;
        ignore-encapsulation-mismatch;
        ignore-mtu-mismatch;
        import-labeled-routes [ routing-instance-name ];
        interface interface-name;
        interface-mac-limit limit;
        label-block-size size;
        mac-flush [ explicit-mac-flush-message-options ];
        mac-table-aging-time time;
        mac-table-size size;
        mesh-group mesh-group-name {
            interface interface-name;
            l2vpn-id (as-number:id | ip-address:id);
            local-switching;
            mac-flush [ explicit-mac-flush-message-options ];
            neighbor address {...};
            peer-as all;
            pseudowire-status-tlv hot-standby-vc-on;
            route-distinguisher (as-number:id | ip-address:id);
            vpls-id number;
            vrf-export [ policy-names ];
            vrf-import [ policy-names ];
            vrf-target {
                community;
                import community-name;
                export community-name;
            }
        }
        mtu mtu;
        no-control-word;
        no-tunnel-services;
        site site-name {
            active-interface interface-name {
                any;
                primary preference-value;
            }
            best-site;
            interface interface-name {
                interface-mac-limit limit;
            }
            mesh-group mesh-group-name;
            multi-homing;
            site-identifier identifier;
```

```

    site-preference preference-value {
        backup;
        primary;
    }
}
site-range number;
traceoptions {
    file filename <files number> <size size> <world-readable | no-world-readable>;
    flag flag <flag-modifier> <disable>;
}
tunnel-services {
    devices device-names;
    primary primary-device-name;
}
}

```

Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols], [edit routing-instances <i>routing-instance-name</i> protocols]
Release Information	Statement introduced before Junos OS Release 7.4. mac-flush option introduced in Junos OS Release 10.0. hot-standby-vc-on , import-labeled-routes [<i>routing-instance-name</i>], and interface <i>interface</i> options introduced in Junos OS Release 15.1R2.
Description	Configure a virtual private LAN service (VPLS) routing instance. The remaining statements are explained separately. See CLI Explorer .
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>Configuring VPLS Routing Instances</i>

vrf-export

Syntax	<code>vrf-export [<i>policy-names</i>];</code>
Hierarchy Level	<code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols</code> <code> vpls mesh-group <i>mesh-group-name</i>]</code> <code>[edit routing-instances <i>routing-instance-name</i>]</code> <code>[edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i>]</code> <code>[edit switch-options]</code>
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 11.1 for EX Series switches. Statement introduced in Junos OS Release 12.3 for ACX Series routers. Statement introduced in Junos OS Release 14.1X53-D30 for QFX Series switches.
Description	<p>Specify how routes are exported from the local PE router's VRF table (<i>routing-instance-name</i>.inet.0) to the remote PE router. If the value vrf is specified for the instance-type statement included in the routing instance configuration, this statement is required.</p> <p>You can configure multiple export policies on the PE router or PE switch.</p>
Default	If the instance-type is vrf , vrf-export is a required statement. The default action is to reject.
Options	<i>policy-names</i> —Names for the export policies.
Required Privilege Level	<code>routing</code> —To view this statement in the configuration. <code>routing-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Implementing EVPN-VXLAN for Data Centers</i>• instance-type on page 333• <i>Configuring Policies for the VRF Table on PE Routers in VPNs</i>

vrf-import

Syntax	<code>vrf-import [<i>policy-names</i>];</code>
Hierarchy Level	<code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols</code> <code> vpls mesh-group <i>mesh-group-name</i>]</code> <code>[edit routing-instances <i>routing-instance-name</i>]</code> <code>[edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i>]</code> <code>[edit switch-options]</code>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 11.1 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 14.1X53-D30 for QFX Series switches.</p>
Description	<p>Specify how routes are imported into the virtual routing and forwarding (VRF) table (<i>routing-instance-name</i>.inet.0) of the local provider edge (PE) router or switch from the remote PE router. If the value vrf is specified for the instance-type statement included in the routing instance configuration, this statement is required.</p> <p>You can configure multiple import policies on the PE router or switch.</p>
Default	If the instance type is vrf , vrf-import is a required statement. The default action is to accept.
Options	<i>policy-names</i> —Names for the import policies.
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>Implementing EVPN-VXLAN for Data Centers</i> • instance-type on page 333 • <i>Configuring Policies for the VRF Table on PE Routers in VPNs</i>

vrf-target

Syntax	<pre>vrf-target { community; auto import community-name; export community-name; }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols l2vpn mesh-group <i>mesh-group-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i>], [edit routing-instances <i>routing-instance-name</i> protocols evpn vni-options], [edit routing-instances <i>routing-instance-name</i> protocols l2vpn mesh-group <i>mesh-group-name</i>], [edit routing-instances <i>routing-instance-name</i> protocols vpls mesh-group <i>mesh-group-name</i>], [edit switch-options]</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 11.1 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 12.3 for ACX Series routers.</p> <p>Statement introduced in Junos OS Release 14.1X53-D30 for QFX Series switches. auto option was also added at this time.</p>
Description	<p>Specify a virtual routing and forwarding (VRF) target community. If you configure the community option only, default VRF import and export policies are generated that accept and tag routes with the specified target community. The purpose of the vrf-target statement is to simplify the configuration by allowing you to configure most statements at the [edit routing-instances] hierarchy level. In effect, this statement configures a single policy for import and a single policy for export to replace the per-VRF policies for every community.</p> <p>You can still create more complex policies by explicitly configuring VRF import and export policies using the import and export options.</p>
Options	<p>community—Community name.</p> <p>auto—Automatically derives the route target (RT) for QFX5100 switches.</p> <p>import community-name—Allowed communities accepted from neighbors.</p> <p>export community-name—Allowed communities sent to neighbors.</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**
- *Configuring Policies for the VRF Table on PE Routers in VPNs*
 - *Example: Configuring FEC 129 BGP Autodiscovery for VPWS*

CHAPTER 12

Operational Commands

- clear ancp access-loop
- clear ancp neighbor
- clear dhcp relay binding
- clear dhcp relay statistics
- clear dhcp server binding
- clear dhcp server statistics
- clear dhcpv6 server binding
- clear dhcpv6 server statistics
- clear network-access aaa subscriber
- request ancp oam port-down
- request ancp oam port-up
- request auto-configuration reconnect-pending
- show ancp neighbor
- show auto-configuration out-of-band pending
- show dhcp relay binding
- show dhcp relay statistics
- show dhcp server binding
- show dhcp server statistics
- show dhcpv6 server binding
- show dhcpv6 server statistics
- show interfaces (Aggregated Ethernet)
- show interfaces (Fast Ethernet)
- show interfaces (Gigabit Ethernet)
- show interfaces (Loopback)
- show interfaces (PPPoE)
- show interfaces demux0 (Demux Interfaces)
- show interfaces filters
- show interfaces l2-routing-instance

- `show interfaces routing`
- `show interfaces routing-instance`
- `show network-access aaa statistics`
- `show network-access aaa statistics authentication`
- `show network-access aaa subscribers`
- `show network-access address-assignment pool`
- `show ppp interface`
- `show subscribers`
- `show subscribers summary`
- `show vpls connections`
- `show vpls flood event-queue`
- `show vpls flood instance`
- `show vpls flood route`
- `show vpls mac-table`
- `show vpls statistics`

clear ancp access-loop

Syntax	clear ancp access-loop (neighbor <i>ip-address</i> subscriber-interface <i>physical-interface-name</i>) circuit-id <i>aci</i> remote-id <i>ari</i> outer-vlan-id <i>vlan-id</i>
Release Information	Command introduced in Junos OS Release 16.1R4.
Description	Clear the connection for the subscriber on the specified access loop for an ANCP-triggered, autosensed dynamic VLAN. The autoconfiguration daemon (autoconfd) deletes any existing cached information about the subscriber. This command simulates a CPE connection reset as seen when the access node sends a Port Down message followed by a Port Up message.
Options	<p><i>aci</i>—ANCP Access-Loop-Circuit-ID TLV that identifies the subscriber-side access loop logical port and partially identifies an access loop to clear.</p> <p><i>ari</i>—ANCP Access-Loop-Remote-ID TLV that uniquely identifies the subscriber on the access loop and partially identifies an access loop to clear.</p> <p><i>ip-address</i>—ANCP neighbor's IP address that specifies an access loop to clear.</p> <p><i>physical-interface-name</i>—Subscriber interface that specifies an access loop to clear.</p> <p><i>vlan-id</i>—ANCP Access-Aggregation-Circuit-ID-Binary TLV that identifies the logical circuit identifier on the NAS side and partially identifies an access loop to clear.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • Clearing ANCP Access Loops on page 174 • Triggering ANCP OAM to Simulate ANCP Port Down and Port Up Messages on page 170 • Layer 2 Wholesale with ANCP-Triggered VLANs Overview on page 99
List of Sample Output	clear ancp access-loop on page 422
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 access loop to verify the clear operation.

Sample Output

clear ancp access-loop

```
user@host> clear ancp-access-loop neighbor 192.168.25.31 circuit-id line-aci-1 remote-id line-ari-1  
outer-vlan-id 126
```

clear ancp neighbor

Syntax	<pre>clear ancp neighbor <ip-address <i>ip-address</i>> <system-name <i>mac-address</i>></pre>
Release Information	Command introduced in Junos OS Release 9.4.
Description	<p>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.</p> <p>This command initiates logout of ANCP-triggered dynamic VLAN sessions on the physical interface associated with the specified neighbor; conventionally autosensed dynamic VLAN sessions and their associated logical interfaces are not affected.</p>
Options	<p>none—Clear all ANCP neighbors.</p> <p>ip-address <i>ip-address</i>—(Optional) Clear the ANCP neighbor specified by the IP address.</p> <p>system-name <i>mac-address</i>—(Optional) Clear the ANCP neighbor specified by the MAC address.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show ancp neighbor on page 447
List of Sample Output	clear ancp neighbor on page 423 show ancp neighbor on page 423
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
203.0.113.102	00:00:5e:00:53:10	Established	5	Topo
203.0.113.122	00:00:5e:00:53:12	Established	5	Topo
203.0.113.132	00:00:5e:00:53:13	Established	5	Topo
203.0.113.142	00:00:5e:00:53:14	Established	5	Topo

```
user@host> clear ancp neighbor ip-address 203.0.113.102
```

```
user@host> show ancp neighbor
```

IP Address	MAC Address	State	Subscriber Count	Capabilities
203.0.113.122	00:00:5e:00:53:12	Established	5	Topo
203.0.113.132	00:00:5e:00:53:13	Established	5	Topo
203.0.113.142	00:00:5e:00:53:14	Established	5	Topo

clear dhcp relay binding

Syntax	<pre>clear dhcp relay binding <address> <all> <dual-stack> <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 8.3.</p> <p>Options all and interface added in Junos OS Release 8.4.</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> <p>Option dual-stack added in Junos OS Release 15.1.</p>
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"> <i>ip-address</i>—The specified IP address. <i>mac-address</i>—The specified MAC address. <i>session-id</i>—The specified session ID. <p>all—(Optional) Clear the binding state for all DHCP clients.</p> <p>dual-stack—(Optional) Clear the binding state for DHCPv4 clients and the associated DHCPv6 bindings in the single-session DHCP dual stack. DHCPv6 clients created in a DHCPv6-only stack are not affected.</p> <p>interface interface-name—(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 logical-system-name—(Optional) Clear the binding state for DHCP clients on the specified logical system.</p> <p>routing-instance routing-instance-name—(Optional) Clear the binding state for DHCP clients on the specified routing instance.</p>

Required Privilege Level view

Related Documentation

- *Clearing DHCP Bindings for Subscriber Access*
- [show dhcp relay binding on page 456](#)

List of Sample Output

- [clear dhcp relay binding on page 426](#)
- [clear dhcp relay binding all on page 426](#)
- [clear dhcp relay binding dual-stack all on page 426](#)
- [clear dhcp relay binding interface on page 427](#)
- [clear dhcp relay binding <interfaces-vlan> on page 427](#)
- [clear dhcp relay binding <interfaces-wildcard> on page 427](#)

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
198.51.100.32    00:00:5e:00:53:01 active    2007-02-08 16:41:17 EST
192.168.14.8     00:00:5e:00:53:02 active    2007-02-10 10:01:06 EST
```

```
user@host> clear dhcp relay binding 198.51.100.32
```

```
user@host> show dhcp relay binding
IP address      Hardware address  Type    Lease expires at
192.168.14.8     00:00:5e:00:53:02 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 dual-stack all](#)

The following command clears all DHCP relay agent bindings for all DHCPv4 clients and the associated DHCPv6 bindings in the single-session DHCP dual stack. DHCPv6 clients created in a DHCPv6-only stack are not affected.

```
user@host> clear dhcp relay binding dual-stack 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	clear dhcp relay statistics <bulk-leasequery-connections> <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>>
Syntax	Syntax for EX Series switches: show dhcp relay statistics <routing-instance <i>routing-instance-name</i>>
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. bulk-leasequery-connections option introduced in Junos OS Release 16.1.
Description	Clear all Dynamic Host Configuration Protocol (DHCP) relay statistics.
Options	bulk-leasequery-connections —(Optional) Clear bulk leasequery statistics. 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 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
Related Documentation	<ul style="list-style-type: none">• show dhcp relay statistics on page 462
List of Sample Output	clear dhcp relay statistics on page 429
Output Fields	Table 14 on page 429 lists the output fields for the clear dhcp relay statistics command.

Table 14: 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 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>`
 `<dual-stack>`

Release Information Command introduced in Junos OS Release 9.0.
 Options *interfaces-vlan* and *interfaces-wildcard* added in Junos OS Release 12.1.
 Command updated with **dual-stack** statement in Junos OS Release 17.3.

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.

dual-stack—(Optional) Remove either both arms or single arm of dual-stack.



NOTE:

- The **dual-stack** command is added in the syntax removes both arms of the dual-stack with a single command entry.
 - When the **dual-stack** command is not added in the syntax, the **clear dhcpv6 server binding** command clears only the family specific arm of the dual-stack.
-

Required Privilege Level

view

Related Documentation

- *Clearing DHCP Bindings for Subscriber Access*
- [show dhcp server binding on page 466](#)

List of Sample Output

[clear dhcp server binding <ip-address> on page 432](#)
[clear dhcp server binding all on page 433](#)
[clear dhcp server binding interface on page 433](#)
[clear dhcp server binding <interfaces-vlan> on page 433](#)
[clear dhcp server binding <interfaces-wildcard> on page 433](#)
[clear dhcp server binding dual-stack all on page 433](#)

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
198.51.100.1	00:00:5e:00:53:01	active	2007-01-17 11:38:47 PST
198.51.100.3	00:00:5e:00:53:02	active	2007-01-17 11:38:41 PST

```
user@host> clear dhcp server binding 198.51.100.1
```

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

```
1 clients, (0 bound, 0 selecting, 0 renewing, 0 rebinding)
```

IP address	Hardware address	Type	Lease expires at
198.51.100.3	00:00:5e:00:53:02	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 binding dual-stack all

The following command clears all the dual-stack local server bindings.

```
user@host> clear dhcp server binding dual-stack all
```

clear dhcp server statistics

Syntax	<code>clear dhcp server statistics</code> <code><bulk-leasequery-connections></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. <code>bulk-leasequery-connections</code> option introduced in Junos OS Release 16.1.
Description	Clear all extended Dynamic Host Configuration Protocol (DHCP) local server statistics.
Options	<code>bulk-leasequery-connections</code> —(Optional) Clear bulk leasequery statistics. <code>logical-system <i>logical-system-name</i></code> —(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. <code>routing-instance <i>routing-instance-name</i></code> —(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.
Required Privilege Level	view
List of Sample Output	clear dhcp server statistics on page 434
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> <dual-stack></pre>
Release Information	Command introduced in Junos OS Release 9.6. Options <i>interfaces-vlan</i> and <i>interfaces-wildcard</i> added in Junos OS Release 12.1. Command updated with dual-stack statement in Junos OS Release 17.3.
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> <p>dual-stack—(Optional) Remove either both arms or single arm of dual-stack.</p>

**NOTE:**

- The **dual-stack** command is added in the syntax removes both arms of the dual-stack with a single command entry.
- When the **dual-stack** command is not added in the syntax, the **clear dhcpv6 server binding** command clears only the family specific arm of the dual-stack.

Required Privilege Level clear

Related Documentation

- *Clearing DHCP Bindings for Subscriber Access*
- [show dhcpv6 server binding on page 477](#)

List of Sample Output

[clear dhcpv6 server binding all on page 437](#)
[clear dhcpv6 server binding <ipv6-prefix> on page 437](#)
[clear dhcpv6 server binding interface on page 437](#)
[clear dhcpv6 server binding <interfaces-vlan> on page 438](#)
[clear dhcpv6 server binding <interfaces-wildcard> on page 438](#)
[clear dhcpv6 server binding dual-stack all on page 438](#)

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 binding dual-stack all

The following command clears all the dual-stack local server bindings.

```
user@host> clear dhcpv6 server binding dual-stack all
```

clear dhcpv6 server statistics

Syntax	<pre>clear dhcpv6 server statistics <bulk-leasequery-connections> <interface <i>interface-name</i>> <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>></pre>
Release Information	<p>Command introduced in Junos OS Release 9.6.</p> <p>bulk-leasequery-connections option introduced in Junos OS Release 16.1.</p>
Description	Clear all extended Dynamic Host Configuration Protocol for IPv6 (DHCPv6) local server statistics.
Options	<p>bulk-leasequery-connections—(Optional) Clear bulk leasequery statistics.</p> <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 483
List of Sample Output	clear dhcpv6 server statistics on page 439
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 network-access aaa subscriber

Syntax	<pre>clear network-access aaa subscriber <session-id <i>identifier</i> <reconnect>> <statistics username <i>username</i>> <username <i>username</i> <reconnect>></pre>
Release Information	Command introduced in Junos OS Release 9.1. reconnect and session-id options added in Junos OS Release 16.1R4.
Description	Clear AAA subscriber statistics and log out subscribers. You can log out subscribers based on the username or on the subscriber session identifier. Use the session identifier when more than one session has the same username string.
Options	<p>reconnect—(Optional) Reconnect as a Layer 2 wholesale session when the subscriber session has been fully logged out. This option is equivalent to issuing a RADIUS-initiated disconnect with reconnect semantics; that is, when the message includes Acct-Terminate-Cause (RADIUS attribute 49) with a value of callback (16). You can apply this option to either a Layer 2 wholesale session or a conventionally auto-sensed dynamic VLAN supporting a PPPoE session.</p> <p>In the latter case, this option triggers a PPPoE session logout and removal of the dynamic VLAN logical interface. This is followed by authorization of the access-line to attempt creation of a dynamic VLAN IFL supporting Layer 2 wholesale session in its place.</p> <p>session-id <i>identifier</i>—(Optional) Log out the subscriber based on the subscriber session identifier.</p> <p>statistics username <i>username</i>—(Optional) Clear AAA subscriber statistics and log out the subscriber.</p> <p>username <i>username</i>—(Optional) Log out the AAA subscriber.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none">• <i>Verifying and Managing Subscriber AAA Information</i>
List of Sample Output	clear network-access aaa subscriber statistics username on page 441 clear network-access aaa subscriber username on page 441 clear network-access aaa subscriber username on page 441
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 user22@example.com
```

clear network-access aaa subscriber username

```
user@host> clear network-access aaa subscriber username user22@example.com
```

clear network-access aaa subscriber username

```
user@host> clear network-access aaa subscriber session-id 18367425
```

request ancp oam port-down

Syntax	request ancp oam port-down (neighbor <i>ip-address</i> subscriber-interface <i>physical-interface-name</i>) circuit-id <i>aci</i> remote-id <i>ari</i> outer-vlan-id <i>vlan-id</i>
Release Information	Command introduced in Junos OS Release 16.1R4.
Description	Simulate an ANCP Port Down message on the specified access loop for troubleshooting or to mitigate an abnormal condition. Triggers removal of the corresponding out-of-band triggered, autosensed dynamic VLAN session for which no ANCP-sourced information exists. You must specify an ACI, an ARI, and an outer VLAN tag. This command is overridden by a genuine ANCP Port-Up message, meaning that you cannot use this command to initiate a Port Down condition when the access node has already reported a Port Up condition.
Options	<p>aci—ANCP Access-Loop-Circuit-ID TLV that corresponds to a subscriber interface on the access node; used to identify the access node from which the message is simulated.</p> <p>ari—ANCP Access-Loop-Remote-ID TLV that identifies the subscriber associated with an interface on the access node; used to identify the access node from which the message is simulated.</p> <p>ip-address—IP address that specifies the access node from which the message is simulated.</p> <p>physical-interface-name—Name of the access-facing subscriber interface that specifies the access node on whose local loop the loopback test is run.</p> <p>vlan-id—ANCP Access-Aggregation-Circuit-ID-Binary TLV, the outer VLAN tag inserted by the access node on upstream traffic; used to identify the access node from which the message is simulated.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• Triggering ANCP OAM to Simulate ANCP Port Down and Port Up Messages on page 170• Layer 2 Wholesale with ANCP-Triggered VLANs Overview on page 99
List of Sample Output	request ancp oam port-down neighbor circuit-id remote-id outer-vlan-id on page 443
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 detail , show subscribers client-type vlan-oob detail , and the show subscribers summary commands before and after initiating the Port Down message to verify the operation.

Sample Output

`request ancp oam port-down neighbor circuit-id remote-id outer-vlan-id`

```
user@host> request ancp oam port-down neighbor 192.168.25.31 circuit-id line-aci-1 remote-id  
line-ari-1 outer-vlan-id 126
```

request ancp oam port-up

Syntax	request ancp oam port-up (neighbor <i>ip-address</i> subscriber-interface <i>physical-interface-name</i>) circuit-id <i>aci</i> remote-id <i>ari</i> outer-vlan-id <i>vlan-id</i>
Release Information	Command introduced in Junos OS Release 16.1R4.
Description	Simulate an ANCP Port Up message on the specified access loop for troubleshooting or to mitigate an abnormal condition. You must specify an ACI, an ARI, and an outer VLAN tag. This command is overridden by a genuine ANCP Port Down message, meaning that you cannot use this command to initiate a Port Up condition when the access node has already reported a Port Down condition.
Options	<p><i>aci</i>—ANCP Access-Loop-Circuit-ID TLV that corresponds to a subscriber interface on the access node; used to identify the access node from which the message is simulated.</p> <p><i>ip-address</i>—IP address that specifies the access node from which the message is simulated.</p> <p><i>ari</i>—ANCP Access-Loop-Remote-ID TLV that identifies the subscriber associated with an interface on the access node; used to identify the access node from which the message is simulated.</p> <p><i>physical-interface-name</i>—Name of the access-facing subscriber interface that specifies the access node on whose local loop the loopback test is run.</p> <p><i>vlan-id</i>—ANCP Access-Aggregation-Circuit-ID-Binary TLV, the outer VLAN tag inserted by the access node on upstream traffic; used to identify the access node from which the message is simulated.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• Triggering ANCP OAM to Simulate ANCP Port Down and Port Up Messages on page 170• Layer 2 Wholesale with ANCP-Triggered VLANs Overview on page 99
List of Sample Output	request ancp oam port-up neighbor circuit-id remote-id outer-vlan-id on page 445
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 detail , show subscribers client-type vlan-oob detail , and the show subscribers summary commands before and after initiating the Port Up message to verify the operation.

Sample Output

`request ancp oam port-up neighbor circuit-id remote-id outer-vlan-id`

```
user@host> request ancp oam port-up neighbor 192.168.25.31 circuit-id line-aci-1 remote-id  
line-ari-1 outer-vlan-id 126
```

request auto-configuration reconnect-pending

Syntax	request auto-configuration reconnect-pending
Release Information	Command introduced in Junos OS Release 16.1R4.
Description	Initiate reestablishment of Layer 2 wholesale sessions that correspond to access lines that are in the pending state. Ordinarily, the most likely situations with pending sessions are handled automatically. This statement is intended to be used only when an uncommon condition might prevent automatic reestablishment. This command has no effect when no pending sessions are present.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• Reestablishing Pending Access Line Sessions for Layer 2 Wholesale on page 173• Layer 2 Wholesale with ANCP-Triggered VLANs Overview on page 99
List of Sample Output	request auto-configuration reconnect-pending on page 446
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 detail , show subscribers client-type vlan-oob detail , and the show subscribers summary commands before and after initiating the Port Up message to verify the operation.

Sample Output

request auto-configuration reconnect-pending

```
user@host> request auto-configuration reconnect-pending
```

show ancp neighbor

Syntax	<pre>show ancp neighbor <brief detail> <ip-address ip-address> <system-name mac-address></pre>
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 ip-address —(Optional) Display information about the neighbor (access node) specified by the IP address.</p> <p>system-name mac-address—(Optional) Display information about the neighbor (access node) specified by the MAC address.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>show ancp cos</i> • <i>show ancp subscriber</i>
List of Sample Output	<p>show ancp neighbor on page 450</p> <p>show ancp neighbor detail on page 451</p> <p>show ancp neighbor ip-address on page 452</p> <p>show ancp neighbor system-name on page 453</p>
Output Fields	Table 15 on page 447 lists the output fields for the show ancp neighbor command. Output fields are listed in the approximate order in which they appear.

Table 15: show ancp neighbor Output Fields

Field Name	Field Description	Level of Output
Version	<p>Version of the ANCP implementation:</p> <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>. 	<p>brief detail</p> <p>none</p>
IP Address	IP address of the ANCP neighbor.	<p>brief detail</p> <p>none</p>

Table 15: show ancp neighbor Output Fields (*continued*)

Field Name	Field Description	Level of Output
Partid	Number that associates the ANCP message with a specific partition.	brief none
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 Established—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

Table 15: show ancp neighbor Output Fields (*continued*)

Field Name	Field Description	Level of Output
Partition Flag	Number that specifies the type of partition requested: 1 (new adjacency) or 2 (recovered adjacency).	detail
Partition Identifier	<p>Number that identifies a logical partition of an access node with which the ANCP agent has formed an adjacency.</p> <p>A value of zero indicates that the 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.</p> <p>A nonzero value indicates that the agent supports each neighbor on an IP address over a single TCP session with a nonzero partition ID.</p>	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

Table 15: show ancp neighbor Output Fields (*continued*)

Field Name	Field Description	Level of Output
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
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
                                Count
    0x31   203.0.113.13      0      Established  11:24      2
  Topo
    0x31   203.0.113.15      0      Not Estblshd  2:45      2
  Topo
  * 0x0    198.51.100.102      0      Establishing  0          0

```



```
* 0x0    192.0.2.0      0    Configured    0    0
* 0x0    192.0.2.1      0    Configured    0    0
```

show ancp neighbor detail

```
user@host> show ancp neighbor detail
```

Neighbor Information

```
Version          : 0x31
IP Address       : 192.0.2.85
System Name      : 00:00:5e:00:53:01
  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
  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
```

```
Version          : 0x32
IP Address       : 192.168.9.1
System Name      : 00:00:5e:00:53:02
  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
Received                      : 0
Sent                          : 0

```

show ancp neighbor ip-address

```
user@host> show ancp neighbor ip-address 192.0.2.85
```

```

Neighbor Information
Version                : 0x32
IP Address             : 192.0.2.85
System Name            : 00:00:5e:00:53:ba
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
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 system-name

```
user@host> show ancp neighbor 00:00:5e:00:53:ba detail
```

Neighbor Information

```

Version           : 0x31
IP Address        : 203.0.113.101
System Name       : 00:00:5e:00:53:ba
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 auto-configuration out-of-band pending

Syntax	show auto-configuration out-of-band pending
Release Information	Command introduced Junos OS Release 16.1R4.
Description	Display a list of access lines that are in the pending state for each routing instance. Access lines transition to the pending state when the Layer 2 wholesale session passes authorized and is assigned to an existing, nondefault routing instance, but profile instantiation to create the dynamic VLAN logical interface fails.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Layer 2 Wholesale with ANCP-Triggered VLANs Overview on page 99
List of Sample Output	show auto-configuration out-of-band pending on page 455
Output Fields	Table 16 on page 455 lists the output fields for the show auto-configuration out-of-band pending command. Output fields are listed in the approximate order in which they appear.

Table 16: show auto-configuration out-of-band pending Output Fields

Field Name	Field Description
Routing-Instance	Name of the routing instance for which the pending count is displayed.
Pending count	Number of access lines in the routing instance that are in the pending state.

Sample Output

show auto-configuration out-of-band pending

```

user@host> show auto-configuration out-of-band pending
Routing-Instance: NSP1
Pending count: 12

Routing-Instance: NSP2
Pending count: 0

```

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](#)
- [clear dhcp relay binding on page 425](#)

List of Sample Output

- [show dhcp relay binding on page 459](#)
- [show dhcp relay binding detail on page 459](#)
- [show dhcp relay binding interface on page 459](#)
- [show dhcp relay binding interface vlan-id on page 460](#)
- [show dhcp relay binding interface svlan-id on page 460](#)
- [show dhcp relay binding ip-address on page 460](#)
- [show dhcp relay binding mac-address on page 460](#)
- [show dhcp relay binding session-id on page 460](#)
- [show dhcp relay binding <interfaces-vlan> on page 460](#)
- [show dhcp relay binding <interfaces-wildcard> on page 460](#)
- [show dhcp relay binding summary on page 461](#)

Output Fields Table 17 on page 457 lists the output fields for the **show dhcp relay binding** command. Output fields are listed in the approximate order in which they appear.

Table 17: 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.	brief detail
Session Id	Session ID of the subscriber session.	brief detail
Generated Remote ID	Remote ID generated by the Option 82 Agent Remote ID (suboption 1)	detail
Hardware address	Hardware address of the DHCP client.	brief detail
Expires	Number of seconds in which the lease expires.	brief detail

Table 17: 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. 	brief detail
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
Dual Stack Group	Name of dual stack that is configured with the DHCP binding.	detail
Dual Stack Peer Prefix	Prefix of dual stack DHCPv6 peer.	detail
Dual Stack Peer Address	Address of the dual stack DHCPv6 peer.	detail

Sample Output

show dhcp relay binding

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

IP address	Session Id	Hardware address	Expires	State	Interface
198.51.100.11	41	00:00:5e:00:53:01	86371	BOUND	ge-1/0/0.0
198.51.100.12	42	00:00:5e:00:53:02	86371	BOUND	ge-1/0/0.0
198.51.100.13	43	00:00:5e:00:53:03	86371	BOUND	ge-1/0/0.0
198.51.100.14	44	00:00:5e:00:53:04	86371	BOUND	ge-1/0/0.0
198.51.100.15	45	00:00:5e:00:53:05	86371	BOUND	ge-1/0/0.0

show dhcp relay binding detail

```
user@host> show dhcp relay binding detail
```

```
Client IP Address: 198.51.100.11
  Hardware Address:      00:00:5e:00:53:01
  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:      198.51.100.22
  Server Interface:       none
  Bootp Relay Address:    198.51.100.32
  Session Id:             41
  Dual Stack Group:       dual-stack-retail6
  Dual Stack Peer Prefix: 2001:db8:0:4::/64
  Dual Stack Peer Address: 2001:db8:1:0:8003::1/128
```

```
Client IP Address: 198.51.100.12
  Hardware Address:      00:00:5e:00:53:02
  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:      198.51.100.22
  Server Interface:       none
  Bootp Relay Address:    198.51.100.32
  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
198.51.100.1	00:00:5e:00:53:01	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
198.51.100.15	6	00:00:5e:00:53:94	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
198.51.100.16	7	00:00:5e:00:53:92	86124	BOUND	ge-1/1/0:10-100

show dhcp relay binding ip-address

```
user@host> show dhcp relay binding 198.51.100.13
```

IP address	Session Id	Hardware address	Expires	State	Interface
198.51.100.13	43	00:00:5e:00:53:03	86293	BOUND	ge-1/0/0.0

show dhcp relay binding mac-address

```
user@host> show dhcp relay binding 00:00:5e:00:53:05
```

IP address	Session Id	Hardware address	Expires	State	Interface
198.51.100.15	45	00:00:5e:00:53:05	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
198.51.100.11	41	00:00:5e:00:53:53	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	00:00:5e:00:53:02	86346	BOUND	ge-1/0/0.1073741827
192.168.0.16	41	00:00:5e:00:53:01	86346	BOUND	ge-1/0/0.1073741827

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	00:00:5e:00:53:04	86361	BOUND	ge-1/3/0.110
192.168.0.8	23	00:00:5e:00:53:03	86361	BOUND	ge-1/3/0.110
192.168.0.7	22	00:00:5e:00:53:02	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	show dhcp relay statistics <bulk-leasequery-connections> <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>>
Syntax	Syntax for EX Series switches: show dhcp relay statistics <routing-instance <i>routing-instance-name</i>>
Release Information	Command introduced in Junos OS Release 8.3. Command 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. bulk-leasequery-connections option introduced in Junos OS Release 16.1.
Description	Display Dynamic Host Configuration Protocol (DHCP) relay statistics.
Options	bulk-leasequery-connections —(Optional) Display information about bulk leasequery operations. 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. 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.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• clear dhcp relay statistics on page 428
List of Sample Output	show dhcp relay statistics on page 464 show dhcp relay statistics bulk-leasequery-connections on page 465
Output Fields	Table 18 on page 463 lists the output fields for the show dhcp relay statistics command. Output fields are listed in the approximate order in which they appear.

Table 18: 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 • DHCPLEASEACTIVE—Number of active DHCP leases • DHCPLEASEUNASSIGNED—Number of DHCP leases that are managed by the server but have not yet been assigned • DHCPLEASEUNKNOWN—Number of unknown DHCP leases • DHCPLEASEQUERYDONE—The leasequery is complete
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 • DHCPLEASEQUERY—Number of DHCP leasequery messages transmitted • DHCPLEASEBULKLEASEQUERY—Number of DHCP bulk leasequery messages transmitted

Table 18: show dhcp relay statistics Output Fields (*continued*)

Field Name	Field Description
External Server Response	State of the external DHCP server responsiveness.
Packets forwarded	Number of packets forwarded. <ul style="list-style-type: none"> BOOTREQUEST—Number of BOOTREQUEST protocol data units (PDUs) forwarded BOOTREPLY—Number of BOOTREPLY protocol data units (PDUs) forwarded
External Server Response	State of the external DHCP server responsiveness.
Total Requested Servers	Total number of servers with which the DHCP relay agent has requested a bulk leasequery connection.
Total Attempted Servers	Total number of servers with which the DHCP relay agent has attempted to create a bulk leasequery connection.
Total Connected	Total number of servers that have formed a bulk leasequery connection with the DHCP relay agent.
Total Terminated by Server	Total number of servers that have terminated a bulk leasequery connection with the DHCP relay agent.
Total Max Attempted	Total number of servers where the DHCP relay agent reached the maximum retry limit when it attempted to create a bulk leasequery connection.
Total Closed due to Errors	Total number of bulk leasequery connections that closed due to an internal error on the DHCP relay agent.
In-Flight Connected	Number of current bulk leasequery connections on the DHCP relay agent.
Bulk Leasequery Reply Packet Retries	Number of bulk leasequery reply packets that the DHCP relay agent has retried.

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
DHCPCDECLINE       0
DHCPDISCOVER       11
DHCPINFORM         0
DHCPRELEASE        0
DHCPREQUEST        105
DHCPLEASEACTIVE    0
DHCPLEASEUNASSIGNED 0
DHCPLEASEUNKNOWN   0
DHCPLEASEQUERYDONE 0

Messages sent:
BOOTREPLY          0
DHCPOFFER          2
DHCPACK            1
DHCPNAK            0
DHCPFORCERENEW     0
DHCPLEASEQUERY     0
DHCPBULKLEASEQUERY 0

Packets forwarded:
Total              4
BOOTREQUEST        2
BOOTREPLY          2

External Server Response:
State              Responding

```

show dhcp relay statistics bulk-leasequery-connections

```

user@host> show dhcp relay statistics bulk-leasequery-connections

Total Requested Servers: 0
Total Attempted Servers: 0
Total Connected: 0
Total Terminated by Server: 0
Total Max Attempted: 0
Total Closed due to Errors: 0
In-Flight Connected: 0
Bulk Leasequery Reply Packet Retries: 0

```

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*
- *Verifying and Managing Agent Circuit Identifier-Based Dynamic VLAN Configuration*
- [clear dhcp server binding on page 431](#)

List of Sample Output

[show dhcp server binding on page 470](#)
[show dhcp server binding detail on page 470](#)
[show dhcp server binding detail \(ACI Interface Set Configured\) on page 471](#)
[show dhcp server binding interface <vlan-id> on page 471](#)
[show dhcp server binding interface <svlan-id> on page 471](#)
[show dhcp server binding <ip-address> on page 471](#)
[show dhcp server binding <session-id> on page 472](#)
[show dhcp server binding summary on page 472](#)
[show dhcp server binding <interfaces-vlan> on page 472](#)
[show dhcp server binding <interfaces-wildcard> on page 472](#)

Output Fields [Table 19 on page 467](#) lists the output fields for the **show dhcp server binding** command. Output fields are listed in the approximate order in which they appear.

Table 19: show dhcp server binding Output Fields

Field Name	Field Description	Level of Output
<i>number clients, (number init, number bound, number selecting, number requesting, number renewing, number releasing)</i>	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 19: 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

Table 19: show dhcp server binding Output Fields (*continued*)

Field Name	Field Description	Level of Output
Liveness Detection State	<p>State of the liveness detection status for a subscriber's Bidirectional Forwarding Detection (BFD) protocol session:</p> <p>NOTE: This output field displays status only when liveness detection has been explicitly configured for a subscriber and the liveness detection protocol is actively functioning for that subscriber.</p> <ul style="list-style-type: none"> DOWN—Liveness detection has been enabled for a subscriber but the broadband network gateway (BNG) detects that the liveness detection session for the BFD protocol is in the DOWN state. A liveness detection session that was previously in an UP state has transitioned to a DOWN state, beginning with a liveness detection failure, and ending with the deletion of the client binding. The DOWN state is reported only during this transition period of time. UNKNOWN—Liveness detection has been enabled for a subscriber but the actual liveness detection state has not yet been determined. The UNKNOWN state is reported after a DHCP subscriber initially logs in while the underlying liveness detection protocol handshake, such as BFD, is still processing and the BFD session has not yet reached the UP state. UP—Liveness detection has been enabled for a subscriber, and the BNG and the subscriber or client have <i>both</i> determined that the liveness detection session for the BFD protocol is in the UP state. WENT_DOWN—State is functionally equivalent to the DOWN state. A liveness detection session that was previously in an UP state has transitioned to a DOWN state implying a liveness detection failure. The WENT_DOWN state applies to the internal distribution of the liveness detection mechanism between the Junos DHCP Daemon for Subscriber Services (JDHCPd), the BFD plug-in within the Broadband Edge Subscriber Management Daemon (BBE-SMGD), and the Packet Forwarding Engine. 	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
Client Profile Name	DHCP client profile name.	detail
Dual Stack Group	DHCP server profile name.	detail
Dual Stack Peer Prefix	IPv6 prefix of peer.	detail

Table 19: show dhcp server binding Output Fields (*continued*)

Field Name	Field Description	Level of Output
Dual Stack Peer Address	IPv6 address of peer.	detail

Sample Output

show dhcp server binding

```

user@host> show dhcp server binding
IP address      Session Id  Hardware address  Expires    State      Interface
198.51.100.15   6           00:00:5e:00:53:01 86180      BOUND      ge-1/0/0.0
198.51.100.16   7           00:00:5e:00:53:02 86180      BOUND      ge-1/0/0.0
198.51.100.17   8           00:00:5e:00:53:03 86180      BOUND      ge-1/0/0.0
198.51.100.18   9           00:00:5e:00:53:04 86180      BOUND      ge-1/0/0.0
198.51.100.19   10          00:00:5e:00:53:05 86180      BOUND      ge-1/0/0.0

```

show dhcp server binding detail

```

user@host> show dhcp server binding detail
Client IP Address: 198.51.100.15
  Hardware Address:      00:00:5e:00:53:01
  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:     198.51.100.9
  Server Interface:      none
  Session Id:            6
  Client Pool Name:      6
  Liveness Detection State: UP
Client IP Address: 198.51.100.16
  Hardware Address:      00:00:5e:00:53:02
  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:     198.51.100.9
  Server Interface:      none
  Session Id:            7
  Client Pool Name:      7
  Liveness Detection State: UP

```

When DHCP binding is configured with dual-stack, we get the following output:

```

user@host> show dhcp server binding detail
Client IP Address: 100.20.0.10
  Hardware Address:      00:00:64:03:01:02
  State:                  BOUND(LOCAL_SERVER_STATE_BOUND)

```

```

Protocol-Used:          DHCP
Lease Expires:          2016-11-07 08:30:39 PST
Lease Expires in:       43706 seconds
Lease Start:            2016-11-04 11:00:37 PDT
Last Packet Received:   2016-11-06 09:00:39 PST
Incoming Client Interface: ae0.3221225472
Client Interface Svlan Id: 2000
Client Interface Vlan Id: 1
Server Ip Address:      100.20.32.2
Session Id:             2
Client Pool Name:       my-v4-pool
Client Profile Name:    dhcp-retail
Dual Stack Group:       my-dual-stack
Dual Stack Peer Prefix: 3ffe:ffff:0:4::/64
Dual Stack Peer Address: 3000:0:0:8003::1/128

```

show dhcp server binding detail (ACI Interface Set Configured)

```

user@host> show dhcp server binding detail
Client IP Address: 198.51.100.14
  Hardware Address: 00:00:5e:00:53:02
  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: 198.51.100.202
  Session Id: 11
  Client Pool Name: poolA
  Client Profile Name: DEMUXprofile
  Liveness Detection State: UP
  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
198.51.100.15   6          00:00:5e:00:53:01  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
198.51.100.16   7          00:00:5e:00:53:02  86124   BOUND
ge-1/1/0:10-100

```

show dhcp server binding <ip-address>

```

user@host> show dhcp server binding 198100.19
IP address      Session Id  Hardware address  Expires  State  Interface
198.51.100.19   10         00:00:5e:00:53:05  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
198.51.100.15   6          00:00:5e:00:53:01 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         00:00:5e:00:53:02 86346    BOUND
ge-1/0/0.1073741827
192.168.0.16    41         00:00:5e:00:53:01 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         00:00:5e:00:53:04 86361    BOUND
ge-1/3/0.110
192.168.0.8     23         00:00:5e:00:53:03 86361    BOUND
ge-1/3/0.110
192.168.0.7     22         00:00:5e:00:53:02 86361    BOUND
ge-1/3/0.110
```

show dhcp server statistics

Syntax	<pre>show dhcp server statistics <bulk-leasequery-connections> <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>></pre>
Release Information	<p>Command introduced in Junos OS Release 9.0.</p> <p>bulk-leasequery-connections option introduced in Junos OS Release 16.1.</p>
Description	Display extended Dynamic Host Configuration Protocol (DHCP) local server statistics.
Options	<p>bulk-leasequery-connections—(Optional) Display bulk leasequery statistics.</p> <p>bulk-leasequery-connections—(Optional) Display information about bulk leasequery statistics.</p> <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 434
List of Sample Output	<p>show dhcp server statistics on page 475</p> <p>show dhcp server statistics on page 476</p>
Output Fields	<p>Table 20 on page 474 lists the output fields for the show dhcp server statistics command. Output fields are listed in the approximate order in which they appear.</p>

Table 20: 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 • DHCPLEASEQUERY—Number of DHCP leasequery messages received. • DHCPBULKLEASEQUERY—Number of DHCP bulk leasequery messages received. • DHCPRENEW—Number of DHCP renew messages received; subset of DHCPREQUEST counter. • DHCPREBIND—Number of DHCP rebind messages received; subset of DHCPREQUEST counter.

Table 20: show dhcp server statistics Output Fields (*continued*)

Field Name	Field Description
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 DHCLEASEUNASSIGNED—Number of DHCP leases that are managed by the server but have not yet been assigned DHCLEASEUNKNOWN—Number of unknown DHCP leases DHCLEASEACTIVE—Number of active DHCP leases DHCLEASEQUERYDONE—The leasequery is complete
Total Accepted Connections	Total number of bulk leasequery connections accepted by the server.
Total Not-Accepted Connections	Total number of bulk leasequery connections not accepted by the server.
Connections Closed due to Errors	Number of bulk leasequery connections that the server closed due to an internal error.
Connections Closed due to max-empty-replies	Number of bulk leasequery connections that the server closed because the maximum number of empty replies was reached.
In-flight Connections	Number of bulk leasequery connections on the server.

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
  DHCPRENEW      4
  DHCPREBIND     2

Messages sent:
  BOOTREPLY      20
  DHCPOFFER      10
  DHCPACK        10

```

DHCPNAK	0
DHCPFORCERENEW	0

show dhcp server statistics

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

Packets dropped:

Total	0
-------	---

Messages received:

BOOTREQUEST	238
DHCPDECLINE	0
DHCPDISCOVER	1
DHCPINFORM	0
DHCPRELEASE	0
DHCPREQUEST	237
DHCPRENEW	236
DHCPREBIND	0

Messages sent:

BOOTREPLY	20
DHCPOFFER	10
DHCPACK	10
DHCPNAK	0
DHCPFORCERENEW	0

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**
- [Clearing DHCP Bindings for Subscriber Access](#)
 - [clear dhcpv6 server binding on page 436](#)

- List of Sample Output**
- [show dhcpv6 server binding on page 480](#)
 - [show dhcpv6 server binding detail on page 480](#)
 - [show dhcpv6 server binding interface on page 480](#)
 - [show dhcpv6 server binding interface detail on page 480](#)
 - [show dhcpv6 server binding \(IPv6 Prefix\) on page 481](#)
 - [show dhcpv6 server binding \(Session ID\) on page 481](#)
 - [show dhcpv6 server binding \(Interfaces VLAN\) on page 481](#)
 - [show dhcpv6 server binding \(Interfaces Wildcard\) on page 481](#)
 - [show dhcpv6 server binding \(Interfaces Wildcard\) on page 482](#)
 - [show dhcpv6 server binding summary on page 482](#)

Output Fields Table 21 on page 478 lists the output fields for the **show dhcpv6 server binding** command. Output fields are listed in the approximate order in which they appear.

Table 21: 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

Table 21: show dhcpv6 server binding Output Fields (*continued*)

Field Name	Field Description	Level of Output
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
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
Server Id	DHCP unique identifier (DUID) for the DHCPv6 server.	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
Dual Stack Group	DHCPv6 server profile name.	detail
Dual Stack Peer Address	DHCPv6 Peer IP address.	detail

Sample Output

show dhcpv6 server binding

```
user@host> show dhcpv6 server binding
Prefix                Session Id Expires State Interface Client DUID
2001:db8:1111:2222::/64 6      86321 BOUND ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:01
2001:db8:1111:2222::/64 7      86321 BOUND ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:02
2001:db8:1111:2222::/64 8      86321 BOUND ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:03
2001:db8:1111:2222::/64 9      86321 BOUND ge-1/0/0.0
LL_TIME0x1-0x2e159c1-00:10:94:00:00:04
2001:db8:1111:2222::/64 10     86321 BOUND ge-1/0/0.0
LL_TIME0x1-0x2e159c1-00:10:94:00:00:05
2001:db8:2002::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: 2
  Client IPv6 Prefix:      3ffe:ffff:0:4::/64
  Client IPv6 Address:    3000:0:0:8003::1/128
  Client DUID:            LL0x1-00:00:64:01:01:02
  State:                  BOUND(DHCPV6_LOCAL_SERVER_STATE_BOUND)

  Lease Expires:          2016-11-07 08:30:39 PST
  Lease Expires in:       43706 seconds
  Preferred Lease Expires: 2016-11-07 08:30:39 PST
  Preferred Lease Expires in: 43706 seconds
  Lease Start:            2016-11-04 11:00:37 PDT
  Last Packet Received:   2016-11-06 09:00:39 PST
  Incoming Client Interface: ae0.3221225472
  Client Interface Svlan Id: 2000
  Client Interface Vlan Id: 1
  Server Ip Address:      3000::2
  Server Interface:       none
  Client Profile Name:    my-dual-stack
  Client Id Length:       10
  Client Id:              /0x00030001/0x00006401/0x0102
  Dual Stack Group:       my-dual-stack
  Dual Stack Peer Address: 100.20.0.10
```

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:db8:1111:2222::/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:db8:1111:2222::/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:db8:1111:2222::/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:db8:19::/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:db8:19::/32 31      79681 BOUND demux0.1073741825
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:db8:C9::/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:db8:19::/32 33         79681  BOUND ge-1/3/0.110
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:db8:C9::/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	<pre>show dhcpv6 server statistics <bulk-leasequery-connections> <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>></pre>
Release Information	<p>Command introduced in Junos OS Release 9.6.</p> <p>bulk-leasequery-connections option introduced in Junos OS Release 16.1.</p>
Description	Display extended Dynamic Host Configuration Protocol for IPv6 (DHCPv6) local server statistics.
Options	<p>bulk-leasequery-connections—(Optional) Display bulk leasequery statistics.</p> <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 439
List of Sample Output	<p>show dhcpv6 server statistics on page 485</p> <p>show dhcpv6 server statistics bulk-leasequery-connections on page 485</p>
Output Fields	<p>Table 22 on page 484 lists the output fields for the show dhcpv6 server statistics command. Output fields are listed in the approximate order in which they appear.</p>

Table 22: 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. • DHCPV6_LEASEQUERY—Number of DHCPv6 leasequery messages received.

Table 22: show dhcpv6 server statistics Output Fields (*continued*)

Field Name	Field Description
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. DHCPV6_LOGICAL_NAK—Number of logical NAK messages sent, signifying T1 and T2 timers with values of zero; subset of DHCPV6_REPLY counter. (Displays only at verbose level. DHC6_RECONFIGURE—Number of DHCPv6 RECONFIGURE PDUs transmitted. DHCPV6_LEASEQUERY_REPLY—Number of DHCPv6 leasequery replies transmitted to the DHCPv6 relay agent. DHCPV6_LEASEQUERY_DATA—Number of DHCPv6 LEASEQUERY-DATA packets transmitted. DHCPV6_LEASEQUERY_DONE—Number of DHCPv6 LEASEQUERY-DONE packets sent.

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
  DHCPV6_LEASEQUERY     0
```

```
Messages sent:
```

```
  DHCPV6_ADVERTISE      9
  DHCPV6_REPLY          5
  DHCPV6_RECONFIGURE    0
  DHCPV6_LEASEQUERY_REPLY 0
  DHCPV6_LEASEQUERY_DATA 0
  DHCPV6_LEASEQUERY_DONE 0
```

show dhcpv6 server statistics bulk-leasequery-connections

```
user@host> show dhcpv6 server statistics bulk-leasequery-connections
```

```
Total Accepted Connections:      0
Total Not-Accepted Connections:  0
Connections Closed due to Errors: 0
Connections Closed due to max-empty-replies: 0
In-flight Connections:           0
```

show interfaces (Aggregated Ethernet)

Syntax	<pre>show interfaces <i>aenumber</i> <brief detail extensive terse> <descriptions> <media> <snmp-index <i>snmp-index</i>> <statistics></pre>
Release Information	Command introduced before Junos OS Release 7.4.
Description	(M Series, T Series, and MX Series routers only) Display status information about the specified aggregated Fast Ethernet or Gigabit Ethernet interface.
Options	<p><i>aenumber</i>—Display standard information about the specified aggregated Fast Ethernet or Gigabit Ethernet interface.</p> <p>brief detail extensive terse—(Optional) Display the specified level of output.</p> <p>descriptions—(Optional) Display interface description strings.</p> <p>media—(Optional) Display media-specific information.</p> <p>snmp-index <i>snmp-index</i>—(Optional) Display information for the specified SNMP index of the interface.</p> <p>statistics—(Optional) Display static interface statistics.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> <i>Ethernet Interfaces Feature Guide for Routing Devices</i>
List of Sample Output	<p>show interfaces (Aggregated Ethernet) on page 491</p> <p>show interfaces brief (Aggregated Ethernet) on page 492</p> <p>show interfaces detail (Aggregated Ethernet) on page 492</p> <p>show interfaces extensive (Aggregated Ethernet) on page 493</p> <p>show interfaces extensive (Aggregated Ethernet with VLAN Stacking) on page 494</p>
Output Fields	Table 23 on page 486 lists the output fields for the show interfaces (Aggregated Ethernet) command. Output fields are listed in the approximate order in which they appear.

Table 23: Aggregated Ethernet show interfaces Output Fields

Field Name	Field Description	Level of Output
Physical Interface		
Physical interface	Name of the physical interface and state of the interface.	All levels

Table 23: Aggregated Ethernet show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Enabled	State of the physical interface. Possible values are described in the “Enabled Field” section under <i>Common Output Fields Description</i> .	All levels
Interface index	Index number of the physical interface, which reflects its initialization sequence.	All levels
SNMP ifIndex	SNMP index number for the physical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Link-level type	Encapsulation being used on the physical interface.	All levels
MTU	Maximum transmission unit size on the physical interface.	All levels
Speed	Speed at which the interface is running.	All levels
Loopback	Loopback status: Enabled or Disabled . If loopback is enabled, type of loopback: Local or Remote .	All levels
Source filtering	Source filtering status: Enabled or Disabled .	All levels
Flow control	Flow control status: Enabled or Disabled .	All levels
Minimum links needed	Number of child links that must be operational for the aggregate interface to be operational.	All levels
Device flags	Information about the physical device. Possible values are described in the “Device Flags” section under <i>Common Output Fields Description</i> .	All levels
Interface flags	Information about the interface. Possible values are described in the “Interfaces Flags” section under <i>Common Output Fields Description</i> .	All levels
Current address	Configured MAC address.	detail extensive
Hardware address	Hardware MAC address.	detail extensive
Last flapped	Date, time, and how long ago the interface went from down to up or from up to down. The format is Last flapped: year-month-day hours:minutes:seconds timezone (hours:minutes:seconds ago) . For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago) .	detail extensive
Input Rate	Input rate in bits per second (bps) and packets per second (pps).	None specified
Output Rate	Output rate in bps and pps.	None specified
Statistics last cleared	Time when the statistics for the interface were last set to zero.	detail extensive

Table 23: Aggregated Ethernet show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Traffic statistics	<p>Number and rate of bytes and packets received and transmitted on the physical interface.</p> <ul style="list-style-type: none"> • Input bytes—Number of bytes and rate, in bps, at which bytes are received on the interface. • Output bytes—Number of bytes and rate, in bps, at which bytes are transmitted on the interface. • Input packets—Number of packets and rate, in pps, at which packets are received on the interface. • Output packets—Number of packets and rate, in pps, at which packets are transmitted on the interface. 	detail extensive
Input errors	<p>Input errors on the interface:</p> <ul style="list-style-type: none"> • Errors—Sum of incoming frame aborts and frame check sequence (FCS) errors. • Drops—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's random early detection (RED) mechanism. • Framing errors—Number of packets received with an invalid frame checksum (FCS). • Runts—Number of frames received that are smaller than the runt threshold. • Giants—Number of frames received that are larger than the giant threshold. • Policed discards—Number of frames that the incoming packet match code discarded because they were not recognized or were not of interest. Usually, this field reports protocols that Junos OS does not handle. • Resource errors—Sum of transmit drops. 	detail extensive
Output errors	<p>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</p> <ul style="list-style-type: none"> • Carrier transitions —Number of times the interface has gone from down to up. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), then the cable, the far-end system, or the PIC is malfunctioning. • Errors—Sum of the outgoing frame aborts and FCS errors. • Drops—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism. • MTU errors—Number of packets whose size exceeded the MTU of the interface. • Resource errors—Sum of transmit drops. 	detail extensive

Table 23: Aggregated Ethernet show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
IPv6 transit statistics	<p>Number of IPv6 transit bytes and packets received and transmitted on the physical interface if IPv6 statistics tracking is enabled.</p> <ul style="list-style-type: none"> • Input bytes—Number of bytes received on the interface. • Output bytes—Number of bytes transmitted on the interface. • Input packets—Number of packets received on the interface. • Output packets—Number of packets transmitted on the interface. 	detail extensive
Queue counters	<p>CoS queue number and its associated user-configured forwarding class name.</p> <ul style="list-style-type: none"> • Queued packets—Number of queued packets. • Transmitted packets—Number of transmitted packets. • Dropped packets—Number of packets dropped by the ASIC's RED mechanism. <p>NOTE: In DPCs that are not of the enhanced type, such as DPC 40x 1GE R, DPCE 20x 1GE + 2x 10GE R, or DPCE 40x 1GE R, you might notice a discrepancy in the output of the show interfaces command because incoming packets might be counted in the Egress queues section of the output. This problem occurs on non-enhanced DPCs because the egress queue statistics are polled from IMQ (Inbound Message Queuing) block of the I-chip. The IMQ block does not differentiate between ingress and egress WAN traffic; as a result, the combined statistics are displayed in the egress queue counters on the Routing Engine. In a simple VPLS scenario, if there is no MAC entry in DMAC table (by sending unidirectional traffic), traffic is flooded and the input traffic is accounted in IMQ. For bidirectional traffic (MAC entry in DMAC table), if the outgoing interface is on the same I-chip then both ingress and egress statistics are counted in a combined way. If the outgoing interface is on a different I-chip or FPC, then only egress statistics are accounted in IMQ. This behavior is expected with non-enhanced DPCs</p>	detail extensive
Logical Interface		
Logical interface	Name of the logical interface.	All levels
Index	Index number of the logical interface (which reflects its initialization sequence).	detail extensive none
SNMP ifIndex	SNMP interface index number of the logical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Flags	Information about the logical interface. Possible values are described in the "Logical Interface Flags Field" section under <i>Common Output Fields Description</i> .	All levels
VLAN-Tag	Tag Protocol Identifier (TPID) and VLAN identifier.	All levels
Demux	<p>IP demultiplexing (demux) value that appears if this interface is used as the demux underlying interface. The output is one of the following:</p> <ul style="list-style-type: none"> • Source Family Inet • Destination Family Inet 	detail extensive none
Encapsulation	Encapsulation on the logical interface.	All levels

Table 23: Aggregated Ethernet show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Statistics	<p>Information about the number of packets, packets per second, number of bytes, and bytes per second on this aggregate interface.</p> <ul style="list-style-type: none"> • Bundle—Information about input and output bundle rates. • Link—(detail and extensive only) Information about specific links in the aggregate, including link state and input and output rates. • Adaptive Statistics—(extensive only) Information about adaptive load balancing counter statistics. <ul style="list-style-type: none"> • Adaptive Adjusts—Number of times traffic flow imbalance was corrected by implementation of adaptive load balancing. • Adaptive Scans—Number of times the link utilization on each member link of the AE bundle was scanned by for adaptive load balancing • Adaptive Tolerance—Tolerance level, in percentage, for load imbalance on link utilization on each member link of the AE bundle. • Adaptive Updates—Number of times traffic flow loads have been updated on an AE bundle. • Marker Statistics—(detail and extensive only) Information about 802.3ad marker protocol statistics on the specified links. <ul style="list-style-type: none"> • Marker Rx—Number of valid marker protocol data units (PDUs) received on this aggregation port. • Resp Tx—Number of marker response PDUs transmitted on this aggregation port. • Unknown Rx—Number of frames received that either carry the slow protocols Ethernet type value (43B.4) but contain an unknown PDU, or are addressed to the slow protocols group MAC address (43B.3) but do not carry the slow protocols Ethernet type. • Illegal Rx—Number of frames received that carry the slow protocols Ethernet type value (43B.4) but contain a badly formed PDU or an illegal value of protocol subtype (43B.4). 	detail extensive none
LACP info	<p>Link Aggregation Control Protocol (LACP) information for each aggregated interface.</p> <ul style="list-style-type: none"> • Role can be one of the following: <ul style="list-style-type: none"> • Actor—Local device participating in LACP negotiation. • Partner—Remote device participating in LACP negotiation. • System priority—Priority assigned to the system (by management or administrative policy), encoded as an unsigned integer. • System identifier—Actor or partner system ID, encoded as a MAC address. • Port priority—Priority assigned to the port by the actor or partner (by management or administrative policy), encoded as an unsigned integer. • Unknown Rx—Number of frames received that either carry the slow protocols Ethernet type value (43B.4) but contain an unknown protocol data unit (PDU), or are addressed to the slow protocols group MAC address (43B.3) but do not carry the slow protocols Ethernet type. • Port key—Operational key value assigned to the port by the actor or partner, encoded as an unsigned integer. 	

Table 23: Aggregated Ethernet show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
LACP Statistics	<p>LACP statistics for each aggregated interface.</p> <ul style="list-style-type: none"> • LACP Rx—LACP received counter that increments for each normal hello. • LACP Tx—Number of LACP transmit packet errors logged. • Unknown Rx—Number of unrecognized packet errors logged. • Illegal Rx—Number of invalid packets received. <p>NOTE: For LACP Rx and LACP Tx, Packet count is updated only on snmp timer expiry (30 secs).</p>	detail extensive none
<i>protocol-family</i>	Protocol family configured on the logical interface. Possible values are described in the "Protocol Field" section under <i>Common Output Fields Description</i> .	brief
Protocol	Protocol family configured on the logical interface. Possible values are described in the "Protocol Field" section under <i>Common Output Fields Description</i> .	detail extensive none
MTU	Maximum transmission unit size on the logical interface.	detail extensive none
Maximum labels	Maximum number of MPLS labels configured for the MPLS protocol family on the logical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Route Table	Routing table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.	detail extensive
Flags	Information about protocol family flags. Possible values are described in the "Family Flags Field" section under <i>Common Output Fields Description</i> .	detail extensive none
Mac-Validate Failures	Number of MAC address validation failures for packets and bytes. This field is displayed when MAC address validation is enabled for the logical interface.	detail extensive none
Addresses, Flags	Information about address flags. Possible values are described in the "Addresses Flags" section under <i>Common Output Fields Description</i> .	detail extensive none
Destination	IP address of the remote side of the connection.	detail extensive none
Local	IP address of the logical interface.	detail extensive none
Broadcast	Broadcast address of the logical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive

Sample Output

show interfaces (Aggregated Ethernet)

```
user@host> show interfaces ae0
```

```

Physical interface: ae0, Enabled, Physical link is Up
Interface index: 153, SNMP ifIndex: 59
Link-level type: Ethernet, MTU: 1514, Speed: 300mbps, Loopback: Disabled,
Source filtering: Disabled, Flow control: Disabled, Minimum links needed: 1
Device flags : Present Running
Interface flags: SNMP-Traps 16384
Current address: 00:00:5e:00:53:f0, Hardware address: 00:00:5e:00:53:f0
Last flapped : Never
Input rate : 0 bps (0 pps)
Output rate : 0 bps (0 pps)

Logical interface ae0.0 (Index 72) (SNMP ifIndex 60)
Flags: SNMP-Traps 16384 Encapsulation: ENET2
Statistics Packets pps Bytes bps
Bundle:
  Input : 0 0 0 0
  Output: 0 0 0 0
Protocol inet, MTU: 1500
Flags: None
Addresses, Flags: Is-Preferred Is-Primary
Destination: 203.0.113/24, Local: 203.0.113.2, Broadcast: 10.100.1.255

```

show interfaces brief (Aggregated Ethernet)

```

user@host> show interfaces ae0 brief
Physical interface: ae0, Enabled, Physical link is Up
Link-level type: Ethernet, MTU: 1514, Speed: 300mbps, Loopback: Disabled,
Source filtering: Disabled, Flow control: Disabled
Device flags : Present Running
Interface flags: SNMP-Traps 16384

Logical interface ae0.0
Flags: SNMP-Traps 16384 Encapsulation: ENET2
inet 203.0.113.2/24

```

show interfaces detail (Aggregated Ethernet)

```

user@host> show interfaces ae0 detail
Physical interface: ae0, Enabled, Physical link is Up
Interface index: 153, SNMP ifIndex: 59, Generation: 36
Link-level type: Ethernet, MTU: 1514, Speed: 300mbps, Loopback: Disabled,
Source filtering: Disabled, Flow control: Disabled, Minimum links needed: 1
Device flags : Present Running
Interface flags: SNMP-Traps 16384
Current address: 00:00:5e:00:53:f0, Hardware address: 00:00:5e:00:53:f0
Last flapped : Never
Statistics last cleared: Never
Traffic statistics:
Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps
Queue counters: Queued packets Transmitted packets Dropped packets

0 best-effort 7375 7375 0
1 expedited-fo 0 0 0
2 assured-forw 0 0 0

```

```
3 network-cont                2268                2268                0
```

```
Logical interface ae0.0 (Index 72) (SNMP ifIndex 60) (Generation 18)
Flags: SNMP-Traps 16384 Encapsulation: ENET2
Statistics          Packets          pps          Bytes          bps
Bundle:
  Input :            0            0            0            0
  Output:            0            0            0            0
Link:
  fe-0/1/0.0
    Input :            0            0            0            0
    Output:            0            0            0            0
  fe-0/1/2.0
    Input :            0            0            0            0
    Output:            0            0            0            0
  fe-0/1/3.0
    Input :            0            0            0            0
    Output:            0            0            0            0
Marker Statistics:  Marker Rx      Resp Tx      Unknown Rx      Illegal Rx
fe-0/1/0.0          0            0            0            0
fe-0/1/2.0          0            0            0            0
fe-0/1/3.0          0            0            0            0
Protocol inet, MTU: 1500, Generation: 37, Route table: 0
Flags: Is-Primary, Mac-Validate-Strict
Mac-Validate Failures: Packets: 0, Bytes: 0
Destination: 203.0.113/24, Local: 203.0.113.2, Broadcast: 203.0.113.255,

Generation: 49
```

show interfaces extensive (Aggregated Ethernet)

```
user@host> show interfaces ae0 extensive
Physical interface: ae0, Enabled, Physical link is Up
Interface index: 153, SNMP ifIndex: 59, Generation: 36
Link-level type: Ethernet, MTU: 1514, Speed: 300mbps, Loopback: Disabled,
Source filtering: Disabled, Flow control: Disabled, Minimum links needed: 1
Device flags : Present Running
Interface flags: SNMP-Traps 16384
Current address: 00:00:5e:00:53:f0, Hardware address: 00:00:5e:00:53:f0
Last flapped : Never
Statistics last cleared: Never
Traffic statistics:
Input bytes :            60            0 bps
Output bytes :            0            0 bps
Input packets:            1            0 pps
Output packets:            0            0 pps
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
Policed discards: 0, Resource errors: 0
Output errors:
Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0,
Resource errors: 0
Queue counters:      Queued packets  Transmitted packets  Dropped packets
0 best-effort        7375                7375                0
1 expedited-fo        0                   0                   0
2 assured-forw        0                   0                   0
```

```
3 network-cont                2268                2268                0
```

Logical interface ae0.0 (Index 72) (SNMP ifIndex 60) (Generation 18)

Flags: SNMP-Traps 16384 Encapsulation: ENET2

Statistics	Packets	pps	Bytes	bps
------------	---------	-----	-------	-----

Bundle:

Input :	1	0	60	0
---------	---	---	----	---

Output:	0	0	0	0
---------	---	---	---	---

Adaptive Statistics:

Adaptive Adjusts:	0
-------------------	---

Adaptive Scans :	0
------------------	---

Adaptive Updates:	0
-------------------	---

Link:

fe-0/1/0.0

Input :	0	0	0	0
---------	---	---	---	---

Output:	0	0	0	0
---------	---	---	---	---

fe-0/1/2.0

Input :	0	0	0	0
---------	---	---	---	---

Output:	0	0	0	0
---------	---	---	---	---

fe-0/1/3.0

Input :	1	0	60	0
---------	---	---	----	---

Output:	0	0	0	0
---------	---	---	---	---

LACP info:	Role	System	System	Port	Port	Port
------------	------	--------	--------	------	------	------

priority	identifier	priority	number	key
----------	------------	----------	--------	-----

fe-1/0/3.0	Actor	127	00:00:5e:00:53:85	127	2	1
------------	-------	-----	-------------------	-----	---	---

fe-1/0/3.0	Partner	127	00:00:5e:00:53:c3	127	1	1
------------	---------	-----	-------------------	-----	---	---

LACP Statistics:	LACP Rx	LACP Tx	Unknown Rx	Illegal Rx
------------------	---------	---------	------------	------------

fe-1/0/3.0	3188	3186	0	0
------------	------	------	---	---

Marker Statistics:	Marker Rx	Resp Tx	Unknown Rx	Illegal Rx
--------------------	-----------	---------	------------	------------

fe-0/1/0.0	0	0	0	0
------------	---	---	---	---

fe-0/1/2.0	0	0	0	0
------------	---	---	---	---

fe-0/1/3.0	0	0	0	0
------------	---	---	---	---

Protocol inet, MTU: 1500, Generation: 37, Route table: 0

Flags: None

Addresses, Flags: Is-Preferred Is-Primary

Destination: 203.0.113/24, Local: 203.0.113.2, Broadcast: 203.0.113.255,

Generation: 49

show interfaces extensive (Aggregated Ethernet with VLAN Stacking)

```
user@host> show interfaces ae0 detail
```

Physical interface: ae0, Enabled, Physical link is Up

Interface index: 155, SNMP ifIndex: 48, Generation: 186

Link-level type: 52, MTU: 1518, Speed: 2000mbps, 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: 00:00:5e:00:53:3f, Hardware address: 00:00:5e:00:53:3f

Last flapped : Never

Statistics last cleared: Never

Traffic statistics:

Input bytes :	2406875	40152 bps
---------------	---------	-----------

Output bytes :	1124470	22056 bps
----------------	---------	-----------

Input packets:	5307	5 pps
----------------	------	-------

```

Output packets:          13295          21 pps
IPv6 transit statistics:
  Input bytes :          0
  Output bytes :          0
  Input packets:         0
  Output packets:        0
Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards:
0, Resource errors: 0
Output errors:
  Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors:
0
Ingress queues: 4 supported, 4 in use
Queue counters:      Queued packets  Transmitted packets      Dropped packets

  0 best-effort          0          859777          0
  1 expedited-fo         0           0          0
  2 assured-forw         0           0          0
  3 network-cont         0           0          0

Egress queues: 4 supported, 4 in use
Queue counters:      Queued packets  Transmitted packets      Dropped packets

  0 best-effort          0        1897615          0
  1 expedited-fo         0           0          0
  2 assured-forw         0           0          0
  3 network-cont         0        662505          0

Logical interface ae0.451 (Index 69) (SNMP ifIndex 167) (Generation 601)
Flags: SNMP-Traps VLAN-Tag [ 0x8100.451 ] Encapsulation: VLAN-VPLS
Statistics      Packets      pps      Bytes      bps
Bundle:
  Input :         289         0        25685        376
  Output:        1698         4       130375       3096
Link:
  ge-1/2/0.451
    Input :         289         0        25685        376
    Output:          0         0           0           0
  ge-1/2/1.451
    Input :          0         0           0           0
    Output:        1698         4       130375       3096
Marker Statistics:  Marker Rx      Resp Tx      Unknown Rx      Illegal Rx
  ge-1/2/0.451           0           0           0           0
  ge-1/2/1.451           0           0           0           0
Protocol vpls, MTU: 1518, Generation: 849, Route table: 3
Flags: Is-Primary

Logical interface ae0.452 (Index 70) (SNMP ifIndex 170) (Generation 602)
Flags: SNMP-Traps VLAN-Tag [ 0x8100.452 ] Encapsulation: VLAN-VPLS
Statistics      Packets      pps      Bytes      bps
Bundle:
  Input :          293         1        26003       1072
  Output:        1694         3       130057       2400
Link:

```

```
ge-1/2/0.452
  Input :      293      1      26003      1072
  Output:    1694      3     130057      2400
ge-1/2/1.452
  Input :      0      0      0      0
  Output:      0      0      0      0
Marker Statistics:  Marker Rx      Resp Tx      Unknown Rx      Illegal Rx
ge-1/2/0.452      0      0      0      0
ge-1/2/1.452      0      0      0      0
Protocol vpls, MTU: 1518, Generation: 850, Route table: 3
Flags: None
...
```

show interfaces (Fast Ethernet)

Syntax `show interfaces interface-type`
`<brief | detail | extensive | terse>`
`<descriptions>`
`<media>`
`<snmp-index snmp-index>`
`<statistics>`

Release Information Command introduced before Junos OS Release 7.4.

Description Display status information about the specified Fast Ethernet interface.

Options *interface-type*—On M Series and T Series routers, the interface type is **fe-fpc/pic/port**.

brief | detail | extensive | terse—(Optional) Display the specified level of output.

descriptions—(Optional) Display interface description strings.

media—(Optional) Display media-specific information about network interfaces.

snmp-index *snmp-index*—(Optional) Display information for the specified SNMP index of the interface.

statistics—(Optional) Display static interface statistics.

Required Privilege Level view

List of Sample Output [show interfaces \(Fast Ethernet\) on page 510](#)
[show interfaces brief \(Fast Ethernet\) on page 511](#)
[show interfaces detail \(Fast Ethernet\) on page 511](#)
[show interfaces extensive \(Fast Ethernet\) on page 511](#)

Output Fields [Table 24 on page 497](#) lists the output fields for the **show interfaces** (Fast Ethernet) command. Output fields are listed in the approximate order in which they appear.

Table 24: show interfaces Fast Ethernet Output Fields

Field Name	Field Description	Level of Output
Physical Interface		
Physical interface	Name of the physical interface.	All levels
Enabled	State of the interface. Possible values are described in the “Enabled Field” section under <i>Common Output Fields Description</i> .	All levels
Interface index	Index number of the physical interface, which reflects its initialization sequence.	detail extensive none
SNMP ifIndex	SNMP index number for the physical interface.	detail extensive none

Table 24: show interfaces Fast Ethernet Output Fields (*continued*)

Field Name	Field Description	Level of Output
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Link-level type	Encapsulation being used on the physical interface.	All levels
MTU	Maximum transmission unit size on the physical interface.	All levels
Link-mode	Type of link connection configured for the physical interface: Full-duplex or Half-duplex	extensive
Speed	Speed at which the interface is running.	All levels
Loopback	Loopback status: Enabled or Disabled . If loopback is enabled, type of loopback: Local or Remote .	All levels
Source filtering	Source filtering status: Enabled or Disabled .	All levels
LAN-PHY mode	10-Gigabit Ethernet interface operating in Local Area Network Physical Layer Device (LAN PHY) mode. LAN PHY allows 10-Gigabit Ethernet wide area links to use existing Ethernet applications.	All levels
WAN-PHY mode	10-Gigabit Ethernet interface operating in Wide Area Network Physical Layer Device (WAN PHY) mode. WAN PHY allows 10-Gigabit Ethernet wide area links to use fiber-optic cables and other devices intended for SONET/SDH.	All levels
Unidirectional	Unidirectional link mode status for 10-Gigabit Ethernet interface: Enabled or Disabled for parent interface; Rx-only or Tx-only for child interfaces.	All levels
Flow control	Flow control status: Enabled or Disabled .	All levels
Auto-negotiation	(Gigabit Ethernet interfaces) Autonegotiation status: Enabled or Disabled .	All levels
Remote-fault	(Gigabit Ethernet interfaces) Remote fault status: <ul style="list-style-type: none"> • Online—Autonegotiation is manually configured as online. • Offline—Autonegotiation is manually configured as offline. 	All levels
Device flags	Information about the physical device. Possible values are described in the "Device Flags" section under <i>Common Output Fields Description</i> .	All levels
Interface flags	Information about the interface. Possible values are described in the "Interface Flags" section under <i>Common Output Fields Description</i> .	All levels
Link flags	Information about the link. Possible values are described in the "Links Flags" section under <i>Common Output Fields Description</i> .	All levels
Wavelength	(10-Gigabit Ethernet dense wavelength-division multiplexing [DWDM] interfaces) Displays the configured wavelength, in nanometers (nm).	All levels

Table 24: show interfaces Fast Ethernet Output Fields (*continued*)

Field Name	Field Description	Level of Output
Frequency	(10-Gigabit Ethernet DWDM interfaces only) Displays the frequency associated with the configured wavelength, in terahertz (THz).	All levels
CoS queues	Number of CoS queues configured.	detail extensive none
Schedulers	(GigabitEthernet intelligent queuing 2 (IQ2) interfaces only) Number of CoS schedulers configured.	extensive
Hold-times	Current interface hold-time up and hold-time down, in milliseconds.	detail extensive
Current address	Configured MAC address.	detail extensive none
Hardware address	Hardware MAC address.	detail extensive none
Last flapped	Date, time, and how long ago the interface went from down to up. The format is Last flapped: year-month-day hour:minute:second:timezone (hour:minute:second ago) . For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago) .	detail extensive none
Input Rate	Input rate in bits per second (bps) and packets per second (pps).	None specified
Output Rate	Output rate in bps and pps.	None specified
Statistics last cleared	Time when the statistics for the interface were last set to zero.	detail extensive
Traffic statistics	<p>Number and rate of bytes and packets received and transmitted on the physical interface.</p> <ul style="list-style-type: none"> • Input bytes—Number of bytes received on the interface • Output bytes—Number of bytes transmitted on the interface. • Input packets—Number of packets received on the interface. • Output packets—Number of packets transmitted on the interface. <p>Gigabit Ethernet and 10-Gigabit Ethernet IQ PICs count the overhead and CRC bytes.</p> <p>For Gigabit Ethernet IQ PICs, the input byte counts vary by interface type. For more information, see Table 31 under the <i>show interfaces (10-Gigabit Ethernet)</i> command.</p>	detail extensive

Table 24: show interfaces Fast Ethernet Output Fields (*continued*)

Field Name	Field Description	Level of Output
Input errors	<p>Input errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</p> <ul style="list-style-type: none"> • Errors—Sum of the incoming frame aborts and FCS errors. • Drops—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism. • Framing errors—Number of packets received with an invalid frame checksum (FCS). • Runts—Number of frames received that are smaller than the runt threshold. • Policed discards—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle. • L3 incompletes—Number of incoming packets discarded because they failed Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with less than 20 bytes of available IP header is discarded. L3 incomplete errors can be ignored by configuring the ignore-l3-incompletes statement. • L2 channel errors—Number of times the software did not find a valid logical interface for an incoming frame. • L2 mismatch timeouts—Number of malformed or short packets that caused the incoming packet handler to discard the frame as unreadable. • FIFO errors—Number of FIFO errors in the receive direction that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning. • Resource errors—Sum of transmit drops. 	extensive

Table 24: show interfaces Fast Ethernet Output Fields (*continued*)

Field Name	Field Description	Level of Output
Output errors	<p>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</p> <ul style="list-style-type: none"> • Carrier transitions—Number of times the interface has gone from down to up. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC or PIM is malfunctioning. • Errors—Sum of the outgoing frame aborts and FCS errors. • Drops—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism. • Collisions—Number of Ethernet collisions. The Gigabit Ethernet PIC supports only full-duplex operation, so for Gigabit Ethernet PICs, this number should always remain 0. If it is nonzero, there is a software bug. • Aged packets—Number of packets that remained in shared packet SDRAM so long that the system automatically purged them. The value in this field should never increment. If it does, it is most likely a software bug or possibly malfunctioning hardware. • FIFO errors—Number of FIFO errors in the send direction as reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning. • HS link CRC errors—Number of errors on the high-speed links between the ASICs responsible for handling the router interfaces. • MTU errors—Number of packets whose size exceeded the MTU of the interface. • Resource errors—Sum of transmit drops. 	extensive
Egress queues	<p>Total number of egress queues supported on the specified interface.</p> <p>NOTE: In DPCs that are not of the enhanced type, such as DPC 40x 1GE R, DPCE 20x 1GE + 2x 10GE R, or DPCE 40x 1GE R, you might notice a discrepancy in the output of the show interfaces command because incoming packets might be counted in the Egress queues section of the output. This problem occurs on non-enhanced DPCs because the egress queue statistics are polled from IMQ (Inbound Message Queuing) block of the I-chip. The IMQ block does not differentiate between ingress and egress WAN traffic; as a result, the combined statistics are displayed in the egress queue counters on the Routing Engine. In a simple VPLS scenario, if there is no MAC entry in DMAC table (by sending unidirectional traffic), traffic is flooded and the input traffic is accounted in IMQ. For bidirectional traffic (MAC entry in DMAC table), if the outgoing interface is on the same I-chip then both ingress and egress statistics are counted in a combined way. If the outgoing interface is on a different I-chip or FPC, then only egress statistics are accounted in IMQ. This behavior is expected with non-enhanced DPCs</p>	detail extensive
Queue counters (Egress)	<p>CoS queue number and its associated user-configured forwarding class name.</p> <ul style="list-style-type: none"> • Queued packets—Number of queued packets. • Transmitted packets—Number of transmitted packets. • Dropped packets—Number of packets dropped by the ASIC's RED mechanism. 	detail extensive

Table 24: show interfaces Fast Ethernet Output Fields (*continued*)

Field Name	Field Description	Level of Output
Ingress queues	Total number of ingress queues supported on the specified interface. Displayed on IQ2 interfaces.	extensive
Queue counters (Ingress)	CoS queue number and its associated user-configured forwarding class name. Displayed on IQ2 interfaces. <ul style="list-style-type: none"> • Queued packets—Number of queued packets. • Transmitted packets—Number of transmitted packets. • Dropped packets—Number of packets dropped by the ASIC's RED mechanism. 	extensive
Active alarms and Active defects	Ethernet-specific defects that can prevent the interface from passing packets. When a defect persists for a certain amount of time, it is promoted to an alarm. Based on the routing device configuration, an alarm can ring the red or yellow alarm bell on the routing device, or turn on the red or yellow alarm LED on the craft interface. These fields can contain the value None or Link . <ul style="list-style-type: none"> • None—There are no active defects or alarms. • Link—Interface has lost its link state, which usually means that the cable is unplugged, the far-end system has been turned off, or the PIC is malfunctioning. 	detail extensive none
OTN FEC statistics	The forward error correction (FEC) counters provide the following statistics: <ul style="list-style-type: none"> • Corrected Errors—The count of corrected errors in the last second. • Corrected Error Ratio—The corrected error ratio in the last 25 seconds. For example, 1e-7 is 1 error per 10 million bits. 	
PCS statistics	(10-Gigabit Ethernet interfaces) Displays Physical Coding Sublayer (PCS) fault conditions from the WAN PHY or the LAN PHY device. <ul style="list-style-type: none"> • Bit errors—The number of seconds during which at least one bit error rate (BER) occurred while the PCS receiver is operating in normal mode. • Errored blocks—The number of seconds when at least one errored block occurred while the PCS receiver is operating in normal mode. 	detail extensive

Table 24: show interfaces Fast Ethernet Output Fields (*continued*)

Field Name	Field Description	Level of Output
MAC statistics	<p>Receive and Transmit statistics reported by the PIC's MAC subsystem, including the following:</p> <ul style="list-style-type: none"> • Total octets and total packets—Total number of octets and packets. For Gigabit Ethernet IQ PICs, the received octets count varies by interface type. For more information, see Table 31 under the <i>show interfaces (10-Gigabit Ethernet)</i> command. • Unicast packets, Broadcast packets, and Multicast packets—Number of unicast, broadcast, and multicast packets. • CRC/Align errors—Total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). • FIFO error—Number of FIFO errors that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC or a cable is probably malfunctioning. • MAC control frames—Number of MAC control frames. • MAC pause frames—Number of MAC control frames with pause operational code. • Oversized frames—Number of frames that exceed 1518 octets. • Jabber frames—Number of frames that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment error. This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition in which any packet exceeds 20 ms. The allowed range to detect jabber is from 20 ms to 150 ms. • Fragment frames—Total number of packets that were less than 64 octets in length (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment error. Fragment frames normally increment because both runts (which are normal occurrences caused by collisions) and noise hits are counted. • VLAN tagged frames—Number of frames that are VLAN tagged. The system uses the TPID of 0x8100 in the frame to determine whether a frame is tagged or not. • Code violations—Number of times an event caused the PHY to indicate "Data reception error" or "invalid data symbol error." 	extensive
OTN Received Overhead Bytes	APS/PCC0: 0x02, APS/PCC1: 0x11, APS/PCC2: 0x47, APS/PCC3: 0x58 Payload Type: 0x08	extensive
OTN Transmitted Overhead Bytes	APS/PCC0: 0x00, APS/PCC1: 0x00, APS/PCC2: 0x00, APS/PCC3: 0x00 Payload Type: 0x08	extensive

Table 24: show interfaces Fast Ethernet Output Fields (*continued*)

Field Name	Field Description	Level of Output
Filter statistics	<p>Receive and Transmit statistics reported by the PIC's MAC address filter subsystem. The filtering is done by the content-addressable memory (CAM) on the PIC. The filter examines a packet's source and destination MAC addresses to determine whether the packet should enter the system or be rejected.</p> <ul style="list-style-type: none"> • Input packet count—Number of packets received from the MAC hardware that the filter processed. • Input packet rejects—Number of packets that the filter rejected because of either the source MAC address or the destination MAC address. • Input DA rejects—Number of packets that the filter rejected because the destination MAC address of the packet is not on the accept list. It is normal for this value to increment. When it increments very quickly and no traffic is entering the routing device from the far-end system, either there is a bad ARP entry on the far-end system, or multicast routing is not on and the far-end system is sending many multicast packets to the local routing device (which the routing device is rejecting). • Input SA rejects—Number of packets that the filter rejected because the source MAC address of the packet is not on the accept list. The value in this field should increment only if source MAC address filtering has been enabled. If filtering is enabled, if the value increments quickly, and if the system is not receiving traffic that it should from the far-end system, it means that the user-configured source MAC addresses for this interface are incorrect. • Output packet count—Number of packets that the filter has given to the MAC hardware. • Output packet pad count—Number of packets the filter padded to the minimum Ethernet size (60 bytes) before giving the packet to the MAC hardware. Usually, padding is done only on small ARP packets, but some very small IP packets can also require padding. If this value increments rapidly, either the system is trying to find an ARP entry for a far-end system that does not exist or it is misconfigured. • Output packet error count—Number of packets with an indicated error that the filter was given to transmit. These packets are usually aged packets or are the result of a bandwidth problem on the FPC hardware. On a normal system, the value of this field should not increment. • CAM destination filters, CAM source filters—Number of entries in the CAM dedicated to destination and source MAC address filters. There can only be up to 64 source entries. If source filtering is disabled, which is the default, the values for these fields should be 0. 	extensive
PMA PHY	<p>(10-Gigabit Ethernet interfaces, WAN PHY mode) SONET error information:</p> <ul style="list-style-type: none"> • Seconds—Number of seconds the defect has been active. • Count—Number of times that the defect has gone from inactive to active. • State—State of the error. Any state other than OK indicates a problem. <p>Subfields are:</p> <ul style="list-style-type: none"> • PHY Lock—Phase-locked loop • PHY Light—Loss of optical signal 	extensive

Table 24: show interfaces Fast Ethernet Output Fields (*continued*)

Field Name	Field Description	Level of Output
WIS section	<p>(10-Gigabit Ethernet interfaces, WAN PHY mode) SONET error information:</p> <ul style="list-style-type: none"> • Seconds—Number of seconds the defect has been active. • Count—Number of times that the defect has gone from inactive to active. • State—State of the error. Any state other than OK indicates a problem. <p>Subfields are:</p> <ul style="list-style-type: none"> • BIP-B1—Bit interleaved parity for SONET section overhead • SEF—Severely errored framing • LOL—Loss of light • LOF—Loss of frame • ES-S—Errored seconds (section) • SES-S—Severely errored seconds (section) • SEFS-S—Severely errored framing seconds (section) 	extensive
WIS line	<p>(10-Gigabit Ethernet interfaces, WAN PHY mode) Active alarms and defects, plus counts of specific SONET errors with detailed information.</p> <ul style="list-style-type: none"> • Seconds—Number of seconds the defect has been active. • Count—Number of times that the defect has gone from inactive to active. • State—State of the error. State other than OK indicates a problem. <p>Subfields are:</p> <ul style="list-style-type: none"> • BIP-B2—Bit interleaved parity for SONET line overhead • REI-L—Remote error indication (near-end line) • RDI-L—Remote defect indication (near-end line) • AIS-L—Alarm indication signal (near-end line) • BERR-SF—Bit error rate fault (signal failure) • BERR-SD—Bit error rate defect (signal degradation) • ES-L—Errored seconds (near-end line) • SES-L—Severely errored seconds (near-end line) • UAS-L—Unavailable seconds (near-end line) • ES-LFE—Errored seconds (far-end line) • SES-LFE—Severely errored seconds (far-end line) • UAS-LFE—Unavailable seconds (far-end line) 	extensive

Table 24: show interfaces Fast Ethernet Output Fields (*continued*)

Field Name	Field Description	Level of Output
WIS path	<p>(10-Gigabit Ethernet interfaces, WAN PHY mode) Active alarms and defects, plus counts of specific SONET errors with detailed information.</p> <ul style="list-style-type: none"> • Seconds—Number of seconds the defect has been active. • Count—Number of times that the defect has gone from inactive to active. • State—State of the error. Any state other than OK indicates a problem. <p>Subfields are:</p> <ul style="list-style-type: none"> • BIP-B3—Bit interleaved parity for SONET section overhead • REI-P—Remote error indication • LOP-P—Loss of pointer (path) • AIS-P—Path alarm indication signal • RDI-P—Path remote defect indication • UNEQ-P—Path unequipped • PLM-P—Path payload (signal) label mismatch • ES-P—Errored seconds (near-end STS path) • SES-P—Severely errored seconds (near-end STS path) • UAS-P—Unavailable seconds (near-end STS path) • SES-PFE—Severely errored seconds (far-end STS path) • UAS-PFE—Unavailable seconds (far-end STS path) 	extensive

Table 24: show interfaces Fast Ethernet Output Fields (*continued*)

Field Name	Field Description	Level of Output
Autonegotiation information	<p>Information about link autonegotiation.</p> <ul style="list-style-type: none"> • Negotiation status: <ul style="list-style-type: none"> • Incomplete—Ethernet interface has the speed or link mode configured. • No autonegotiation—Remote Ethernet interface has the speed or link mode configured, or does not perform autonegotiation. • Complete—Ethernet interface is connected to a device that performs autonegotiation and the autonegotiation process is successful. • Link partner status—OK when Ethernet interface is connected to a device that performs autonegotiation and the autonegotiation process is successful. • Link partner: <ul style="list-style-type: none"> • Link mode—Depending on the capability of the attached Ethernet device, either Full-duplex or Half-duplex. • Flow control—Types of flow control supported by the remote Ethernet device. For Fast Ethernet interfaces, the type is None. For Gigabit Ethernet interfaces, types are Symmetric (link partner supports PAUSE on receive and transmit), Asymmetric (link partner supports PAUSE on transmit), and Symmetric/Asymmetric (link partner supports both PAUSE on receive and transmit or only PAUSE receive). • Remote fault—Remote fault information from the link partner—Failure indicates a receive link error. OK indicates that the link partner is receiving. Negotiation error indicates a negotiation error. Offline indicates that the link partner is going offline. • Local resolution—Information from the link partner: <ul style="list-style-type: none"> • Flow control—Types of flow control supported by the remote Ethernet device. For Gigabit Ethernet interfaces, types are Symmetric (link partner supports PAUSE on receive and transmit), Asymmetric (link partner supports PAUSE on transmit), and Symmetric/Asymmetric (link partner supports both PAUSE on receive and transmit or only PAUSE receive). • Remote fault—Remote fault information. Link OK (no error detected on receive), Offline (local interface is offline), and Link Failure (link error detected on receive). 	extensive
Received path trace, Transmitted path trace	<p>(10-Gigabit Ethernet interfaces, WAN PHY mode) SONET/SDH interfaces allow path trace bytes to be sent inband across the SONET/SDH link. Juniper Networks and other routing device manufacturers use these bytes to help diagnose misconfigurations and network errors by setting the transmitted path trace message so that it contains the system hostname and name of the physical interface. The received path trace value is the message received from the routing device at the other end of the fiber. The transmitted path trace value is the message that this routing device transmits.</p>	extensive
Packet Forwarding Engine configuration	<p>Information about the configuration of the Packet Forwarding Engine:</p> <ul style="list-style-type: none"> • Destination slot—FPC slot number. 	extensive

Table 24: show interfaces Fast Ethernet Output Fields (*continued*)

Field Name	Field Description	Level of Output
CoS information	Information about the CoS queue for the physical interface. <ul style="list-style-type: none"> • CoS transmit queue—Queue number and its associated user-configured forwarding class name. • Bandwidth %—Percentage of bandwidth allocated to the queue. • Bandwidth bps—Bandwidth allocated to the queue (in bps). • Buffer %—Percentage of buffer space allocated to the queue. • Buffer usec—Amount of buffer space allocated to the queue, in microseconds. This value is nonzero only if the buffer size is configured in terms of time. • Priority—Queue priority: low or high. • Limit—Displayed if rate limiting is configured for the queue. Possible values are none and exact. If exact is configured, the queue transmits only up to the configured bandwidth, even if excess bandwidth is available. If none is configured, the queue transmits beyond the configured bandwidth if bandwidth is available. 	extensive
Logical Interface		
Logical interface	Name of the logical interface.	All levels
Index	Index number of the logical interface, which reflects its initialization sequence.	detail extensive none
SNMP ifIndex	SNMP interface index number for the logical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Flags	Information about the logical interface. Possible values are described in the “Logical Interface Flags” section under <i>Common Output Fields Description</i> .	All levels
VLAN-Tag	Rewrite profile applied to incoming or outgoing frames on the outer (Out) VLAN tag or for both the outer and inner (In) VLAN tags. <ul style="list-style-type: none"> • push—An outer VLAN tag is pushed in front of the existing VLAN tag. • pop—The outer VLAN tag of the incoming frame is removed. • swap—The outer VLAN tag of the incoming frame is overwritten with the user specified VLAN tag information. • push-pop—An outer VLAN tag is pushed in front of the existing VLAN tag, and then removed. • push-push—Two VLAN tags are pushed in from the incoming frame. • swap-push—The outer VLAN tag of the incoming frame is replaced by a user-specified VLAN tag value. A user-specified outer VLAN tag is pushed in front. The outer tag becomes an inner tag in the final frame. • swap-swap—Both the inner and the outer VLAN tags of the incoming frame are replaced by the user specified VLAN tag value. • pop-swap—The outer VLAN tag of the incoming frame is removed, and the inner VLAN tag of the incoming frame is replaced by the user-specified VLAN tag value. The inner tag becomes the outer tag in the final frame. • pop-pop—Both the outer and inner VLAN tags of the incoming frame are removed. 	brief detail extensive none

Table 24: show interfaces Fast Ethernet Output Fields (*continued*)

Field Name	Field Description	Level of Output
Demux:	IP demultiplexing (demux) value that appears if this interface is used as the demux underlying interface. The output is one of the following: <ul style="list-style-type: none"> Source Family Inet Destination Family Inet 	detail extensive none
Encapsulation	Encapsulation on the logical interface.	All levels
Protocol	Protocol family. Possible values are described in the “Protocol Field” section under <i>Common Output Fields Description</i> .	detail extensive none
MTU	Maximum transmission unit size on the logical interface.	detail extensive none
Maximum labels	Maximum number of MPLS labels configured for the MPLS protocol family on the logical interface.	detail extensive none
Traffic statistics	Number and rate of bytes and packets received and transmitted on the specified interface set. <ul style="list-style-type: none"> Input bytes, Output bytes—Number of bytes received and transmitted on the interface set Input packets, Output packets—Number of packets received and transmitted on the interface set. 	detail extensive
IPv6 transit statistics	Number of IPv6 transit bytes and packets received and transmitted on the logical interface if IPv6 statistics tracking is enabled.	extensive
Local statistics	Number and rate of bytes and packets destined to the routing device.	extensive
Transit statistics	Number and rate of bytes and packets transiting the switch. <p>NOTE: For Gigabit Ethernet intelligent queuing 2 (IQ2) interfaces, the logical interface egress statistics might not accurately reflect the traffic on the wire when output shaping is applied. Traffic management output shaping might drop packets after they are tallied by the Output bytes and Output packets interface counters. However, correct values display for both of these egress statistics when per-unit scheduling is enabled for the Gigabit Ethernet IQ2 physical interface, or when a single logical interface is actively using a shared scheduler.</p>	extensive
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Route Table	Route table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.	detail extensive none
Flags	Information about protocol family flags. Possible values are described in the “Family Flags” section under <i>Common Output Fields Description</i> .	detail extensive
Donor interface	(Unnumbered Ethernet) Interface from which an unnumbered Ethernet interface borrows an IPv4 address.	detail extensive none

Table 24: show interfaces Fast Ethernet Output Fields (*continued*)

Field Name	Field Description	Level of Output
Preferred source address	(Unnumbered Ethernet) Secondary IPv4 address of the donor loopback interface that acts as the preferred source address for the unnumbered Ethernet interface.	detail extensive none
Input Filters	Names of any input filters applied to this interface. If you specify a precedence value for any filter in a dynamic profile, filter precedence values appear in parenthesis next to all interfaces.	detail extensive
Output Filters	Names of any output filters applied to this interface. If you specify a precedence value for any filter in a dynamic profile, filter precedence values appear in parenthesis next to all interfaces.	detail extensive
Mac-Validate Failures	Number of MAC address validation failures for packets and bytes. This field is displayed when MAC address validation is enabled for the logical interface.	detail extensive none
Addresses, Flags	Information about the address flags. Possible values are described in the “Addresses Flags” section under <i>Common Output Fields Description</i> .	detail extensive none
<i>protocol-family</i>	Protocol family configured on the logical interface. If the protocol is inet , the IP address of the interface is also displayed.	brief
Flags	Information about address flag (possible values are described in the “Addresses Flags” section under <i>Common Output Fields Description</i>).	detail extensive none
Destination	IP address of the remote side of the connection.	detail extensive none
Local	IP address of the logical interface.	detail extensive none
Broadcast	Broadcast address of the logical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive

Sample Output

show interfaces (Fast Ethernet)

```

user@host> show interfaces fe-0/0/0
Physical interface: fe-0/0/0, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 22
  Link-level type: Ethernet, MTU: 1514, Speed: 100mbps, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Enabled
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  CoS queues    : 4 supported, 4 maximum usable queues
  Current address: 00:00:5e:00:53:38, Hardware address: 00:00:5e:00:53:38
  Last flapped  : 2006-01-20 14:50:58 PST (2w4d 00:44 ago)
  Input rate    : 0 bps (0 pps)
  Output rate   : 0 bps (0 pps)
  Active alarms : None
  Active defects: None
  Logical interface fe-0/0/0.0 (Index 66) (SNMP ifIndex 198)
    Flags: SNMP-Traps Encapsulation: ENET2

```

```

Protocol inet, MTU: 1500
Flags: None
Addresses, Flags: Is-Preferred Is-Primary
Destination: 203.0.113/24, Local: 203.0.113.1, Broadcast: 203.0.113.255

```

show interfaces brief (Fast Ethernet)

```

user@host> show interfaces fe-0/0/0 brief
Physical interface: fe-0/0/0, Enabled, Physical link is Up
Link-level type: Ethernet, MTU: 1514, Speed: 100mbps, Loopback: Disabled,
Source filtering: Disabled, Flow control: Enabled
Device flags   : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
Logical interface fe-0/0/0.0
Flags: SNMP-Traps Encapsulation: ENET2
inet 203.0.113.1/24

```

show interfaces detail (Fast Ethernet)

```

user@host> show interfaces fe-0/0/0 detail
Physical interface: fe-0/0/0, Enabled, Physical link is Up
Interface index: 128, SNMP ifIndex: 22, Generation: 5391
Link-level type: Ethernet, MTU: 1514, Speed: 100mbps, Loopback: Disabled,
Source filtering: Disabled, Flow control: Enabled
Device flags   : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
CoS queues     : 4 supported, 4 maximum usable queues
Hold-times     : Up 0 ms, Down 0 ms
Current address: 00:00:5e:00:53:38, Hardware address: 00:00:5e:00:53:3f:38
Last flapped   : 2006-01-20 14:50:58 PST (2w4d 00:45 ago)
Statistics last cleared: Never
Traffic statistics:
Input bytes   : 0                      0 bps
Output bytes  : 42                     0 bps
Input packets : 0                      0 pps
Output packets: 1                      0 pps
Active alarms : None
Active defects: None
Logical interface fe-0/0/0.0 (Index 66) (SNMP ifIndex 198) (Generation 67)
Flags: SNMP-Traps Encapsulation: ENET2
Protocol inet, MTU: 1500, Generation: 105, Route table: 0
Flags: Is-Primary, Mac-Validate-Strict
Mac-Validate Failures: Packets: 0, Bytes: 0
Addresses, Flags: Is-Preferred Is-Primary
Destination: 203.0.113/24, Local: 203.0.113.1, Broadcast: 203.0.113.255,
Generation: 136

```

show interfaces extensive (Fast Ethernet)

```

user@host> show interfaces fe-0/0/0 extensive
Physical interface: fe-0/0/0, Enabled, Physical link is Up
Interface index: 128, SNMP ifIndex: 22, Generation: 5391
Link-level type: Ethernet, MTU: 1514, Link-mode: Full-duplex, Speed:
100mbps, Loopback: Disabled,
Source filtering: Disabled, Flow control: Enabled
Device flags   : Present Running
Interface flags: SNMP-Traps Internal: 0x4000
CoS queues     : 4 supported, 4 maximum usable queues
Hold-times     : Up 0 ms, Down 0 ms
Current address: 00:00:5e:00:53:38, Hardware address: 00:00:5e:00:53:38

```

```

Last flapped   : 2006-01-20 14:50:58 PST (2w4d 00:46 ago)
Statistics last cleared: Never
Traffic statistics:
  Input bytes   :          0          0 bps
  Output bytes  :         42          0 bps
  Input packets :          0          0 pps
  Output packets:          1          0 pps
Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0,
  L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0,
  FIFO errors: 0, Resource errors: 0
Output errors:
  Carrier transitions: 3, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,

  FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
Active alarms : None
Active defects : None
MAC statistics:
  Receive      Transmit
  Total octets      0         64
  Total packets     0          1
  Unicast packets   0          0
  Broadcast packets 0          1
  Multicast packets 0          0
  CRC/Align errors  0          0
  FIFO errors       0          0
  MAC control frames 0          0
  MAC pause frames   0          0
  Oversized frames   0
  Jabber frames      0
  Fragment frames    0
  VLAN tagged frames 0
  Code violations     0
Filter statistics:
  Input packet count      0
  Input packet rejects    0
  Input DA rejects        0
  Input SA rejects        0
  Output packet count     1
  Output packet pad count 0
  Output packet error count 0
  CAM destination filters: 1, CAM source filters: 0
Autonegotiation information:
  Negotiation status: Complete
  Link partner:
    Link partner: Full-duplex, Flow control: None, Remote fault: Ok
  Local resolution:
Packet Forwarding Engine configuration:
  Destination slot: 0
CoS information:
  Bandwidth      Buffer Priority  Limit
                %      bps      %      usec
0 best-effort    95    950000000  95      0    low  none
3 network-control 5     50000000  5      0    low  none
Logical interface fe-0/0/0.0 (Index 66) (SNMP ifIndex 198) (Generation 67)
Flags: SNMP-Traps Encapsulation: ENET2
Protocol inet, MTU: 1500, Generation: 105, Route table: 0
Flags: None
Addresses, Flags: Is-Preferred Is-Primary
  Destination: 203.0.113/24, Local: 203.0.113.1, Broadcast: 203.0.113.255,

  Generation: 136

```


show interfaces (Gigabit Ethernet)

Syntax	<code>show interfaces <i>ge-fpc/pic/port</i></code> <code><brief detail extensive terse></code> <code><descriptions></code> <code><media></code> <code><snmp-index <i>snmp-index</i>></code> <code><statistics></code>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display status information about the specified Gigabit Ethernet interface.
Options	<p><i>ge-fpc/pic/port</i>—Display standard information about the specified Gigabit Ethernet interface.</p> <p><i>brief detail extensive terse</i>—(Optional) Display the specified level of output.</p> <p><i>descriptions</i>—(Optional) Display interface description strings.</p> <p><i>media</i>—(Optional) Display media-specific information about network interfaces.</p> <p><i>snmp-index snmp-index</i>—(Optional) Display information for the specified SNMP index of the interface.</p> <p><i>statistics</i>—(Optional) Display static interface statistics.</p>
Additional Information	In a logical system, this command displays information only about the logical interfaces and not about the physical interfaces.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• <i>Verifying and Managing Agent Circuit Identifier-Based Dynamic VLAN Configuration</i>• <i>Verifying and Managing Configurations for Dynamic VLANs Based on Access-Line Identifiers</i>
List of Sample Output	<p>show interfaces (Gigabit Ethernet) on page 530</p> <p>show interfaces (Gigabit Ethernet on MX Series Routers) on page 531</p> <p>show interfaces (link degrade status) on page 531</p> <p>show interfaces extensive (Gigabit Ethernet on MX Series Routers showing interface transmit statistics configuration) on page 532</p> <p>show interfaces brief (Gigabit Ethernet) on page 532</p> <p>show interfaces detail (Gigabit Ethernet) on page 533</p> <p>show interfaces extensive (Gigabit Ethernet IQ2) on page 534</p> <p>show interfaces (Gigabit Ethernet Unnumbered Interface) on page 537</p> <p>show interfaces (ACI Interface Set Configured) on page 537</p>

[show interfaces \(ALI Interface Set\) on page 538](#)

Output Fields [Table 25 on page 515](#) describes the output fields for the **show interfaces** (Gigabit Ethernet) command. Output fields are listed in the approximate order in which they appear. For Gigabit Ethernet IQ and IQE PICs, the traffic and MAC statistics vary by interface type. For more information, see [Table 26 on page 530](#).

Table 25: show interfaces (Gigabit Ethernet) Output Fields

Field Name	Field Description	Level of Output
Physical Interface		
Physical interface	Name of the physical interface.	All levels
Enabled	State of the interface. Possible values are described in the “Enabled Field” section under <i>Common Output Fields Description</i> .	All levels
Interface index	Index number of the physical interface, which reflects its initialization sequence.	detail extensive none
SNMP ifIndex	SNMP index number for the physical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Link-level type	Encapsulation being used on the physical interface.	All levels
MTU	Maximum transmission unit size on the physical interface.	All levels
Speed	Speed at which the interface is running.	All levels
Loopback	Loopback status: Enabled or Disabled . If loopback is enabled, type of loopback: Local or Remote .	All levels
Source filtering	Source filtering status: Enabled or Disabled .	All levels
LAN-PHY mode	10-Gigabit Ethernet interface operating in Local Area Network Physical Layer Device (LAN PHY) mode. LAN PHY allows 10-Gigabit Ethernet wide area links to use existing Ethernet applications.	All levels
WAN-PHY mode	10-Gigabit Ethernet interface operating in Wide Area Network Physical Layer Device (WAN PHY) mode. WAN PHY allows 10-Gigabit Ethernet wide area links to use fiber-optic cables and other devices intended for SONET/SDH.	All levels
Unidirectional	Unidirectional link mode status for 10-Gigabit Ethernet interface: Enabled or Disabled for parent interface; Rx-only or Tx-only for child interfaces.	All levels
Flow control	Flow control status: Enabled or Disabled .	All levels
Auto-negotiation	(Gigabit Ethernet interfaces) Autonegotiation status: Enabled or Disabled .	All levels

Table 25: show interfaces (Gigabit Ethernet) Output Fields (*continued*)

Field Name	Field Description	Level of Output
Remote-fault	(Gigabit Ethernet interfaces) Remote fault status: <ul style="list-style-type: none"> • Online—Autonegotiation is manually configured as online. • Offline—Autonegotiation is manually configured as offline. 	All levels
Device flags	Information about the physical device. Possible values are described in the “Device Flags” section under <i>Common Output Fields Description</i> .	All levels
Interface flags	Information about the interface. Possible values are described in the “Interface Flags” section under <i>Common Output Fields Description</i> .	All levels
Link flags	Information about the link. Possible values are described in the “Links Flags” section under <i>Common Output Fields Description</i> .	All levels
Wavelength	(10-Gigabit Ethernet dense wavelength-division multiplexing [DWDM] interfaces) Displays the configured wavelength, in nanometers (nm).	All levels
Frequency	(10-Gigabit Ethernet DWDM interfaces only) Displays the frequency associated with the configured wavelength, in terahertz (THz).	All levels
CoS queues	Number of CoS queues configured.	detail extensive none
Schedulers	(Gigabit Ethernet intelligent queuing 2 [IQ2] interfaces only) Number of CoS schedulers configured.	extensive
Hold-times	Current interface hold-time up and hold-time down, in milliseconds (ms).	detail extensive
Current address	Configured MAC address.	detail extensive none
Hardware address	Hardware MAC address.	detail extensive none
Last flapped	Date, time, and how long ago the interface went from down to up. The format is Last flapped: year-month-day hour:minute:second:timezone (hour:minute:second ago) . For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago) .	detail extensive none
Input Rate	Input rate in bits per second (bps) and packets per second (pps). The value in this field also includes the Layer 2 overhead bytes for ingress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level.	None
Output Rate	Output rate in bps and pps. The value in this field also includes the Layer 2 overhead bytes for egress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level.	None
Statistics last cleared	Time when the statistics for the interface were last set to zero.	detail extensive
Egress account overhead	Layer 2 overhead in bytes that is accounted in the interface statistics for egress traffic.	detail extensive

Table 25: show interfaces (Gigabit Ethernet) Output Fields (*continued*)

Field Name	Field Description	Level of Output
Ingress account overhead	Layer 2 overhead in bytes that is accounted in the interface statistics for ingress traffic.	detail extensive
Traffic statistics	<p>Number and rate of bytes and packets received and transmitted on the physical interface.</p> <ul style="list-style-type: none"> • Input bytes—Number of bytes received on the interface. The value in this field also includes the Layer 2 overhead bytes for ingress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level. • Output bytes—Number of bytes transmitted on the interface. The value in this field also includes the Layer 2 overhead bytes for egress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level. • Input packets—Number of packets received on the interface. • Output packets—Number of packets transmitted on the interface. <p>Gigabit Ethernet and 10-Gigabit Ethernet IQ PICs count the overhead and CRC bytes.</p> <p>For Gigabit Ethernet IQ PICs, the input byte counts vary by interface type. For more information, see Table 31 under the <i>show interfaces (10-Gigabit Ethernet)</i> command.</p>	detail extensive
Input errors	<p>Input errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</p> <ul style="list-style-type: none"> • Errors—Sum of the incoming frame aborts and FCS errors. • Drops—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism. • Framing errors—Number of packets received with an invalid frame checksum (FCS). • Runts—Number of frames received that are smaller than the runt threshold. • Policed discards—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that Junos OS does not handle. • L3 incompletes—Number of incoming packets discarded because they failed Layer 3 (usually IPv4) sanity checks of the header. For example, a frame with less than 20 bytes of available IP header is discarded. L3 incomplete errors can be ignored by configuring the ignore-l3-incompletes statement. • L2 channel errors—Number of times the software did not find a valid logical interface for an incoming frame. • L2 mismatch timeouts—Number of malformed or short packets that caused the incoming packet handler to discard the frame as unreadable. • FIFO errors—Number of FIFO errors in the receive direction that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning. • Resource errors—Sum of transmit drops. 	extensive

Table 25: show interfaces (Gigabit Ethernet) Output Fields (*continued*)

Field Name	Field Description	Level of Output
Output errors	<p>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</p> <ul style="list-style-type: none"> • Carrier transitions—Number of times the interface has gone from down to up. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC or PIM is malfunctioning. • Errors—Sum of the outgoing frame aborts and FCS errors. • Drops—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism. <p>NOTE: Due to accounting space limitations on certain Type 3 FPCs (which are supported in M320 and T640 routers), the Drops field does not always use the correct value for queue 6 or queue 7 for interfaces on 10-port 1-Gigabit Ethernet PICs.</p> <ul style="list-style-type: none"> • Collisions—Number of Ethernet collisions. The Gigabit Ethernet PIC supports only full-duplex operation, so for Gigabit Ethernet PICs, this number must always be 0. If it is nonzero, there is a software bug. • Aged packets—Number of packets that remained in shared packet SDRAM so long that the system automatically purged them. The value in this field must never increment. If it does, it is most likely a software bug or possibly malfunctioning hardware. • FIFO errors—Number of FIFO errors in the send direction as reported by the ASIC on the PIC. If this value is ever nonzero, the PIC is probably malfunctioning. • HS link CRC errors—Number of errors on the high-speed links between the ASICs responsible for handling the router interfaces. • MTU errors—Number of packets whose size exceeded the MTU of the interface. • Resource errors—Sum of transmit drops. 	extensive
Egress queues	<p>Total number of egress queues supported on the specified interface.</p> <p>NOTE: In DPCs that are not of the enhanced type, such as DPC 40x 1GER, DPCE 20x 1GE + 2x 10GE R, or DPCE 40x 1GE R, you might notice a discrepancy in the output of the show interfaces command because incoming packets might be counted in the Egress queues section of the output. This problem occurs on non-enhanced DPCs because the egress queue statistics are polled from IMQ (Inbound Message Queuing) block of the I-chip. The IMQ block does not differentiate between ingress and egress WAN traffic; as a result, the combined statistics are displayed in the egress queue counters on the Routing Engine. In a simple VPLS scenario, if there is no MAC entry in DMAC table (by sending unidirectional traffic), traffic is flooded and the input traffic is accounted in IMQ. For bidirectional traffic (MAC entry in DMAC table), if the outgoing interface is on the same I-chip then both ingress and egress statistics are counted in a combined way. If the outgoing interface is on a different I-chip or FPC, then only egress statistics are accounted in IMQ. This behavior is expected with non-enhanced DPCs</p>	detail extensive

Table 25: show interfaces (Gigabit Ethernet) Output Fields (*continued*)

Field Name	Field Description	Level of Output
Queue counters (Egress)	<p>CoS queue number and its associated user-configured forwarding class name.</p> <ul style="list-style-type: none"> • Queued packets—Number of queued packets. • Transmitted packets—Number of transmitted packets. • Dropped packets—Number of packets dropped by the ASIC's RED mechanism. <p>NOTE: Due to accounting space limitations on certain Type 3 FPCs (which are supported in M320 and T640 routers), the Dropped packets field does not always display the correct value for queue 6 or queue 7 for interfaces on 10-port 1-Gigabit Ethernet PICs.</p>	detail extensive
Ingress queues	Total number of ingress queues supported on the specified interface. Displayed on IQ2 interfaces.	extensive
Queue counters (Ingress)	<p>CoS queue number and its associated user-configured forwarding class name. Displayed on IQ2 interfaces.</p> <ul style="list-style-type: none"> • Queued packets—Number of queued packets. • Transmitted packets—Number of transmitted packets. • Dropped packets—Number of packets dropped by the ASIC's RED mechanism. 	extensive
Active alarms and Active defects	<p>Ethernet-specific defects that can prevent the interface from passing packets. When a defect persists for a certain amount of time, it is promoted to an alarm. Based on the router configuration, an alarm can ring the red or yellow alarm bell on the router, or turn on the red or yellow alarm LED on the craft interface. These fields can contain the value None or Link.</p> <ul style="list-style-type: none"> • None—There are no active defects or alarms. • Link—Interface has lost its link state, which usually means that the cable is unplugged, the far-end system has been turned off, or the PIC is malfunctioning. 	detail extensive none
Interface transmit statistics	<p>(On MX Series devices) Status of the interface-transmit-statistics configuration: Enabled or Disabled.</p> <ul style="list-style-type: none"> • Enabled—When the interface-transmit-statistics statement is included in the configuration. If this is configured, the interface statistics show the actual transmitted load on the interface. • Disabled—When the interface-transmit-statistics statement is not included in the configuration. If this is not configured, the interface statistics show the offered load on the interface. 	detail extensive
OTN FEC statistics	<p>The forward error correction (FEC) counters provide the following statistics:</p> <ul style="list-style-type: none"> • Corrected Errors—Count of corrected errors in the last second. • Corrected Error Ratio—Corrected error ratio in the last 25 seconds. For example, 1e-7 is 1 error per 10 million bits. 	detail extensive

Table 25: show interfaces (Gigabit Ethernet) Output Fields (*continued*)

Field Name	Field Description	Level of Output
PCS statistics	<p>(10-Gigabit Ethernet interfaces) Displays Physical Coding Sublayer (PCS) fault conditions from the WAN PHY or the LAN PHY device.</p> <ul style="list-style-type: none"> • Bit errors—Number of seconds during which at least one bit error rate (BER) occurred while the PCS receiver is operating in normal mode. • Errored blocks—Number of seconds when at least one errored block occurred while the PCS receiver is operating in normal mode. 	detail extensive
Link Degrad	<p>Shows the link degrade status of the physical link and the estimated bit error rates (BERs). This field is available only for the PICs supporting the physical link monitoring feature.</p> <ul style="list-style-type: none"> • Link Monitoring—Indicates if physical link degrade monitoring is enabled on the interface. <ul style="list-style-type: none"> • Enable—Indicates that link degrade monitoring has been enabled (using the link-degrade-monitor statement) on the interface. • Disable—Indicates that link degrade monitoring has not been enabled on the interface. If link degrade monitoring has not been enabled, the output does not show any related information, such as BER values and thresholds. • Link Degrad Set Threshold—The BER threshold value at which the link is considered degraded and a corrective action is triggered. • Link Degrad Clear Threshold—The BER threshold value at which the degraded link is considered recovered and the corrective action applied to the interface is reverted. • Estimated BER—The estimated bit error rate. • Link-degrade event—Shows link degrade event information. <ul style="list-style-type: none"> • Seconds—Time (in seconds) elapsed after a link degrade event occurred. • Count—The number of link degrade events recorded. • State—Shows the link degrade status (example: Defect Active). 	detail extensive

Table 25: show interfaces (Gigabit Ethernet) Output Fields (*continued*)

Field Name	Field Description	Level of Output
MAC statistics	<p>Receive and Transmit statistics reported by the PIC's MAC subsystem, including the following:</p> <ul style="list-style-type: none"> • Total octets and total packets—Total number of octets and packets. For Gigabit Ethernet IQ PICs, the received octets count varies by interface type. For more information, see Table 31 under the <i>show interfaces (10-Gigabit Ethernet)</i> command. • Unicast packets, Broadcast packets, and Multicast packets—Number of unicast, broadcast, and multicast packets. • CRC/Align errors—Total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a nonintegral number of octets (Alignment Error). • FIFO error—Number of FIFO errors that are reported by the ASIC on the PIC. If this value is ever nonzero, the PIC or a cable is probably malfunctioning. • MAC control frames—Number of MAC control frames. • MAC pause frames—Number of MAC control frames with pause operational code. • Oversized frames—There are two possible conditions regarding the number of oversized frames: <ul style="list-style-type: none"> • Packet length exceeds 1518 octets, or • Packet length exceeds MRU • Jabber frames—Number of frames that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS error or an alignment error. This definition of jabber is different from the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition in which any packet exceeds 20 ms. The allowed range to detect jabber is from 20 ms to 150 ms. • Fragment frames—Total number of packets that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS error or an alignment error. Fragment frames normally increment because both runs (which are normal occurrences caused by collisions) and noise hits are counted. • VLAN tagged frames—Number of frames that are VLAN tagged. The system uses the TPID of 0x8100 in the frame to determine whether a frame is tagged or not. <p>NOTE: The 20-port Gigabit Ethernet MIC (MIC-3D-20GE-SFP) does not have hardware counters for VLAN frames. Therefore, the VLAN tagged frames field displays 0 when the show interfaces command is executed on a 20-port Gigabit Ethernet MIC. In other words, the number of VLAN tagged frames cannot be determined for the 20-port Gigabit Ethernet MIC.</p> • Code violations—Number of times an event caused the PHY to indicate "Data reception error" or "invalid data symbol error." 	extensive
OTN Received Overhead Bytes	APS/PCC0: 0x02, APS/PCC1: 0x11, APS/PCC2: 0x47, APS/PCC3: 0x58 Payload Type: 0x08	extensive
OTN Transmitted Overhead Bytes	APS/PCC0: 0x00, APS/PCC1: 0x00, APS/PCC2: 0x00, APS/PCC3: 0x00 Payload Type: 0x08	extensive

Table 25: show interfaces (Gigabit Ethernet) Output Fields (*continued*)

Field Name	Field Description	Level of Output
Filter statistics	<p>Receive and Transmit statistics reported by the PIC's MAC address filter subsystem. The filtering is done by the content-addressable memory (CAM) on the PIC. The filter examines a packet's source and destination MAC addresses to determine whether the packet may enter the system or be rejected.</p> <ul style="list-style-type: none"> • Input packet count—Number of packets received from the MAC hardware that the filter processed. • Input packet rejects—Number of packets that the filter rejected because of either the source MAC address or the destination MAC address. • Input DA rejects—Number of packets that the filter rejected because the destination MAC address of the packet is not on the accept list. It is normal for this value to increment. When it increments very quickly and no traffic is entering the router from the far-end system, either there is a bad ARP entry on the far-end system, or multicast routing is not on and the far-end system is sending many multicast packets to the local router (which the router is rejecting). • Input SA rejects—Number of packets that the filter rejected because the source MAC address of the packet is not on the accept list. The value in this field must increment only if source MAC address filtering has been enabled. If filtering is enabled, if the value increments quickly, and if the system is not receiving traffic that it should from the far-end system, it means that the user-configured source MAC addresses for this interface are incorrect. • Output packet count—Number of packets that the filter has given to the MAC hardware. • Output packet pad count—Number of packets the filter padded to the minimum Ethernet size (60 bytes) before giving the packet to the MAC hardware. Usually, padding is done only on small ARP packets, but some very small IP packets can also require padding. If this value increments rapidly, either the system is trying to find an ARP entry for a far-end system that does not exist or it is misconfigured. • Output packet error count—Number of packets with an indicated error that the filter was given to transmit. These packets are usually aged packets or are the result of a bandwidth problem on the FPC hardware. On a normal system, the value of this field must not increment. • CAM destination filters, CAM source filters—Number of entries in the CAM dedicated to destination and source MAC address filters. There can only be up to 64 source entries. If source filtering is disabled, which is the default, the values for these fields must be 0. 	extensive
PMA PHY	<p>(10-Gigabit Ethernet interfaces, WAN PHY mode) SONET error information:</p> <ul style="list-style-type: none"> • Seconds—Number of seconds the defect has been active. • Count—Number of times that the defect has gone from inactive to active. • State—State of the error. Any state other than OK indicates a problem. <p>Subfields are:</p> <ul style="list-style-type: none"> • PHY Lock—Phase-locked loop • PHY Light—Loss of optical signal 	extensive

Table 25: show interfaces (Gigabit Ethernet) Output Fields (*continued*)

Field Name	Field Description	Level of Output
WIS section	<p>(10-Gigabit Ethernet interfaces, WAN PHY mode) SONET error information:</p> <ul style="list-style-type: none"> • Seconds—Number of seconds the defect has been active. • Count—Number of times that the defect has gone from inactive to active. • State—State of the error. Any state other than OK indicates a problem. <p>Subfields are:</p> <ul style="list-style-type: none"> • BIP-B1—Bit interleaved parity for SONET section overhead • SEF—Severely errored framing • LOL—Loss of light • LOF—Loss of frame • ES-S—Errored seconds (section) • SES-S—Severely errored seconds (section) • SEFS-S—Severely errored framing seconds (section) 	extensive
WIS line	<p>(10-Gigabit Ethernet interfaces, WAN PHY mode) Active alarms and defects, plus counts of specific SONET errors with detailed information:</p> <ul style="list-style-type: none"> • Seconds—Number of seconds the defect has been active. • Count—Number of times that the defect has gone from inactive to active. • State—State of the error. Any state other than OK indicates a problem. <p>Subfields are:</p> <ul style="list-style-type: none"> • BIP-B2—Bit interleaved parity for SONET line overhead • REI-L—Remote error indication (near-end line) • RDI-L—Remote defect indication (near-end line) • AIS-L—Alarm indication signal (near-end line) • BERR-SF—Bit error rate fault (signal failure) • BERR-SD—Bit error rate defect (signal degradation) • ES-L—Errored seconds (near-end line) • SES-L—Severely errored seconds (near-end line) • UAS-L—Unavailable seconds (near-end line) • ES-LFE—Errored seconds (far-end line) • SES-LFE—Severely errored seconds (far-end line) • UAS-LFE—Unavailable seconds (far-end line) 	extensive

Table 25: show interfaces (Gigabit Ethernet) Output Fields (*continued*)

Field Name	Field Description	Level of Output
WIS path	<p>(10-Gigabit Ethernet interfaces, WAN PHY mode) Active alarms and defects, plus counts of specific SONET errors with detailed information:</p> <ul style="list-style-type: none"> • Seconds—Number of seconds the defect has been active. • Count—Number of times that the defect has gone from inactive to active. • State—State of the error. Any state other than OK indicates a problem. <p>Subfields are:</p> <ul style="list-style-type: none"> • BIP-B3—Bit interleaved parity for SONET section overhead • REI-P—Remote error indication • LOP-P—Loss of pointer (path) • AIS-P—Path alarm indication signal • RDI-P—Path remote defect indication • UNEQ-P—Path unequipped • PLM-P—Path payload (signal) label mismatch • ES-P—Errored seconds (near-end STS path) • SES-P—Severely errored seconds (near-end STS path) • UAS-P—Unavailable seconds (near-end STS path) • SES-PFE—Severely errored seconds (far-end STS path) • UAS-PFE—Unavailable seconds (far-end STS path) 	extensive

Table 25: show interfaces (Gigabit Ethernet) Output Fields (*continued*)

Field Name	Field Description	Level of Output
Autonegotiation information	<p>Information about link autonegotiation.</p> <ul style="list-style-type: none"> • Negotiation status: <ul style="list-style-type: none"> • Incomplete—Ethernet interface has the speed or link mode configured. • No autonegotiation—Remote Ethernet interface has the speed or link mode configured, or does not perform autonegotiation. • Complete—Ethernet interface is connected to a device that performs autonegotiation and the autonegotiation process is successful. • Link partner status—OK when Ethernet interface is connected to a device that performs autonegotiation and the autonegotiation process is successful. • Link partner—Information from the remote Ethernet device: <ul style="list-style-type: none"> • Link mode—Depending on the capability of the link partner, either Full-duplex or Half-duplex. • Flow control—Types of flow control supported by the link partner. For Gigabit Ethernet interfaces, types are Symmetric (link partner supports PAUSE on receive and transmit), Asymmetric (link partner supports PAUSE on transmit), Symmetric/Asymmetric (link partner supports PAUSE on receive and transmit or only PAUSE on transmit), and None (link partner does not support flow control). • Remote fault—Remote fault information from the link partner—Failure indicates a receive link error. OK indicates that the link partner is receiving. Negotiation error indicates a negotiation error. Offline indicates that the link partner is going offline. • Local resolution—Information from the local Ethernet device: <ul style="list-style-type: none"> • Flow control—Types of flow control supported by the local device. For Gigabit Ethernet interfaces, advertised capabilities are Symmetric/Asymmetric (local device supports PAUSE on receive and transmit or only PAUSE on receive) and None (local device does not support flow control). Depending on the result of the negotiation with the link partner, local resolution flow control type will display Symmetric (local device supports PAUSE on receive and transmit), Asymmetric (local device supports PAUSE on receive), and None (local device does not support flow control). • Remote fault—Remote fault information. Link OK (no error detected on receive), Offline (local interface is offline), and Link Failure (link error detected on receive). 	extensive
Received path trace, Transmitted path trace	<p>(10-Gigabit Ethernet interfaces, WAN PHY mode) SONET/SDH interfaces allow path trace bytes to be sent inband across the SONET/SDH link. Juniper Networks and other router manufacturers use these bytes to help diagnose misconfigurations and network errors by setting the transmitted path trace message so that it contains the system hostname and name of the physical interface. The received path trace value is the message received from the router at the other end of the fiber. The transmitted path trace value is the message that this router transmits.</p>	extensive
Packet Forwarding Engine configuration	<p>Information about the configuration of the Packet Forwarding Engine:</p> <ul style="list-style-type: none"> • Destination slot—FPC slot number. 	extensive

Table 25: show interfaces (Gigabit Ethernet) Output Fields (*continued*)

Field Name	Field Description	Level of Output
CoS information	Information about the CoS queue for the physical interface. <ul style="list-style-type: none"> • CoS transmit queue—Queue number and its associated user-configured forwarding class name. • Bandwidth %—Percentage of bandwidth allocated to the queue. • Bandwidth bps—Bandwidth allocated to the queue (in bps). • Buffer %—Percentage of buffer space allocated to the queue. • Buffer usec—Amount of buffer space allocated to the queue, in microseconds. This value is nonzero only if the buffer size is configured in terms of time. • Priority—Queue priority: low or high. • Limit—Displayed if rate limiting is configured for the queue. Possible values are none and exact. If exact is configured, the queue transmits only up to the configured bandwidth, even if excess bandwidth is available. If none is configured, the queue transmits beyond the configured bandwidth if bandwidth is available. 	extensive
Logical Interface		
Logical interface	Name of the logical interface.	All levels
Index	Index number of the logical interface, which reflects its initialization sequence.	detail extensive none
SNMP ifIndex	SNMP interface index number for the logical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Flags	Information about the logical interface. Possible values are described in the "Logical Interface Flags" section under <i>Common Output Fields Description</i> .	All levels

Table 25: show interfaces (Gigabit Ethernet) Output Fields (*continued*)

Field Name	Field Description	Level of Output
VLAN-Tag	<p>Rewrite profile applied to incoming or outgoing frames on the outer (Out) VLAN tag or for both the outer and inner (In) VLAN tags.</p> <ul style="list-style-type: none"> push—An outer VLAN tag is pushed in front of the existing VLAN tag. pop—The outer VLAN tag of the incoming frame is removed. swap—The outer VLAN tag of the incoming frame is overwritten with the user-specified VLAN tag information. push—An outer VLAN tag is pushed in front of the existing VLAN tag. push-push—Two VLAN tags are pushed in from the incoming frame. swap-push—The outer VLAN tag of the incoming frame is replaced by a user-specified VLAN tag value. A user-specified outer VLAN tag is pushed in front. The outer tag becomes an inner tag in the final frame. swap-swap—Both the inner and the outer VLAN tags of the incoming frame are replaced by the user-specified VLAN tag value. pop-swap—The outer VLAN tag of the incoming frame is removed, and the inner VLAN tag of the incoming frame is replaced by the user-specified VLAN tag value. The inner tag becomes the outer tag in the final frame. pop-pop—Both the outer and inner VLAN tags of the incoming frame are removed. 	brief detail extensive none
Demux	<p>IP demultiplexing (demux) value that appears if this interface is used as the demux underlying interface. The output is one of the following:</p> <ul style="list-style-type: none"> Source Family Inet Destination Family Inet 	detail extensive none
Encapsulation	Encapsulation on the logical interface.	All levels
ACI VLAN	<p>Information displayed for agent circuit identifier (ACI) interface set configured with the agent-circuit-id autoconfiguration stanza.</p> <p>Dynamic Profile—Name of the dynamic profile that defines the ACI interface set.</p> <p>If configured, the ACI interface set enables the underlying Ethernet interface to create dynamic VLAN subscriber interfaces based on ACI information.</p> <p>NOTE: The ACI VLAN field is replaced with the Line Identity field when an ALI interface set is configured with the line-identity autoconfiguration stanza.</p>	brief detail extensive none
Line Identity	<p>Information displayed for access-line-identifier (ALI) interface sets configured with the line-identity autoconfiguration stanza.</p> <ul style="list-style-type: none"> Dynamic Profile—Name of the dynamic profile that defines the ALI interface set. Trusted option used to create the ALI interface set: Circuit-id, Remote-id, or Accept-no-ids. More than one option can be configured. <p>If configured, the ALI interface set enables the underlying Ethernet interface to create dynamic VLAN subscriber interfaces based on ALI information.</p> <p>NOTE: The Line Identity field is replaced with the ACI VLAN field when an ACI interface set is configured with the agent-circuit-id autoconfiguration stanza.</p>	detail

Table 25: show interfaces (Gigabit Ethernet) Output Fields (*continued*)

Field Name	Field Description	Level of Output
Protocol	Protocol family. Possible values are described in the "Protocol Field" section under <i>Common Output Fields Description</i> .	detail extensive none
MTU	Maximum transmission unit size on the logical interface.	detail extensive none
Neighbor Discovery Protocol (NDP) Queue Statistics	NDP statistics for protocol inet6 under logical interface statistics. <ul style="list-style-type: none"> • Max nh cache—Maximum interface neighbor discovery nexthop cache size. • New hold nh limit—Maximum number of new unresolved nexthops. • Curr nh cnt—Current number of resolved nexthops in the NDP queue. • Curr new hold cnt—Current number of unresolved nexthops in the NDP queue. • NH drop cnt—Number of NDP requests not serviced. 	All levels
Dynamic Profile	Name of the dynamic profile that was used to create this interface configured with a Point-to-Point Protocol over Ethernet (PPPoE) family.	detail extensive none
Service Name Table	Name of the service name table for the interface configured with a PPPoE family.	detail extensive none
Max Sessions	Maximum number of PPPoE logical interfaces that can be activated on the underlying interface.	detail extensive none
Duplicate Protection	State of PPPoE duplicate protection: On or Off . When duplicate protection is configured for the underlying interface, a dynamic PPPoE logical interface cannot be activated when an existing active logical interface is present for the same PPPoE client.	detail extensive none
Direct Connect	State of the configuration to ignore DSL Forum VSAs: On or Off . When configured, the router ignores any of these VSAs received from a directly connected CPE device on the interface.	detail extensive none
AC Name	Name of the access concentrator.	detail extensive none
Maximum labels	Maximum number of MPLS labels configured for the MPLS protocol family on the logical interface.	detail extensive none
Traffic statistics	Number and rate of bytes and packets received and transmitted on the specified interface set. <ul style="list-style-type: none"> • Input bytes, Output bytes—Number of bytes received and transmitted on the interface set. The value in this field also includes the Layer 2 overhead bytes for ingress or egress traffic on Ethernet interfaces if you enable accounting of Layer 2 overhead at the PIC level or the logical interface level. • Input packets, Output packets—Number of packets received and transmitted on the interface set. 	detail extensive
IPv6 transit statistics	Number of IPv6 transit bytes and packets received and transmitted on the logical interface if IPv6 statistics tracking is enabled.	extensive
Local statistics	Number and rate of bytes and packets destined to the router.	extensive

Table 25: show interfaces (Gigabit Ethernet) Output Fields (*continued*)

Field Name	Field Description	Level of Output
Transit statistics	Number and rate of bytes and packets transiting the switch. NOTE: For Gigabit Ethernet intelligent queuing 2 (IQ2) interfaces, the logical interface egress statistics might not accurately reflect the traffic on the wire when output shaping is applied. Traffic management output shaping might drop packets after they are tallied by the Output bytes and Output packets interface counters. However, correct values display for both of these egress statistics when per-unit scheduling is enabled for the Gigabit Ethernet IQ2 physical interface, or when a single logical interface is actively using a shared scheduler.	extensive
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Route Table	Route table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.	detail extensive none
Flags	Information about protocol family flags. Possible values are described in the “Family Flags” section under <i>Common Output Fields Description</i> .	detail extensive
Donor interface	(Unnumbered Ethernet) Interface from which an unnumbered Ethernet interface borrows an IPv4 address.	detail extensive none
Preferred source address	(Unnumbered Ethernet) Secondary IPv4 address of the donor loopback interface that acts as the preferred source address for the unnumbered Ethernet interface.	detail extensive none
Input Filters	Names of any input filters applied to this interface. If you specify a precedence value for any filter in a dynamic profile, filter precedence values appear in parentheses next to all interfaces.	detail extensive
Output Filters	Names of any output filters applied to this interface. If you specify a precedence value for any filter in a dynamic profile, filter precedence values appear in parentheses next to all interfaces.	detail extensive
Mac-Validate Failures	Number of MAC address validation failures for packets and bytes. This field is displayed when MAC address validation is enabled for the logical interface.	detail extensive none
Addresses, Flags	Information about the address flags. Possible values are described in the “Addresses Flags” section under <i>Common Output Fields Description</i> .	detail extensive none
<i>protocol-family</i>	Protocol family configured on the logical interface. If the protocol is inet , the IP address of the interface is also displayed.	brief
Flags	Information about the address flag. Possible values are described in the “Addresses Flags” section under <i>Common Output Fields Description</i> .	detail extensive none
Destination	IP address of the remote side of the connection.	detail extensive none
Local	IP address of the logical interface.	detail extensive none
Broadcast	Broadcast address of the logical interface.	detail extensive none

Table 25: show interfaces (Gigabit Ethernet) Output Fields (*continued*)

Field Name	Field Description	Level of Output
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive

Table 26: Gigabit Ethernet IQ PIC Traffic and MAC Statistics by Interface Type

Interface Type	Sample Command	Byte and Octet Counts Include	Comments
Inbound physical interface	show interfaces ge-0/3/0 extensive	<p>Traffic statistics:</p> <p>Input bytes: 496 bytes per packet, representing the Layer 2 packet</p> <p>MAC statistics:</p> <p>Received octets: 500 bytes per packet, representing the Layer 2 packet + 4 bytes</p>	The additional 4 bytes are for the CRC.
Inbound logical interface	show interfaces ge-0/3/0.50 extensive	<p>Traffic statistics:</p> <p>Input bytes: 478 bytes per packet, representing the Layer 3 packet</p>	
Outbound physical interface	show interfaces ge-0/0/0 extensive	<p>Traffic statistics:</p> <p>Input bytes: 490 bytes per packet, representing the Layer 3 packet + 12 bytes</p> <p>MAC statistics:</p> <p>Received octets: 478 bytes per packet, representing the Layer 3 packet</p>	For input bytes, the additional 12 bytes include 6 bytes for the destination MAC address plus 4 bytes for VLAN plus 2 bytes for the Ethernet type.
Outbound logical interface	show interfaces ge-0/0/0.50 extensive	<p>Traffic statistics:</p> <p>Input bytes: 478 bytes per packet, representing the Layer 3 packet</p>	

Sample Output

show interfaces (Gigabit Ethernet)

```

user@host> show interfaces ge-3/0/2
Physical interface: ge-3/0/2, Enabled, Physical link is Up
  Interface index: 167, SNMP ifIndex: 35
  Link-level type: 52, MTU: 1522, Speed: 1000mbps, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled
  Remote fault: Online
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  CoS queues    : 4 supported, 4 maximum usable queues
  Current address: 00:00:5e:00:53:7c, Hardware address: 00:00:5e:00:53:7c
  Last flapped  : 2006-08-10 17:25:10 PDT (00:01:08 ago)
  Input rate    : 0 bps (0 pps)
  Output rate   : 0 bps (0 pps)

```



```

Ingress rate at Packet Forwarding Engine      : 0 bps (0 pps)
Ingress drop rate at Packet Forwarding Engine : 0 bps (0 pps)
Active alarms      : None
Active defects     : None

Logical interface ge-3/0/2.0 (Index 72) (SNMP ifIndex 69)
  Flags: SNMP-Traps 0x4000
  VLAN-Tag [ 0x8100.512 0x8100.513 ] In(pop-swap 0x8100.530) Out(swap-push
0x8100.512 0x8100.513)
  Encapsulation: VLAN-CCC
  Egress account overhead: 100
  Ingress account overhead: 90
  Input packets : 0
  Output packets: 0
  Protocol ccc, MTU: 1522
  Flags: Is-Primary

```

show interfaces (Gigabit Ethernet on MX Series Routers)

```

user@host> show interfaces ge-2/2/2
Physical interface: ge-2/2/2, Enabled, Physical link is Up
  Interface index: 156, SNMP ifIndex: 188
  Link-level type: Ethernet, MTU: 1514, Speed: 1000mbps, MAC-REWRITE Error: None,
  Loopback: Disabled,
  Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
  Remote fault: Online
  Device flags      : Present Running
  Interface flags:  SNMP-Traps Internal: 0x4000
  Link flags        : None
  CoS queues        : 8 supported, 4 maximum usable queues
  Schedulers        : 0
  Current address: 00:00:5e:00:53:c0, Hardware address: 00:00:5e:00:53:76
  Last flapped      : 2008-09-05 16:44:30 PDT (3d 01:04 ago)
  Input rate        : 0 bps (0 pps)
  Output rate       : 0 bps (0 pps)
  Active alarms     : None
  Active defects    : None
Logical interface ge-2/2/2.0 (Index 82) (SNMP ifIndex 219)
  Flags: Up SNMP-Traps 0x4004000 Encapsulation: ENET2
  Input packets : 10232
  Output packets: 10294
  Protocol inet, MTU: 1500
    Flags: Sendbroadcast-pkt-to-re
    Addresses, Flags: Is-Preferred Is-Primary
      Destination: 203.0.113/24, Local: 203.0.113.1, Broadcast: 203.0.113.255
  Protocol inet6, MTU: 1500
    Max nh cache: 4, New hold nh limit: 100000, Curr nh cnt: 4, Curr new hold
cnt: 4, NH drop cnt: 0
    Flags: Is-Primary
    Addresses, Flags: Is-Default Is-Preferred Is-Primary
      Destination: 2001:db8:/32, Local: 2001:db8::5
    Addresses, Flags: Is-Preferred
      Destination: 2001:db8:1::/32, Local: 2001:db8:223:9cff:fe9f:3e78
  Protocol multiservice, MTU: Unlimited
  Flags: Is-Primary

```

show interfaces (link degrade status)

```

user@host> show interfaces et-3/0/0

```

```

Physical interface: et-3/0/0, Enabled, Physical link is Down
  Interface index: 157, SNMP ifIndex: 537
  Link-level type: Ethernet, MTU: 1514, MRU: 0, Speed: 100Gbps, BPDU Error: None,
  Loopback: Disabled, Source filtering: Disabled, Flow control: Enabled
  Device flags   : Present Running Down
  Interface flags: Hardware-Down SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues     : 8 supported, 8 maximum usable queues
  Current address: 54:e0:32:23:9d:38, Hardware address: 54:e0:32:23:9d:38
  Last flapped   : 2014-06-18 02:36:38 PDT (02:50:50 ago)
  Input rate     : 0 bps (0 pps)
  Output rate    : 0 bps (0 pps)
  Active alarms  : LINK
  Active defects : LINK
  PCS statistics
    Bit errors           Seconds
    Errored blocks       0
  Link Degraded* :
  Link Monitoring      : Enable
  Link Degraded Set Threshold: 1E-7
  Link Degraded Clear Threshold: 1E-12
  Estimated BER        : 1E-7
  Link-degraded event   : Seconds Count State
                        782      1 Defect Active

```

show interfaces extensive (Gigabit Ethernet on MX Series Routers showing interface transmit statistics configuration)

```

user@host> show interfaces ge-2/1/2 extensive | match "output|interface"
Physical interface: ge-2/1/2, Enabled, Physical link is Up
  Interface index: 151, SNMP ifIndex: 530, Generation: 154
  Interface flags: SNMP-Traps Internal: 0x4000
    Output bytes   : 240614363944      772721536 bps
    Output packets : 3538446506        1420444 pps
    Direction      : Output
  Interface transmit statistics: Enabled

Logical interface ge-2/1/2.0 (Index 331) (SNMP ifIndex 955) (Generation 146)
  Output bytes   : 195560312716      522726272 bps
  Output packets : 4251311146        1420451 pps

```

show interfaces brief (Gigabit Ethernet)

```

user@host> show interfaces ge-3/0/2 brief
Physical interface: ge-3/0/2, Enabled, Physical link is Up
  Link-level type: 52, MTU: 1522, Speed: 1000mbps, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
  Remote fault: Online
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags     : None

Logical interface ge-3/0/2.0
  Flags: SNMP-Traps 0x4000
  VLAN-Tag [ 0x8100.512 0x8100.513 ] In(pop-swap 0x8100.530) Out(swap-push
  0x8100.512 0x8100.513)
  Encapsulation: VLAN-CCC
  ccc

```

```

Logical interface ge-3/0/2.32767
  Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x0000.0 ] Encapsulation: ENET2

```

show interfaces detail (Gigabit Ethernet)

```

user@host> show interfaces ge-3/0/2 detail
Physical interface: ge-3/0/2, Enabled, Physical link is Up
  Interface index: 167, SNMP ifIndex: 35, Generation: 177
  Link-level type: 52, MTU: 1522, Speed: 1000Mbps, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
  Remote fault: Online
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues     : 4 supported, 4 maximum usable queues
  Hold-times     : Up 0 ms, Down 0 ms
  Current address: 00:00:5e:00:53:7c, Hardware address: 00:00:5e:00:53:7c
  Last flapped   : 2006-08-09 17:17:00 PDT (01:31:33 ago)
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes  : 0          0 bps
    Output bytes : 0          0 bps
    Input packets: 0          0 pps
    Output packets: 0         0 pps
  Ingress traffic statistics at Packet Forwarding Engine:
    Input bytes  : 0          0 bps
    Input packets: 0          0 pps
    Drop bytes   : 0          0 bps
    Drop packets: 0          0 pps
  Ingress queues: 4 supported, 4 in use
  Queue counters:

```

	Queued packets	Transmitted packets	Dropped packets
0 best-effort	0	0	0
1 expedited-fo	0	0	0
2 assured-forw	0	0	0
3 network-cont	0	0	0

```

  Egress queues: 4 supported, 4 in use
  Queue counters:

```

	Queued packets	Transmitted packets	Dropped packets
0 best-effort	0	0	0
1 expedited-fo	0	0	0
2 assured-forw	0	0	0
3 network-cont	0	0	0

```

  Active alarms : None
  Active defects: None

Logical interface ge-3/0/2.0 (Index 72) (SNMP ifIndex 69) (Generation 140)
  Flags: SNMP-Traps 0x4000
  VLAN-Tag [0x8100.512 0x8100.513 ] In(pop-swap 0x8100.530)
  Out(swap-push 0x8100.512 0x8100.513)
  Encapsulation: VLAN-CCC
  Egress account overhead: 100
  Ingress account overhead: 90

```

```

Traffic statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
Local statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
Transit statistics:
  Input bytes : 0 0 bps
  Output bytes : 0 0 bps
  Input packets: 0 0 pps
  Output packets: 0 0 pps
Protocol ccc, MTU: 1522, Generation: 149, Route table: 0
Flags: Is-Primary

```

```

Logical interface ge-3/0/2.32767 (Index 71) (SNMP ifIndex 70)
(Generation 139)
Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x0000.0 ] Encapsulation: ENET2
Traffic statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
Local statistics:
  Input bytes : 0
  Output bytes : 0
  Input packets: 0
  Output packets: 0
Transit statistics:
  Input bytes : 0 0 bps
  Output bytes : 0 0 bps
  Input packets: 0 0 pps
  Output packets: 0 0 pps

```

show interfaces extensive (Gigabit Ethernet IQ2)

```

user@host> show interfaces ge-7/1/3 extensive
Physical interface: ge-7/1/3, Enabled, Physical link is Up
Interface index: 170, SNMP ifIndex: 70, Generation: 171
Link-level type: Ethernet, MTU: 1514, Speed: 1000mbps, Loopback: Disabled,
Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
Remote fault: Online
Device flags : Present Running
Interface flags: SNMP-Traps Internal: 0x4004000
Link flags : None
CoS queues : 8 supported, 4 maximum usable queues
Schedulers : 256
Hold-times : Up 0 ms, Down 0 ms
Current address: 00:00:5e:00:53:74, Hardware address: 00:00:5e:00:53:74
Last flapped : 2007-11-07 21:31:41 PST (02:03:33 ago)
Statistics last cleared: Never
Traffic statistics:
  Input bytes : 38910844056 7952 bps
  Output bytes : 7174605 8464 bps
  Input packets: 418398473 11 pps
  Output packets: 78903 12 pps
IPv6 transit statistics:
  Input bytes : 0

```

```

Output bytes :          0
Input packets:          0
Output packets:         0
Ingress traffic statistics at Packet Forwarding Engine:
Input bytes :          38910799145          7952 bps
Input packets:         418397956           11 pps
Drop bytes :           0                   0 bps
Drop packets:          0                   0 pps
Input errors:
  Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Policed discards: 0,
  L3 incompletes: 0, L2 channel errors: 0, L2 mismatch timeouts: 0,
  FIFO errors: 0, Resource errors: 0
Output errors:
  Carrier transitions: 1, Errors: 0, Drops: 0, Collisions: 0, Aged packets: 0,

  FIFO errors: 0, HS link CRC errors: 0, MTU errors: 0, Resource errors: 0
Ingress queues: 4 supported, 4 in use
Queue counters:      Queued packets  Transmitted packets      Dropped packets

0 best-effort          418390823          418390823              0

1 expedited-fo          0                  0                    0

2 assured-forw          0                  0                    0

3 network-cont          7133              7133                  0

Egress queues: 4 supported, 4 in use
Queue counters:      Queued packets  Transmitted packets      Dropped packets

0 best-effort          1031              1031                  0

1 expedited-fo          0                  0                    0

2 assured-forw          0                  0                    0

3 network-cont          77872            77872                  0

Active alarms : None
Active defects : None
MAC statistics:
  Receive      Transmit
Total octets   38910844056    7174605
Total packets  418398473     78903
Unicast packets 408021893366  1026
Broadcast packets 10      12
Multicast packets 418398217    77865
CRC/Align errors 0      0
FIFO errors      0      0
MAC control frames 0      0
MAC pause frames 0      0
Oversized frames 0
Jabber frames    0
Fragment frames  0
VLAN tagged frames 0
Code violations  0 OTN Received Overhead Bytes:
APS/PCC0: 0x02, APS/PCC1: 0x11, APS/PCC2: 0x47, APS/PCC3: 0x58
Payload Type: 0x08
OTN Transmitted Overhead Bytes:
APS/PCC0: 0x00, APS/PCC1: 0x00, APS/PCC2: 0x00, APS/PCC3: 0x00
Payload Type: 0x08
Filter statistics:

```

```

Input packet count          418398473
Input packet rejects        479
Input DA rejects            479
Input SA rejects            0
Output packet count         78903
Output packet pad count     0
Output packet error count   0
CAM destination filters: 0, CAM source filters: 0
Autonegotiation information:
Negotiation status: Complete
Link partner:
  Link mode: Full-duplex, Flow control: Symmetric/Asymmetric,
  Remote fault: OK
Local resolution:
  Flow control: Symmetric, Remote fault: Link OK
Packet Forwarding Engine configuration:
Destination slot: 7
CoS information:
Direction : Output
CoS transmit queue          Bandwidth          Buffer          Priority          Limit
                             %             bps            %             usec
0 best-effort               95             950000000      95              0
low none
3 network-control           5              50000000       5              0
low none
Direction : Input
CoS transmit queue          Bandwidth          Buffer          Priority          Limit
                             %             bps            %             usec
0 best-effort               95             950000000      95              0
low none
3 network-control           5              50000000       5              0
low none

Logical interface ge-7/1/3.0 (Index 70) (SNMP ifIndex 85) (Generation 150)
Flags: SNMP-Traps Encapsulation: ENET2
Traffic statistics:
Input bytes :                812400
Output bytes :              1349206
Input packets:                9429
Output packets:              9449
IPv6 transit statistics:
Input bytes :                 0
Output bytes :                 0
Input packets:                 0
Output packets:                 0
Local statistics:
Input bytes :                812400
Output bytes :              1349206
Input packets:                9429
Output packets:              9449
Transit statistics:
Input bytes :                 0          7440 bps
Output bytes :                 0          7888 bps
Input packets:                 0          10 pps
Output packets:                 0          11 pps
IPv6 transit statistics:
Input bytes :                 0
Output bytes :                 0
Input packets:                 0
Output packets:                 0
Protocol inet, MTU: 1500, Generation: 169, Route table: 0

```

```

Flags: Is-Primary, Mac-Validate-Strict
Mac-Validate Failures: Packets: 0, Bytes: 0
Addresses, Flags: Is-Preferred Is-Primary
Input Filters: F1-ge-3/0/1.0-in, F3-ge-3/0/1.0-in
Output Filters: F2-ge-3/0/1.0-out (53)
Destination: 203.0.113/24, Local: 203.0.113.2, Broadcast: 203.0.113.255,
Generation: 196
Protocol multiservice, MTU: Unlimited, Generation: 170, Route table: 0
Flags: Is-Primary
Policer: Input: __default_arp_policer__

```

NOTE: For Gigabit Ethernet intelligent queuing 2 (IQ2) interfaces, the logical interface egress statistics displayed in the **show interfaces** command output might not accurately reflect the traffic on the wire when output shaping is applied. Traffic management output shaping might drop packets after they are tallied by the interface counters. For detailed information, see the description of the logical interface **Transit statistics** fields in [Table 25 on page 515](#).

show interfaces (Gigabit Ethernet Unnumbered Interface)

```

user@host> show interfaces ge-3/2/0
Physical interface: ge-3/2/0, Enabled, Physical link is Up
  Interface index: 148, SNMP ifIndex: 50
  Link-level type: Ethernet, MTU: 1514, Speed: 1000mbps, Loopback: Disabled,
  Source filtering: Disabled, Flow control: Enabled, Auto-negotiation: Enabled,
  Remote fault: Online
  Device flags   : Present Running
  Interface flags: SNMP-Traps Internal: 0x4000
  Link flags     : None
  CoS queues     : 8 supported, 4 maximum usable queues
  Current address: 00:00:5e:00:53:f8, Hardware address: 00:00:5e:00:53:f8
  Last flapped   : 2006-10-27 04:42:23 PDT (08:01:52 ago)
  Input rate     : 0 bps (0 pps)
  Output rate    : 624 bps (1 pps)
  Active alarms  : None
  Active defects : None

Logical interface ge-3/2/0.0 (Index 67) (SNMP ifIndex 85)
  Flags: SNMP-Traps Encapsulation: ENET2
  Input packets : 0
  Output packets: 6
  Protocol inet, MTU: 1500
  Flags: Unnumbered
  Donor interface: lo0.0 (Index 64)
  Preferred source address: 203.0.113.22

```

show interfaces (ACI Interface Set Configured)

```

user@host> show interfaces ge-1/0/0.4001
Logical interface ge-1/0/0.4001 (Index 340) (SNMP ifIndex 548)
  Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.4001 ] Encapsulation: PPP-over-

Ethernet
ACI VLAN:
  Dynamic Profile: aci-vlan-set-profile
PPPoE:
  Dynamic Profile: aci-vlan-pppoe-profile,
  Service Name Table: None,

```

```
Max Sessions: 32000, Max Sessions VSA Ignore: Off,  
Duplicate Protection: On, Short Cycle Protection: Off,  
Direct Connect: Off,  
AC Name: nbc  
Input packets : 9  
Output packets: 8  
Protocol multiservice, MTU: Unlimited
```

show interfaces (ALI Interface Set)

```
user@host> show interfaces ge-1/0/0.10  
Logical interface ge-1/0/0.10 (Index 346) (SNMP ifIndex 554) (Generation 155)  
Flags: Up SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.10 ] Encapsulation: ENET2  
Line Identity:  
  Dynamic Profile: ali-set-profile  
  Circuit-id Remote-id Accept-no-ids  
PPPoE:  
  Dynamic Profile: ali-vlan-pppoe-profile,  
  Service Name Table: None,  
  Max Sessions: 32000, Max Sessions VSA Ignore: Off,  
  Duplicate Protection: On, Short Cycle Protection: Off,  
  Direct Connect: Off,  
  AC Name: nbc  
  Input packets : 9  
  Output packets: 8  
  Protocol multiservice, MTU: Unlimited
```


show interfaces (Loopback)

Syntax `show interfaces lo0`
`<brief | detail | extensive | terse>`
`<descriptions>`
`<media>`
`<snmp-index snmp-index>`
`<statistics>`

Release Information Command introduced before Junos OS Release 7.4.

Description Display status information about the local loopback interface.



NOTE: Logical interface lo0.16385 is the loopback interface for the internal routing instance. Created by the internal routing service process, this interface facilitates internal traffic. It prevents any filter created on loopback lo0.0 from blocking internal traffic.

Options **lo0**—Display standard status information about the local loopback interface.

brief | detail | extensive | terse—(Optional) Display the specified level of output.

descriptions—(Optional) Display interface description strings.

media—(Optional) Display media-specific information.

snmp-index *snmp-index*—(Optional) Display information for the specified SNMP index of the interface.

statistics—(Optional) Display static interface statistics.

Required Privilege Level view

List of Sample Output [show interfaces \(Loopback\) on page 542](#)
[show interfaces brief \(Loopback\) on page 543](#)
[show interfaces detail \(Loopback\) on page 543](#)
[show interfaces extensive \(Loopback\) on page 544](#)

Output Fields [Table 27 on page 539](#) lists the output fields for the **show interfaces** (loopback) command. Output fields are listed in the approximate order in which they appear.

Table 27: Loopback show interfaces Output Fields

Field Name	Field Description	Level of Output
Physical Interface		

Table 27: Loopback show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Physical Interface	Name of the physical interface.	All levels
Enabled	State of the interface. Possible values are described in the “Enabled Field” section under <i>Common Output Fields Description</i> .	All levels
Interface index	Physical interface index number, which reflects its initialization sequence.	detail extensive none
SNMP ifIndex	SNMP index number for the physical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Type	Type of interface.	All levels
Link-level type	Encapsulation type used on the physical interface.	All levels
MTU	Size of the largest packet to be transmitted.	All levels
Clocking	Reference clock source of the interface.	All levels
Speed	Network speed on the interface.	All levels
Device flags	Information about the physical device. Possible values are described in the “Device Flags” section under <i>Common Output Fields Description</i> .	All levels
Interface flags	Information about the interface. Possible values are described in the “Interface Flags” section under <i>Common Output Fields Description</i> .	All levels
Link type	Data transmission type.	detail extensive
Link flags	Information about the link. Possible values are described in the “Link Flags” section under <i>Common Output Fields Description</i> .	detail extensive none
Physical info	Information about the physical interface.	detail extensive
Hold-times	Current interface hold-time up and hold-time down. Value is in milliseconds.	detail extensive
Current address	Configured MAC address.	detail extensive
Hardware address	Media access control (MAC) address of the interface.	detail extensive
Alternate link address	Backup link address.	detail extensive
Last flapped	Date, time, and how long ago the interface went from down to up. The format is Last flapped: year-month-day hour:minute:second timezone (hour:minute:second ago) . For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago) .	detail extensive

Table 27: Loopback show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Statistics last cleared	Time when the statistics for the interface were last set to zero.	detail extensive
Traffic statistics	<p>Number and rate of bytes and packets received and transmitted on the physical interface.</p> <ul style="list-style-type: none"> • Input bytes, Output bytes—Number of bytes received and transmitted on the interface. • Input packets, Output packets—Number of packets received and transmitted on the interface. 	detail extensive
Input errors	<ul style="list-style-type: none"> • Errors—Input errors on the interface. • Drops—Number of packets dropped by the output queue of the I/O Manager ASIC. • Framing errors—Number of packets received with an invalid frame checksum (FCS). • Runts—Frames received smaller than the runt threshold. • Giants—Frames received larger than the giant threshold. • Policed Discards—Frames that the incoming packet match code discarded because the frames were not recognized or were not of interest. Usually, this field reports protocols that Junos does not support. • Resource errors—Sum of transmit drops. 	extensive
Output errors	<ul style="list-style-type: none"> • Carrier transitions—Number of times the interface has gone from down to up. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly, possibly once every 10 seconds, the cable, the remote system, or the interface is malfunctioning. • Errors—Sum of outgoing frame aborts and FCS errors. • Drops—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet dropped by the ASIC RED mechanism. • MTU errors—Number of packets larger than the MTU threshold. • Resource errors—Sum of transmit drops. 	extensive
Logical Interface		
Logical interface	Name of the logical interface.	All levels
Index	Logical interface index number, which reflects its initialization sequence.	detail extensive
SNMP ifIndex	Logical interface SNMP interface index number.	detail extensive
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Flags	Information about the logical interface; values are described in the “Logical Interface Flags” section under <i>Common Output Fields Description</i> .	brief detail extensive
Encapsulation	Encapsulation on the logical interface.	brief detail extensive

Table 27: Loopback show interfaces Output Fields (*continued*)

Field Name	Field Description	Level of Output
Input packets	Number of packets received on the logical interface.	None specified
Output packets	Number of packets transmitted on the logical interface.	None specified
Traffic statistics	Total number of bytes and packets received and transmitted on the logical interface. These statistics are the sum of the local and transit statistics. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.	detail extensive
Local statistics	Statistics for traffic received from and transmitted to the Routing Engine. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. It takes awhile (generally, less than 1 second) for this counter to stabilize.	detail extensive
Protocol	Protocol family configured on the logical interface (such as iso or inet6).	detail extensive none
MTU	MTU size on the logical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Route Table	Route table in which this address exists; for example, Route table:0 refers to inet.0.	detail extensive
Flags	Information about the protocol family flags. Possible values are described in the “Family Flags” section under <i>Common Output Fields Description</i> .	detail extensive none
Addresses, Flags	Information about the address flags. Possible values are described in the “Addresses Flags” section under <i>Common Output Fields Description</i> .	detail extensive
Destination	IP address of the remote side of the connection.	detail extensive none
Local	IP address of the logical interface.	detail extensive none
Broadcast	Broadcast address on the logical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive

Sample Output

show interfaces (Loopback)

```

user@host> show interfaces lo0
Physical interface: lo0, Enabled, Physical link is Up
  Interface index: 6, SNMP ifIndex: 6
  Type: Loopback, MTU: Unlimited
  Device flags   : Present Running Loopback
  Interface flags: SNMP-Traps
  Link flags    : None

```

```

Last flapped   : Never
Input packets  : 0
Output packets : 0

Logical interface lo0.0 (Index 64) (SNMP ifIndex 16)
Flags: SNMP-Traps Encapsulation: Unspecified
Input packets  : 0
Output packets : 0
Protocol inet, MTU: Unlimited
Flags: None
Addresses, Flags: Is-Default Is-Primary
Local: 203.0.113.1
Addresses
Local: 127.0.0.1
Protocol iso, MTU: Unlimited
Flags: None
Addresses, Flags: Is-Default Is-Primary
Local: 49.0004.1000.0000.0001

Logical interface lo0.16385 (Index 65) (SNMP ifIndex 76)
Flags: SNMP-Traps Encapsulation: Unspecified
Input packets  : 0
Output packets : 0
Protocol inet, MTU: Unlimited
Flags: None

```

show interfaces brief (Loopback)

```

user@host> show interfaces lo0 brief
Physical interface: lo0, Enabled, Physical link is Up
Type: Loopback, Link-level type: Unspecified, MTU: Unlimited,
Clocking: Unspecified, Speed: Unspecified
Device flags   : Present Running Loopback
Interface flags: SNMP-Traps

Logical interface lo0.0
Flags: SNMP-Traps Encapsulation: Unspecified
inet  203.0.113.1      --> 0/0
      127.0.0.1       --> 0/0
iso   49.0004.1000.0000.0001

Logical interface lo0.16385
Flags: SNMP-Traps Encapsulation: Unspecified
inet

```

show interfaces detail (Loopback)

```

user@host> show interfaces lo0 detail
Physical interface: lo0, Enabled, Physical link is Up
Interface index: 6, SNMP ifIndex: 6, Generation: 4
Type: Loopback, Link-level type: Unspecified, MTU: Unlimited,
Clocking: Unspecified, Speed: Unspecified
Device flags   : Present Running Loopback
Interface flags: SNMP-Traps
Link type      : Unspecified
Link flags     : None
Physical info   : Unspecified
Hold-times     : Up 0 ms, Down 0 ms
Current address: Unspecified, Hardware address: Unspecified
Alternate link address: Unspecified

```

```
Last flapped      : Never
Statistics last cleared: Never
Traffic statistics:
  Input bytes      :          0
  Output bytes     :          0
  Input packets    :          0
  Output packets   :          0
Logical interface lo0.0 (Index 64) (SNMP ifIndex 16) (Generation 3)
  Flags: SNMP-Traps Encapsulation: Unspecified
  Traffic statistics:
    Input bytes      :          0
    Output bytes     :          0
    Input packets    :          0
    Output packets   :          0
  Local statistics:
    Input bytes      :          0
    Output bytes     :          0
    Input packets    :          0
    Output packets   :          0

Protocol inet, MTU: Unlimited, Generation: 10, Route table: 0
  Flags: None
  Addresses, Flags: Is-Default Is-Primary
    Destination: Unspecified, Local: 203.0.113.1, Broadcast: Unspecified,
    Generation: 10
  Addresses, Flags: None
    Destination: Unspecified, Local: 127.0.0.1, Broadcast: Unspecified,
    Generation: 12
Protocol iso, MTU: Unlimited, Generation: 11, Route table: 0
  Flags: None
  Addresses, Flags: Is-Default Is-Primary
    Destination: Unspecified, Local: 49.0004.1000.0000.0001,
    Broadcast: Unspecified, Generation: 14

Logical interface lo0.16385 (Index 65) (SNMP ifIndex 76) (Generation 4)
  Flags: SNMP-Traps Encapsulation: Unspecified
  Traffic statistics:
    Input bytes      :          0
    Output bytes     :          0
    Input packets    :          0
    Output packets   :          0
  Local statistics:
    Input bytes      :          0
    Output bytes     :          0
    Input packets    :          0
    Output packets   :          0
Protocol inet, MTU: Unlimited, Generation: 12, Route table: 1
  Flags: None
```

show interfaces extensive (Loopback)

```
user@host> show interfaces lo0 extensive
Physical interface: lo0, Enabled, Physical link is Up
Interface index: 6, SNMP ifIndex: 6, Generation: 4
Type: Loopback, Link-level type: Unspecified, MTU: Unlimited,
Clocking: Unspecified, Speed: Unspecified
Device flags      : Present Running Loopback
Interface flags: SNMP-Traps
Link type         : Unspecified
Link flags        : None
```

```

Physical info : Unspecified
Hold-times    : Up 0 ms, Down 0 ms
Current address: Unspecified, Hardware address: Unspecified
Alternate link address: Unspecified
Last flapped  : Never
Statistics last cleared: Never
Traffic statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
Policed discards: 0, Resource errors: 0
Output errors:
Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0,
Resource errors: 0

```

```

Logical interface lo0.0 (Index 64) (SNMP ifIndex 16) (Generation 3)
Flags: SNMP-Traps Encapsulation: Unspecified
Traffic statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Local statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Protocol inet, MTU: Unlimited, Generation: 10, Route table: 0
Flags: None
Addresses, Flags: Is-Default Is-Primary
Destination: Unspecified, Local: 203.0.113.1, Broadcast: Unspecified,
Generation: 10
Addresses, Flags: None
Destination: Unspecified, Local: 127.0.0.1, Broadcast: Unspecified,
Generation: 12
Protocol iso, MTU: Unlimited, Generation: 11, Route table: 0
Flags: None
Addresses, Flags: Is-Default Is-Primary
Destination: Unspecified, Local: 49.0004.1000.0000.0001,
Broadcast: Unspecified, Generation: 14

```

```

Logical interface lo0.16385 (Index 65) (SNMP ifIndex 76) (Generation 4)
Flags: SNMP-Traps Encapsulation: Unspecified
Traffic statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Local statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Protocol inet, MTU: Unlimited, Generation: 12, Route table: 1
Flags: None

```

show interfaces (PPPoE)

Syntax `show interfaces pp0.logical`
`<brief | detail | extensive | terse>`
`<descriptions>`
`<media>`
`<snmp-index snmp-index>`
`<statistics>`

Release Information Command introduced before Junos OS Release 7.4.

Description (M120 routers, M320 routers, and MX Series routers only). Display status information about the PPPoE interface.

Options **pp0.logical**—Display standard status information about the PPPoE interface.

brief | detail | extensive | terse—(Optional) Display the specified level of output.

descriptions—(Optional) Display interface description strings.

media—(Optional) Display media-specific information about PPPoE interfaces.

snmp-index *snmp-index*—(Optional) Display information for the specified SNMP index of the interface.

statistics—(Optional) Display PPPoE interface statistics.

Required Privilege Level view

List of Sample Output [show interfaces \(PPPoE\) on page 552](#)
[show interfaces \(PPPoE over Aggregated Ethernet\) on page 552](#)
[show interfaces brief \(PPPoE\) on page 553](#)
[show interfaces detail \(PPPoE\) on page 553](#)
[show interfaces extensive \(PPPoE on M120 and M320 Routers\) on page 554](#)

Output Fields [Table 28 on page 546](#) lists the output fields for the **show interfaces (PPPoE)** command. Output fields are listed in the approximate order in which they appear.

Table 28: show interfaces (PPPoE) Output Fields

Field Name	Field Description	Level of Output
Physical Interface		
Physical interface	Name of the physical interface.	All levels
Enabled	State of the interface. Possible values are described in the “Enabled Field” section under <i>Common Output Fields Description</i> .	All levels
Interface index	Physical interface index number, which reflects its initialization sequence.	detail extensive none

Table 28: show interfaces (PPPoE) Output Fields (*continued*)

Field Name	Field Description	Level of Output
SNMP ifIndex	SNMP index number for the physical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Type	Physical interface type (PPPoE).	All levels
Link-level type	Encapsulation on the physical interface (PPPoE).	All levels
MTU	MTU size on the physical interface.	All levels
Clocking	Reference clock source. It can be Internal or External .	All levels
Speed	Speed at which the interface is running.	All levels
Device flags	Information about the physical device. Possible values are described in the "Device Flags" section under <i>Common Output Fields Description</i> .	All levels
Interface flags	Information about the interface. Possible values are described in the "Interface Flags" section under <i>Common Output Fields Description</i> .	All levels
Link type	Physical interface link type: full duplex or half duplex .	All levels
Link flags	Information about the interface. Possible values are described in the "Link Flags" section under <i>Common Output Fields Description</i> .	All levels
Input rate	Input rate in bits per second (bps) and packets per second (pps).	None specified
Output rate	Output rate in bps and pps.	None specified
Physical Info	Physical interface information.	All levels
Hold-times	Current interface hold-time up and hold-time down, in milliseconds.	detail extensive
Current address	Configured MAC address.	detail extensive
Hardware address	MAC address of the hardware.	detail extensive
Alternate link address	Backup address of the link.	detail extensive
Statistics last cleared	Time when the statistics for the interface were last set to zero.	detail extensive

Table 28: show interfaces (PPPoE) Output Fields (*continued*)

Field Name	Field Description	Level of Output
Traffic statistics	<p>Number and rate of bytes and packets received and transmitted on the physical interface.</p> <ul style="list-style-type: none"> • Input bytes—Number of bytes received on the interface. • Output bytes—Number of bytes transmitted on the interface. • Input packets—Number of packets received on the interface. • Output packets—Number of packets transmitted on the interface. 	detail extensive
IPv6 transit statistics	<p>Number of IPv6 transit bytes and packets received and transmitted on the physical interface if IPv6 statistics tracking is enabled.</p> <p>NOTE: These fields include dropped traffic and exception traffic, as those fields are not separately defined.</p> <ul style="list-style-type: none"> • Input bytes—Number of bytes received on the interface. • Output bytes—Number of bytes transmitted on the interface. • Input packets—Number of packets received on the interface. • Output packets—Number of packets transmitted on the interface. 	detail extensive
Input errors	<p>Input errors on the interface:</p> <ul style="list-style-type: none"> • Errors—Sum of incoming frame aborts and FCS errors. • Drops—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism. • Framing errors—Number of packets received with an invalid frame checksum (FCS). • Runts—Number of frames received that are smaller than the runt threshold. • Giants—Number of frames received that are larger than the giant threshold. • Policed discards—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle. • Resource errors—Sum of B chip Tx drops and IXP Tx net transmit drops. 	extensive
Output errors	<p>Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious:</p> <ul style="list-style-type: none"> • Carrier transitions —Number of times the interface has gone from down to up. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), then the cable, the far-end system, or the PIM is malfunctioning. • Errors—Sum of the outgoing frame aborts and FCS errors. • Drops—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism. • MTU errors—Number of packets whose size exceeded the MTU of the interface. • Resource errors—Sum of B chip Tx drops and IXP Tx net transmit drops. 	extensive

Logical Interface

Table 28: show interfaces (PPPoE) Output Fields (*continued*)

Field Name	Field Description	Level of Output
Logical interface	Name of the logical interface.	All levels
Index	Logical interface index number (which reflects its initialization sequence).	detail extensive none
SNMP ifIndex	Logical interface SNMP interface index number.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Flags	Information about the logical interface. Possible values are described in the “Logical Interface Flags” section under <i>Common Output Fields Description</i> .	All levels
Encapsulation	Type of encapsulation configured on the logical interface.	All levels
PPP parameters	PPP status: <ul style="list-style-type: none"> • LCP restart timer—Length of time (in milliseconds) between successive Link Control Protocol (LCP) configuration requests. • NCP restart timer—Length of time (in milliseconds) between successive Network Control Protocol (NCP) configuration requests. 	detail
PPPoE	PPPoE status: <ul style="list-style-type: none"> • State—State of the logical interface (up or down). • Session ID—PPPoE session ID. • Service name—Type of service required. Can be used to indicate an Internet service provider (ISP) name or a class or quality of service. • Configured AC name—Configured access concentrator name. • Auto-reconnect timeout—Time after which to try to reconnect after a PPPoE session is terminated, in seconds. • Idle Timeout—Length of time (in seconds) that a connection can be idle before disconnecting. • Underlying interface—Interface on which PPPoE is running. 	All levels
Link	Name of the physical interfaces for member links in an aggregated Ethernet bundle for a PPPoE over aggregated Ethernet configuration. PPPoE traffic goes out on these interfaces.	All levels
Traffic statistics	Total number of bytes and packets received and transmitted on the logical interface. These statistics are the sum of the local and transit statistics. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. This counter usually takes less than 1 second to stabilize.	detail extensive

Table 28: show interfaces (PPPoE) Output Fields (*continued*)

Field Name	Field Description	Level of Output
IPv6 transit statistics	<p>Number of IPv6 transit bytes and packets received and transmitted on the logical interface if IPv6 statistics tracking is enabled.</p> <p>NOTE: The packet and byte counts in these fields include traffic that is dropped and does not leave the router.</p> <ul style="list-style-type: none"> • Input bytes—Number of bytes received on the interface. • Output bytes—Number of bytes transmitted on the interface. • Input packets—Number of packets received on the interface. • Output packets—Number of packets transmitted on the interface. 	detail extensive
Local statistics	<p>Statistics for traffic received from and transmitted to the Routing Engine. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. This counter usually takes less than 1 second to stabilize.</p>	detail extensive
Transit statistics	<p>Statistics for traffic transiting the router. When a burst of traffic is received, the value in the output packet rate field might briefly exceed the peak cell rate. This counter usually takes less than 1 second to stabilize.</p> <p>NOTE: The packet and byte counts in these fields include traffic that is dropped and does not leave the router.</p>	detail extensive
Keepalive settings	<p>(PPP and HDLC) Configured settings for keepalives.</p> <ul style="list-style-type: none"> • interval seconds—The time in seconds between successive keepalive requests. The range is 10 seconds through 32,767 seconds, with a default of 10 seconds. • down-count number—The number of keepalive packets a destination must fail to receive before the network takes a link down. The range is 1 through 255, with a default of 3. • up-count number—The number of keepalive packets a destination must receive to change a link's status from down to up. The range is 1 through 255, with a default of 1. 	detail extensive
Keepalive statistics	<p>(PPP and HDLC) Information about keepalive packets.</p> <ul style="list-style-type: none"> • Input—Number of keepalive packets received by PPP. <ul style="list-style-type: none"> • (last seen 00:00:00 ago)—Time the last keepalive packet was received, in the format <i>hh:mm:ss</i>. • Output—Number of keepalive packets sent by PPP and how long ago the last keepalive packets were sent and received. <ul style="list-style-type: none"> • (last seen 00:00:00 ago)—Time the last keepalive packet was sent, in the format <i>hh:mm:ss</i>. <p>(MX Series routers with MPCs/MICs) When an MX Series router with MPCs/MICs is using PPP fast keepalive for a PPP link, the display does not include the number of keepalive packets received or sent, or the amount of time since the router received or sent the last keepalive packet.</p>	detail extensive
Input packets	Number of packets received on the logical interface.	None specified
Output packets	Number of packets transmitted on the logical interface.	None specified

Table 28: show interfaces (PPPoE) Output Fields (*continued*)

Field Name	Field Description	Level of Output
LCP state	(PPP) Link Control Protocol state. <ul style="list-style-type: none"> • Conf-ack-received—Acknowledgement was received. • Conf-ack-sent—Acknowledgement was sent. • Conf-req-sent—Request was sent. • Down—LCP negotiation is incomplete (not yet completed or has failed). • Not-configured—LCP is not configured on the interface. • Opened—LCP negotiation is successful. 	none detail extensive
NCP state	(PPP) Network Control Protocol state. <ul style="list-style-type: none"> • Conf-ack-received—Acknowledgement was received. • Conf-ack-sent—Acknowledgement was sent. • Conf-req-sent—Request was sent. • Down—NCP negotiation is incomplete (not yet completed or has failed). • Not-configured—NCP is not configured on the interface. • Opened—NCP negotiation is successful. 	detail extensive none
CHAP state	(PPP) Displays the state of the Challenge Handshake Authentication Protocol (CHAP) during its transaction. <ul style="list-style-type: none"> • Chap-Chal-received—Challenge was received but response not yet sent. • Chap-Chal-sent—Challenge was sent. • Chap-Resp-received—Response was received for the challenge sent, but CHAP has not yet moved into the Success state. (Most likely with RADIUS authentication.) • Chap-Resp-sent—Response was sent for the challenge received. • Closed—CHAP authentication is incomplete. • Failure—CHAP authentication failed. • Not-configured—CHAP is not configured on the interface. • Success—CHAP authentication was successful. 	none detail extensive
Protocol	Protocol family configured on the logical interface.	detail extensive none
<i>protocol-family</i>	Protocol family configured on the logical interface. If the protocol is inet , the IP address of the interface is also displayed.	brief
MTU	MTU size on the logical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Route table	Routing table in which the logical interface address is located. For example, 0 refers to the routing table inet.0 .	detail extensive none
Flags	Information about the protocol family flags. Possible values are described in the “Family Flags” section under <i>Common Output Fields Description</i> .	detail extensive none

Table 28: show interfaces (PPPoE) Output Fields (*continued*)

Field Name	Field Description	Level of Output
Addresses, Flags	Information about the addresses configured for the protocol family. Possible values are described in the "Addresses Flags" section under <i>Common Output Fields Description</i> .	detail extensive none
Destination	IP address of the remote side of the connection.	detail extensive none
Local	IP address of the logical interface.	detail extensive none
Broadcast	Broadcast address.	detail extensive none

Sample Output

show interfaces (PPPoE)

```

user@host> show interfaces pp0
Physical interface: pp0, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 24
  Type: PPPoE, Link-level type: PPPoE, MTU: 1532
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Link type      : Full-Duplex
  Link flags     : None
  Input rate     : 0 bps (0 pps)
  Output rate    : 0 bps (0 pps)

Logical interface pp0.0 (Index 72) (SNMP ifIndex 72)
  Flags: Hardware-Down Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPPoE
  PPPoE:
    State: SessionDown, Session ID: None,
    Service name: None, Configured AC name: sapphire,
    Auto-reconnect timeout: 100 seconds, Idle timeout: Never,
    Underlying interface: at-5/0/0.0 (Index 70)
  Input packets : 0
  Output packets: 0
  LCP state: Not-configured
  NCP state: inet: Not-configured, inet6: Not-configured, iso: Not-configured,
  mp1s: Not-configured
  CHAP state: Closed
    Protocol inet, MTU: 100
    Flags: User-MTU, Negotiate-Address

```

show interfaces (PPPoE over Aggregated Ethernet)

```

user@host> show interfaces pp0.1073773821
Logical interface pp0.1073773821 (Index 80) (SNMP ifIndex 32584)
  Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPPoE
  PPPoE:
    State: SessionUp, Session ID: 1,
    Session AC name: alcor, Remote MAC address: 00:00:5e:00:53:01,
    Underlying interface: demux0.100 (Index 88)
  Link:
    ge-1/0/0.32767
    ge-1/0/1.32767

```

```

    Input packets : 6
    Output packets: 6
    LCP state: Opened
    NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured, mp1s:
Not-configured
    CHAP state: Closed
    PAP state: Success
    Protocol inet, MTU: 1500
    Flags: Sendbcst-pkt-to-re
    Addresses, Flags: Is-Primary
    Local: 203.0.113.1

```

show interfaces brief (PPPoE)

```

user@host> show interfaces pp0 brief
Physical interface: pp0, Enabled, Physical link is Up
  Type: PPPoE, Link-level type: PPPoE, MTU: 1532, Speed: Unspecified
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps

Logical interface pp0.0
  Flags: Hardware-Down Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPPoE
  PPPoE:
    State: SessionDown, Session ID: None,
    Service name: None, Configured AC name: sapphire,
    Auto-reconnect timeout: 100 seconds, Idle timeout: Never,
    Underlying interface: at-5/0/0.0 (Index 70)
  inet

```

show interfaces detail (PPPoE)

```

user@host> show interfaces pp0 detail
Physical interface: pp0, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 24, Generation: 9
  Type: PPPoE, Link-level type: PPPoE, MTU: 1532, Speed: Unspecified
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Link type      : Full-Duplex
  Link flags     : None
  Physical info  : Unspecified
  Hold-times    : Up 0 ms, Down 0 ms
  Current address: Unspecified, Hardware address: Unspecified
  Alternate link address: Unspecified
  Statistics last cleared: Never
  Traffic statistics:
    Input bytes   : 0          0 bps
    Output bytes  : 0          0 bps
    Input packets : 0          0 pps
    Output packets: 0          0 pps
Logical interface pp0.0 (Index 72) (SNMP ifIndex 72) (Generation 14)
  Flags: Hardware-Down Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPPoE
  PPPoE:
    State: SessionDown, Session ID: None,
    Service name: None, Configured AC name: sapphire,
    Auto-reconnect timeout: 100 seconds, Idle timeout: Never,
    Underlying interface: at-5/0/0.0 (Index 70)
  Traffic statistics:
    Input bytes   : 0
    Output bytes  : 0
    Input packets : 0

```

```

Output packets:                0
Local statistics:
Input bytes :                  0
Output bytes :                 0
Input packets:                 0
Output packets:                0
Transit statistics:
Input bytes :                  0          0 bps
Output bytes :                 0          0 bps
Input packets:                 0          0 pps
Output packets:                0          0 pps
LCP state: Not-configured
NCP state: inet: Not-configured, inet6: Not-configured, iso: Not-configured,
mpls: Not-configured
CHAP state: Closed
Protocol inet, MTU: 100, Generation: 14, Route table: 0
Flags: User-MTU, Negotiate-Address

```

show interfaces extensive (PPPoE on M120 and M320 Routers)

```

user@host> show interfaces pp0 extensive
Physical interface: pp0, Enabled, Physical link is Up
Interface index: 128, SNMP ifIndex: 93, Generation: 129
Type: PPPoE, Link-level type: PPPoE, MTU: 1532, Speed: Unspecified
Device flags : Present Running
Interface flags: Point-To-Point SNMP-Traps
Link type : Full-Duplex
Link flags : None
Physical info : Unspecified
Hold-times : Up 0 ms, Down 0 ms
Current address: Unspecified, Hardware address: Unspecified
Alternate link address: Unspecified
Statistics last cleared: Never
Traffic statistics:
Input bytes :          972192          0 bps
Output bytes :         975010          0 bps
Input packets:          1338          0 pps
Output packets:         1473          0 pps
IPv6 transit statistics:
Input bytes :          0
Output bytes :          0
Input packets:          0
Output packets:          0
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0, Policed discards:
0,
Resource errors: 0
Output errors:
Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0, Resource errors:
0

Logical interface pp0.0 (Index 69) (SNMP ifIndex 96) (Generation 194)
Flags: Point-To-Point SNMP-Traps 0x4000 Encapsulation: PPPoE
PPPoE:
State: SessionUp, Session ID: 26,
Session AC name: None, AC MAC address: 00:00:5e:00:53:12,
Service name: None, Configured AC name: None,
Auto-reconnect timeout: Never, Idle timeout: Never,
Underlying interface: ge-3/0/1.0 (Index 67)
Traffic statistics:
Input bytes :          252

```



```

Output bytes :                296
Input  packets:                7
Output packets:               8
IPv6 transit statistics:
  Input bytes :                0
  Output bytes :                0
  Input packets:               0
  Output packets:              0
Local statistics:
  Input bytes :                252
  Output bytes :                296
  Input packets:                7
  Output packets:               8
Transit statistics:
  Input bytes :                0          0 bps
  Output bytes :                0          0 bps
  Input packets:                0          0 pps
  Output packets:               0          0 pps
IPv6 transit statistics:
  Input bytes :                0
  Output bytes :                0
  Input packets:               0
  Output packets:              0
Keepalive settings: Interval 10 seconds, Up-count 1, Down-count 3
Keepalive statistics:
  Input : 1 (last seen 00:00:00 ago)
  Output: 1 (last sent 00:00:03 ago)
LCP state: Opened
NCP state: inet: Opened, inet6: Not-configured, iso: Not-configured, mpls:
Not-configured
CHAP state: Closed
PAP state: Closed
Protocol inet, MTU: 1492, Generation: 171, Route table: 0
Flags: None
Addresses, Flags: Is-Preferred Is-Primary
Destination: 203.0.113.2, Local: 203.0.113.1, Broadcast: Unspecified,
Generation: 206

```

show interfaces demux0 (Demux Interfaces)

Syntax	<pre>show interfaces demux0.logical-interface-number <brief detail extensive terse> <descriptions> <media> <snmp-index snmp-index> <statistics></pre>
Release Information	Command introduced in Junos OS Release 9.0.
Description	(MX Series and M Series routers only) Display status information about the specified demux interface.
Options	<p>none—Display standard information about the specified demux interface.</p> <p>brief detail extensive terse—(Optional) Display the specified level of output.</p> <p>descriptions—(Optional) Display interface description strings.</p> <p>media—(Optional) Display media-specific information about network interfaces.</p> <p>snmp-index snmp-index—(Optional) Display information for the specified SNMP index of the interface.</p> <p>statistics—(Optional) Display static interface statistics.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • <i>Verifying and Managing Agent Circuit Identifier-Based Dynamic VLAN Configuration</i>
List of Sample Output	<p>show interfaces demux0 (Demux) on page 562</p> <p>show interfaces demux0 (PPPoE over Aggregated Ethernet) on page 563</p> <p>show interfaces demux0 extensive (Targeted Distribution for Aggregated Ethernet Links) on page 564</p> <p>show interfaces demux0 (ACI Interface Set Configured) on page 564</p>
Output Fields	Table 29 on page 556 lists the output fields for the show interfaces demux0 (Demux Interfaces) command. Output fields are listed in the approximate order in which they appear.

Table 29: show interfaces demux0 (Demux Interfaces) Output Fields

Field Name	Field Description	Level of Output
Physical Interface		

Table 29: show interfaces demux0 (Demux Interfaces) Output Fields (*continued*)

Field Name	Field Description	Level of Output
Physical interface	Name of the physical interface.	brief detail extensive none
Interface index	Index number of the physical interface, which reflects its initialization sequence.	brief detail extensive none
Enabled	State of the interface. Possible values are described in the “Enabled Field” section under <i>Common Output Fields Description</i> .	brief detail extensive none
Physical link	Status of the physical link (Up or Down).	detail extensive none
Admin	Administrative state of the interface (Up or Down).	terse
Interface index	Index number of the physical interface, which reflects its initialization sequence.	detail extensive none
Link	Status of the physical link (Up or Down).	terse
Targeting summary	Status of aggregated Ethernet links that are configured with targeted distribution (primary or backup)	extensive
Bandwidth	Bandwidth allocated to the aggregated Ethernet links that are configured with targeted distribution.	extensive
Proto	Protocol family configured on the interface.	terse
SNMP ifIndex	SNMP index number for the physical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Type	Type of interface. Software-Pseudo indicates a standard software interface with no associated hardware device.	brief detail extensive none
Link-level type	Encapsulation being used on the physical interface.	brief detail extensive
MTU	Maximum transmission unit size on the physical interface.	brief detail extensive
Clocking	Reference clock source: Internal (1) or External (2).	brief detail extensive
Speed	Speed at which the interface is running.	brief detail extensive
Device flags	Information about the physical device. Possible values are described in the “Device Flags” section under <i>Common Output Fields Description</i> .	brief detail extensive none
Interface flags	Information about the interface. Possible values are described in the “Interface Flags” section under <i>Common Output Fields Description</i> .	brief detail extensive none
Link type	Data transmission type.	detail extensive none

Table 29: show interfaces demux0 (Demux Interfaces) Output Fields (*continued*)

Field Name	Field Description	Level of Output
Link flags	Information about the link. Possible values are described in the “Link Flags” section under <i>Common Output Fields Description</i> .	detail extensive none
Physical info	Information about the physical interface.	detail extensive
Hold-times	Current interface hold-time up and hold-time down, in milliseconds.	detail extensive
Current address	Configured MAC address.	detail extensive
Hardware address	Hardware MAC address.	detail extensive
Alternate link address	Backup address of the link.	detail extensive
Last flapped	Date, time, and how long ago the interface went from down to up. The format is Last flapped: year-month-day hour:minute:second:timezone (hour:minute:second ago) . For example, Last flapped: 2002-04-26 10:52:40 PDT (04:33:20 ago) .	detail extensive none
Statistics last cleared	Time when the statistics for the interface were last set to zero.	detail extensive
Traffic statistics	<p>Number and rate of bytes and packets received and transmitted on the physical interface.</p> <ul style="list-style-type: none"> • Input bytes—Number of bytes received on the interface. • Output bytes—Number of bytes transmitted on the interface. • Input packets—Number of packets received on the interface. • Output packets—Number of packets transmitted on the interface. • IPv6 transit statistics—Number of IPv6 transit bytes and packets received and transmitted on the physical interface if IPv6 statistics tracking is enabled. <p>NOTE: These fields include dropped traffic and exception traffic, as those fields are not separately defined.</p> <ul style="list-style-type: none"> • Input bytes—Number of bytes received on the interface • Output bytes—Number of bytes transmitted on the interface. • Input packets—Number of packets received on the interface. • Output packets—Number of packets transmitted on the interface. 	detail extensive

Table 29: show interfaces demux0 (Demux Interfaces) Output Fields (*continued*)

Field Name	Field Description	Level of Output
Input errors	Input errors on the interface whose definitions are as follows: <ul style="list-style-type: none"> • Errors—Sum of the incoming frame aborts and FCS errors. • Drops—Number of packets dropped by the input queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism. • Framing errors—Number of packets received with an invalid frame checksum (FCS). • Runts—Number of frames received that are smaller than the runt threshold. • Giants—Number of frames received that are larger than the giant packet threshold. • Policed discards—Number of frames that the incoming packet match code discarded because they were not recognized or not of interest. Usually, this field reports protocols that the Junos OS does not handle. • Resource errors—Sum of transmit drops. 	extensive
Input Rate	Input rate in bits per second (bps) and packets per second (pps).	none
Output errors	Output errors on the interface. The following paragraphs explain the counters whose meaning might not be obvious: <ul style="list-style-type: none"> • Carrier transitions—Number of times the interface has gone from down to up. This number does not normally increment quickly, increasing only when the cable is unplugged, the far-end system is powered down and then up, or another problem occurs. If the number of carrier transitions increments quickly (perhaps once every 10 seconds), the cable, the far-end system, or the PIC or PIM is malfunctioning. • Errors—Sum of the outgoing frame aborts and FCS errors. • Drops—Number of packets dropped by the output queue of the I/O Manager ASIC. If the interface is saturated, this number increments once for every packet that is dropped by the ASIC's RED mechanism. • MTU errors—Number of packets whose size exceeded the MTU of the interface. • Resource errors—Sum of transmit drops. 	extensive
Output Rate	Output rate in bps and pps.	none
Logical Interface		
Logical interface	Name of the logical interface.	brief detail extensive none
Index	Index number of the logical interface, which reflects its initialization sequence.	detail extensive none
SNMP ifIndex	SNMP interface index number for the logical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail
Flags	Information about the logical interface. Possible values are described in the "Logical Interface Flags" section under <i>Common Output Fields Description</i> .	brief detail extensive none
Encapsulation	Encapsulation on the logical interface.	brief extensive none

Table 29: show interfaces demux0 (Demux Interfaces) Output Fields (*continued*)

Field Name	Field Description	Level of Output
ACI VLAN: Dynamic Profile	Name of the dynamic profile that defines the agent circuit identifier (ACI) interface set. If configured, the ACI interface set enables the underlying demux interface to create dynamic VLAN subscriber interfaces based on ACI information.	brief detail extensive none
Demux	Specific IP demultiplexing (demux) values: <ul style="list-style-type: none"> • Underlying interface—The underlying interface that the demux interface uses. • Index—Index number of the logical interface. • Family—Protocol family configured on the logical interface. • Source prefixes, total—Total number of source prefixes for the underlying interface. • Destination prefixes, total—Total number of destination prefixes for the underlying interface. • Prefix—inet family prefix. 	detail extensive none
<i>protocol-family</i>	Protocol family configured on the logical interface.	brief
Traffic statistics	Number and rate of bytes and packets received and transmitted on the specified interface set. <ul style="list-style-type: none"> • Input bytes, Output bytes—Number of bytes received and transmitted on the interface set. • Input packets, Output packets—Number of packets received and transmitted on the interface set. • IPv6 transit statistics—Number of IPv6 transit bytes and packets received and transmitted on the logical interface if IPv6 statistics tracking is enabled. <p>NOTE: The packet and byte counts in these fields include traffic that is dropped and does not leave the router.</p> <ul style="list-style-type: none"> • Input bytes—Number of bytes received on the interface. • Output bytes—Number of bytes transmitted on the interface. • Input packets—Number of packets received on the interface. • Output packets—Number of packets transmitted on the interface. 	detail extensive
Local statistics	Number of transit bytes and packets received and transmitted on the local interface. <ul style="list-style-type: none"> • Input bytes—Number of bytes received on the interface. • Output bytes—Number of bytes transmitted on the interface. • Input packets—Number of packets received on the interface. • Output packets—Number of packets transmitted on the interface. 	detail extensive

Table 29: show interfaces demux0 (Demux Interfaces) Output Fields (*continued*)

Field Name	Field Description	Level of Output
Transit statistics	<p>Number and rate of bytes and packets transiting the switch.</p> <p>NOTE: The packet and byte counts in these fields include traffic that is dropped and does not leave the router.</p> <ul style="list-style-type: none"> • Input bytes—Number of bytes received on the interface. • Output bytes—Number of bytes transmitted on the interface. • Input packets—Number of packets received on the interface. • Output packets—Number of packets transmitted on the interface. 	detail extensive
IPv6 Transit statistics	<p>Number of IPv6 transit bytes and packets received and transmitted on the logical interface if IPv6 statistics tracking is enabled.</p> <p>NOTE: The packet and byte counts in these fields include traffic that is dropped and does not leave the router.</p> <ul style="list-style-type: none"> • Input bytes—Number of bytes received on the interface. • Output bytes—Number of bytes transmitted on the interface. • Input packets—Number of packets received on the interface. • Output packets—Number of packets transmitted on the interface. 	detail extensive
Input packets	Number of packets received on the interface.	none
Output packets	Number of packets transmitted on the interface.	none
Protocol	Protocol family. Possible values are described in the “Protocol Field” section under <i>Common Output Fields Description</i> .	detail extensive none
MTU	Maximum transmission unit size on the logical interface.	detail extensive none
Maximum labels	Maximum number of MPLS labels configured for the MPLS protocol family on the logical interface.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Route table	Route table in which the logical interface address is located. For example, 0 refers to the routing table inet.0.	detail extensive
Flags	Information about protocol family flags. Possible values are described in the “Family Flags” section under <i>Common Output Fields Description</i> .	detail extensive none
Mac-Validate Failures	Number of MAC address validation failures for packets and bytes. This field is displayed when MAC address validation is enabled for the logical interface.	detail extensive none
Addresses, Flags	Information about the address flags. Possible values are described in the “Addresses Flags” section under <i>Common Output Fields Description</i> .	detail extensive none
Destination	IP address of the remote side of the connection.	detail extensive statistics none

Table 29: show interfaces demux0 (Demux Interfaces) Output Fields (*continued*)

Field Name	Field Description	Level of Output
Local	IP address of the logical interface.	detail extensive terse none
Remote	IP address of the remote interface.	terse
Broadcast	Broadcast address of the logical interlace.	detail extensive none
Generation	Unique number for use by Juniper Networks technical support only.	detail extensive
Link	Name of the physical interfaces for member links in an aggregated Ethernet bundle for a PPPoE over aggregated Ethernet configuration. PPPoE traffic goes out on these interfaces.	detail extensive none
Dynamic-profile	Name of the PPPoE dynamic profile assigned to the underlying interface.	detail extensive none
Service Name Table	Name of the PPPoE service name table assigned to the PPPoE underlying interface.	detail extensive none
Max Sessions	Maximum number of dynamic PPPoE logical interfaces that the router can activate on the underlying interface.	detail extensive none
Duplicate Protection	State of duplicate protection: On or Off . Duplicate protection prevents the activation of another dynamic PPPoE logical interface on the same underlying interface when a dynamic PPPoE logical interface for a client with the same MAC address is already active on that interface.	detail extensive none
Direct Connect	State of the configuration to ignore DSL Forum VSAs: On or Off . When configured, the router ignores any of these VSAs received from a directly connected CPE device on the interface.	detail extensive none
AC Name	Name of the access concentrator.	detail extensive none

Sample Output

show interfaces demux0 (Demux)

```

user@host> show interfaces demux0
Physical interface: demux0, Enabled, Physical link is Up
  Interface index: 128, SNMP ifIndex: 79, Generation: 129
  Type: Software-Pseudo, Link-level type: Unspecified, MTU: 9192, Clocking: 1,
  Speed: Unspecified
  Device flags   : Present Running
  Interface flags: Point-To-Point SNMP-Traps
  Link type      : Full-Duplex
  Link flags     : None
  Physical info  : Unspecified
  Hold-times    : Up 0 ms, Down 0 ms
  Current address: Unspecified, Hardware address: Unspecified
  Alternate link address: Unspecified
  Last flapped  : Never
  Statistics last cleared: Never

```



```

Traffic statistics:
Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps
IPv6 transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Input errors:
Errors: 0, Drops: 0, Framing errors: 0, Runts: 0, Giants: 0,
Policed discards: 0, Resource errors: 0
Output errors:
Carrier transitions: 0, Errors: 0, Drops: 0, MTU errors: 0,
Resource errors: 0

Logical interface demux0.0 (Index 87) (SNMP ifIndex 84) (Generation 312)
Flags: SNMP-Traps 0x4000 Encapsulation: ENET2
Demux:
Underlying interface: ge-2/0/1.0 (Index 74)
Family Inet Source prefixes, total 1
Prefix: 203.0.113/24
Traffic statistics:
Input bytes : 0
Output bytes : 1554
Input packets: 0
Output packets: 37
IPv6 transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Local statistics:
Input bytes : 0
Output bytes : 1554
Input packets: 0
Output packets: 37
Transit statistics:
Input bytes : 0 0 bps
Output bytes : 0 0 bps
Input packets: 0 0 pps
Output packets: 0 0 pps
IPv6 transit statistics:
Input bytes : 0
Output bytes : 0
Input packets: 0
Output packets: 0
Protocol inet, MTU: 1500, Generation: 395, Route table: 0
Flags: Is-Primary, Mac-Validate-Strict
Mac-Validate Failures: Packets: 0, Bytes: 0
Addresses, Flags: Is-Preferred Is-Primary
Destination: 203.0.113/24, Local: 203.0.113.13, Broadcast: 203.0.113.255,

Generation: 434

```

show interfaces demux0 (PPPoE over Aggregated Ethernet)

```

user@host> show interfaces demux0.100
Logical interface demux0.100 (Index 76) (SNMP ifIndex 61160)
Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.100 ]

```

```
Encapsulation: ENET2
Demux:
  Underlying interface: ae0 (Index 199)
Link:
  ge-1/0/0
  ge-1/1/0
Input packets : 0
Output packets: 0
Protocol pppoe
  Dynamic Profile: pppoe-profile,
  Service Name Table: service-table1,
  Max Sessions: 100, Duplicate Protection: On,
  Direct Connect: Off,
  AC Name: pppoe-server-1
```

show interfaces demux0 extensive (Targeted Distribution for Aggregated Ethernet Links)

```
user@host> show interfaces demux0.1073741824 extensive
```

```
Logical interface demux0.1073741824 (Index 75) (SNMP ifIndex 558) (Generation 346)
Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.1 ] Encapsulation: ENET2
Demux:
  Underlying interface: ae0 (Index 201)
Link:
  ge-1/0/0
  ge-1/1/0
  ge-2/0/7
  ge-2/0/8
Targeting summary:
  ge-1/1/0, primary, Physical link is Up
  ge-2/0/8, backup, Physical link is Up
Bandwidth: 1000mbps
```

show interfaces demux0 (ACI Interface Set Configured)

```
user@host> show interfaces demux0.1073741827
Logical interface demux0.1073741827 (Index 346) (SNMP ifIndex 527)
Flags: SNMP-Traps 0x4000 VLAN-Tag [ 0x8100.1802 0x8100.302 ] Encapsulation: ENET2
Demux: Source Family Inet
ACI VLAN:
  Dynamic Profile: aci-vlan-set-profile
Demux:
  Underlying interface: ge-1/0/0 (Index 138)
Input packets : 18
Output packets: 16
Protocol inet, MTU: 1500
  Flags: Sendbcst-pkt-to-re, Unnumbered
  Donor interface: lo0.0 (Index 322)
  Preferred source address: 203.0.113.202
  Addresses, Flags: Primary Is-Default Is-Primary
    Local: 203.0.113.119
Protocol pppoe
  Dynamic Profile: aci-vlan-pppoe-profile,
  Service Name Table: None,
  Max Sessions: 32000, Max Sessions VSA Ignore: Off,
  Duplicate Protection: On, Short Cycle Protection: Off,
  Direct Connect: Off,
  AC Name: nbc
```


show interfaces filters

Syntax	<code>show interfaces filters</code> <code><interface-name></code>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced on PTX Series Packet Transport Routers for Junos OS Release 12.1.
Description	Display all firewall filters that are installed on each interface in a system.
Options	none —Display filter information about all interfaces. interface-name —(Optional) Display filter information about a particular interface.
Additional Information	For information about how to configure firewall filters, see the <i>Routing Policies, Firewall Filters, and Traffic Policers Feature Guide</i> . For related operational mode commands, see the CLI Explorer .
Required Privilege Level	view
List of Sample Output	show interfaces filters on page 567 show interfaces filters (Interface-Name) on page 567 show interfaces filters (PTX Series Packet Transport Routers) on page 567
Output Fields	Table 30 on page 566 lists the output fields for the show interfaces filters command. Output fields are listed in the approximate order in which they appear.

Table 30: show interfaces filters Output Fields

Field Name	Field Description
Interface	Name of the interface.
Admin	Interface state: up or down .
Link	Link state: up or down .
Proto	Protocol configured on the interface.
Input Filter	Names of any firewall filters to be evaluated when packets are received on the interface, including any filters attached through activation of dynamic service.
Output Filter	Names of any firewall filters to be evaluated when packets are transmitted on the interface, including any filters attached through activation of dynamic service.

Sample Output

show interfaces filters

```

user@host> show interfaces filters
Interface      Admin Link Proto Input Filter      Output Filter
ge-0/0/0       up    up
ge-0/0/0.0     up    up    inet
               iso
ge-5/0/0       up    up
ge-5/0/0.0     up    up    any
               inet
               multiservice
f-any
f-inet

gr-0/3/0       up    up
ip-0/3/0       up    up
mt-0/3/0       up    up
pd-0/3/0       up    up
pe-0/3/0       up    up
vt-0/3/0       up    up
at-1/0/0       up    up
at-1/0/0.0     up    up    inet
               iso
at-1/1/0       up    down
at-1/1/0.0     up    down inet
               iso
....

```

show interfaces filters (Interface-Name)

```

user@host> show interfaces filters so-2/1/0
Interface      Admin Link Proto Input Filter      Output Filter
so-2/1/0       up    down
so-2/1/0.0     up    down inet goop
               iso
               inet6 v6in      v6out

user@host > show interfaces filters ge-3/0/1
Interface      Admin Link Proto Input Filter      Output Filter
ge-3/0/1       up    up
ge-3/0/1.0     up    up    inet F1-ge-3/0/1.0-in  F2-ge-3/0/1.0-out
               inet F3-ge-3/0/1.0-in

```

show interfaces filters (PTX Series Packet Transport Routers)

```

user@host > show interfaces filters em0
Interface      Admin Link Proto Input Filter      Output Filter
em0            up    up
em0.0          up    up    inet

```

show interfaces l2-routing-instance

Syntax	<code>show interfaces l2-routing-instance <i>routing-instance-name</i></code>
Release Information	Command introduced in Junos OS Release 16.1R4.
Description	Display information about core-facing physical interfaces in the specified routing instance. The routing instance must be configured for Layer 2 wholesale operations or the command displays no output.
Options	<i>routing-instance-name</i> —Name of the routing instance.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> Layer 2 Wholesale with ANCP-Triggered VLANs Overview on page 99
List of Sample Output	show interfaces l2-routing-instance on page 568
Output Fields	Table 31 on page 568 lists the output fields for the show interfaces l2-routing-instance command. Output fields are listed in the approximate order in which they appear.

Table 31: show interfaces l2-routing-instance Output Fields

Field Name	Field Description
Interface	Name of the core-facing physical interface.
VLAN Id	Trunk VLAN ID assigned to the core-facing physical interface within its input VLAN map.
Inner VLAN Id total	Aggregate number of VLAN IDs assigned to this physical interface based on the inner VLAN ID-swap-ranges configured for the interface.
Inner VLAN range	Inner VLAN ID swap range; numbers that can be used for swapping inner VLAN IDs.
Inner VLAN range total	Size of the inner VLAN ID swap range.
Inner VLAN id use count	Number of inner VLAN ID tags in use.
Inner VLAN id free count	Number of inner VLAN ID tags not in use.

Sample Output

show interfaces l2-routing-instance

```
user@host> show interfaces l2-routing-instance NSP1
```

```
Interface: ge-1/1/1.0
VLAN Id: 100
  Inner VLAN Id total: 6
  Inner VLAN range: 15-20
    Inner VLAN range total : 6
    Inner VLAN id use count : 1
    Inner VLAN id free count : 5
```

show interfaces routing

Syntax	show interfaces routing <brief detail> <interface-name> <logical-system (all <i>logical-system-name</i>)>
Release Information	Command introduced before Junos OS Release 7.4.
Description	Display the state of the router's interfaces. Use this command for performing router diagnostics only, when you are determining whether the routing protocols and the Junos OS differ about the state of an interface.
Options	<p>none—Display standard information about the state of all router interfaces on all logical systems.</p> <p>brief detail—(Optional) Display the specified level of output.</p> <p>interface-name—(Optional) Name of a specific 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>
Additional Information	For information about how to configure routing protocols, see the <i>Junos OS Routing Protocols Library</i> . For information about related operational mode commands for routing instances and protocols, see the CLI Explorer .
Required Privilege Level	view
List of Sample Output	show interfaces routing brief on page 572 show interfaces routing brief (TX Matrix Plus Router) on page 572 show interfaces routing detail on page 573 show interfaces routing detail (TX Matrix Plus Router) on page 573
Output Fields	Table 32 on page 570 lists the output fields for the show interfaces routing command. Output fields are listed in the approximate order in which they appear.

Table 32: show interfaces routing Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the physical interface.	none brief
State	State of the physical interface: Up or Down .	none brief
Addresses	Protocols and addresses configured on the interface.	none brief

Table 32: show interfaces routing Output Fields (*continued*)

Field Name	Field Description	Level of Output
Index	Interface index number, which reflects its initialization sequence.	detail
Refcount	Number of references to the interface in the routing software.	detail
State	State (Up or Down) and type of interface.	detail
Change	Reflects one or more of the following recent changes to the interface: <ul style="list-style-type: none"> • Add—The interface was just added. • Address—The interface's link-layer address has changed. • Delete—The interface is being deleted. • Encapsulation—The type of encapsulation on the interface has changed. • Metric—The interface's metric value has changed. • MTU—The interface's maximim transmission unit size has changed. • UpDown—The interface has made an up or down transition. 	detail
Up/down transitions	Number of times the interface has gone from Down to Up .	detail
Link layer	Describes the link layer of the interface.	detail
Encapsulation	Encapsulation on the interface.	detail
Bandwidth	Speed at which the interface is running.	detail
Protocol address	Information about the configuration of protocols on the interface: <ul style="list-style-type: none"> • Address—Address configured on the interface for the protocol type. • State—State (Up or down) and type of interface. • Change—Reflects one or more of the following recent changes to the interface: <ul style="list-style-type: none"> • Add—The interface was just added. • Address—The interface's address has changed. • Broadcast—The interface's broadcast address has changed. • Delete—The interface is being deleted. • Netmask—The interface's netmask has changed. • UpDown—The interface has made an up or down transition. • Preference—Preference value for the route for this address. • Metric—Metric value on the interface for the protocol type. • MTU—Maximim transmission unit value of the interface. • Local address—On a point-to-point link, the address of the local side of the link. Not used for multicast links. • Destination—For a point-to-point link, the address of the remote side of the link. For multicast links, the network address. 	detail

Sample Output

show interfaces routing brief

```

user@host> show interfaces routing brief
Interface      State Addresses
so-5/0/3.0     Down  ISO    enabled
so-5/0/2.0     Up    MPLS   enabled
               ISO    enabled
               INET   192.168.2.120
               INET   enabled
so-5/0/1.0     Up    MPLS   enabled
               ISO    enabled
               INET   192.168.2.130
               INET   enabled
at-1/0/0.3     Up    CCC    enabled
at-1/0/0.2     Up    CCC    enabled
at-1/0/0.0     Up    ISO    enabled
               INET   192.168.90.10
               INET   enabled
1o0.0          Up    ISO    47.0005.80ff.f800.0000.0108.0001.1921.6800.5061.00
               ISO    enabled
               INET   127.0.0.1
fxp1.0         Up
fxp0.0         Up    INET   192.168.6.90

```

show interfaces routing brief (TX Matrix Plus Router)

```

user@host> show interfaces routing brief
Interface      State Addresses
...
ge-23/0/4.0    Up    INET   203.0.113.91
               ISO    enabled
               MPLS   enabled
ge-23/0/3.0    Up    INET   203.0.113.81
               ISO    enabled
               MPLS   enabled
ge-23/0/2.0    Up    INET   203.0.113.71
               ISO    enabled
               MPLS   enabled
ge-23/0/1.0    Up    INET   203.0.113.61
               ISO    enabled
               MPLS   enabled
ge-23/0/0.0    Up    INET   203.0.113.51
               ISO    enabled
               MPLS   enabled
ge-31/0/7.599  Up    INET   192.0.2.93
ge-31/0/7.598  Up    INET   192.0.2.89
ge-31/0/7.597  Up    INET   192.0.2.85
ge-31/0/7.596  Up    INET   192.0.2.81
ge-31/0/7.595  Up    INET   192.0.2.77
ge-31/0/7.594  Up    INET   192.0.2.73
...
ixgbe1.0       Up    INET   203.0.113.34
               INET   198.51.100.4
               INET6   fe80::200:1ff:fe22:4
               INET6   fec0::a:22:0:4
ixgbe0.0       Up    INET   203.0.113.34
               INET   198.51.100
               INET6   fe80::200:ff:fe22:4

```

```

em0.0          Up    INET6 fec0::a:22:0:4
                INET  192.168.178.11

```

show interfaces routing detail

```

user@host> show interfaces routing detail
so-5/0/3.0
  Index: 15, Refcount: 2, State: Up <Broadcast PointToPoint Multicast> Change:<>

  Metric: 0, Up/down transitions: 0, Full-duplex
  Link layer: HDLC serial line Encapsulation: PPP Bandwidth: 155Mbps
  ISO address (null)
    State: <Broadcast PointToPoint Multicast> Change: <>
    Preference: 0 (120 down), Metric: 0, MTU: 4470 bytes
so-5/0/2.0
  Index: 14, Refcount: 7, State: <Up Broadcast PointToPoint Multicast> Change:<>

  Metric: 0, Up/down transitions: 0, Full-duplex
  Link layer: HDLC serial line Encapsulation: PPP Bandwidth: 155Mbps
  MPLS address (null)
    State: <Up Broadcast PointToPoint Multicast> Change: <>
    Preference: 0 (120 down), Metric: 0, MTU: 4458 bytes
  ISO address (null)
    State: <Up Broadcast PointToPoint Multicast> Change: <>
    Preference: 0 (120 down), Metric: 0, MTU: 4470 bytes
  INET address 192.168.2.120
    State: <Up Broadcast PointToPoint Multicast Localup> Change: <>
    Preference: 0 (120 down), Metric: 0, MTU: 4470 bytes
    Local address: 192.168.2.120
    Destination: 192.168.2.110/32
  INET address (null)
    State: <Up Broadcast PointToPoint Multicast> Change: <>
    Preference: 0 (120 down), Metric: 0, MTU: 4470 bytes
...

```

show interfaces routing detail (TX Matrix Plus Router)

```

user@host> show interfaces routing detail
ge-23/0/4.0
  Index: 77, Refcount: 5, State: <Up Broadcast Multicast> Change: <>
  0 metric, 0 up/down transitions, reth state 0, full-duplex
  Link layer: Ethernet Encapsulation: Ethernet Bandwidth: 1000Mbps
  Link address #0 0.1d.b5.14.da.2d
  INET address 203.0.113.91
    State: <Up Broadcast Multicast Localup> Change: <> Flags: <RT-Change>
    Preference 0, metric 0, MTU 1500 bytes
    Broadcast address 203.0.113.93
    Destination: 203.0.113.0/30
    System flags: <Is-Preferred Is-Primary>
  ISO address (null)
    State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
    Preference 0, metric 0, MTU 1497 bytes
    System flags: <>
  MPLS address (null)
    State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
    Preference 0, metric 0, MTU 1488 bytes
    System flags: <>
ge-23/0/3.0
  Index: 76, Refcount: 5, State: <Up Broadcast Multicast> Change: <>
  0 metric, 0 up/down transitions, reth state 0, full-duplex

```

```
Link layer: Ethernet Encapsulation: Ethernet Bandwidth: 1000Mbps
Link address #0 0.1d.b5.14.da.2c
INET address 203.0.113.81
  State: <Up Broadcast Multicast Localup> Change: <> Flags: <RT-Change>
  Preference 0, metric 0, MTU 1500 bytes
  Broadcast address 2.8.1.3
  Destination: 203.0.113.80/30
  System flags: <Is-Preferred Is-Primary>
ISO address (null)
  State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
  Preference 0, metric 0, MTU 1497 bytes
  System flags: <>
MPLS address (null)
  State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
  Preference 0, metric 0, MTU 1488 bytes
  System flags: <>
ge-23/0/2.0
  Index: 75, Refcount: 5, State: <Up Broadcast Multicast> Change: <>
  0 metric, 0 up/down transitions, reth state 0, full-duplex
Link layer: Ethernet Encapsulation: Ethernet Bandwidth: 1000Mbps
Link address #0 0.1d.b5.14.da.2b
INET address 203.0.113.71
  State: <Up Broadcast Multicast Localup> Change: <> Flags: <RT-Change>
  Preference 0, metric 0, MTU 1500 bytes
  Broadcast address 203.0.113.73
  Destination: 203.0.113.70/30
  System flags: <Is-Preferred Is-Primary>
ISO address (null)
  State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
  Preference 0, metric 0, MTU 1497 bytes
  System flags: <>
MPLS address (null)
  State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
  Preference 0, metric 0, MTU 1488 bytes
  System flags: <>
ge-23/0/1.0
  Index: 74, Refcount: 5, State: <Up Broadcast Multicast> Change: <>
  0 metric, 0 up/down transitions, reth state 0, full-duplex
Link layer: Ethernet Encapsulation: Ethernet Bandwidth: 1000Mbps
Link address #0 0.1d.b5.14.da.2a
INET address 203.0.113.61
  State: <Up Broadcast Multicast Localup> Change: <> Flags: <RT-Change>
  Preference 0, metric 0, MTU 1500 bytes
  Broadcast address 203.0.113.63
...
ixgbe1.0
  Index: 5, Refcount: 5, State: <Up Broadcast Multicast> Change: <>
  0 metric, 0 up/down transitions, reth state 0, full-duplex
Link layer: Ethernet Encapsulation: Ethernet Bandwidth: 1000Mbps
Link address #0 2.0.1.22.0.4
INET address 203.0.113.34
  State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
  Preference 0, metric 0, MTU 1500 bytes
  Broadcast address 203.0.113.255
  Destination: 203.0.113.0/8
  System flags: <Is-Preferred>
INET address 198.51.100.4
  State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
  Preference 0, metric 0, MTU 1500 bytes
  Broadcast address 191.255.255.255
  Destination: 192.0.2.0/2
```

```

    System flags: <Primary Is-Preferred Is-Primary>
INET6 address fe80::200:1ff:fe22:4
    State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
    Preference 0, metric 0, MTU 1500 bytes
    Destination: fe80::/64
    System flags: <Is-Preferred>
INET6 address fec0::a:22:0:4
    State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
    Preference 0, metric 0, MTU 1500 bytes
    Destination: fec0::/64
    System flags: <Is-Preferred Is-Primary>
ixgbe0.0
    Index: 4, Refcount: 5, State: <Up Broadcast Multicast> Change: <>
    0 metric, 0 up/down transitions, reth state 0, full-duplex
    Link layer: Ethernet Encapsulation: Ethernet Bandwidth: 1000Mbps
    Link address #0 2.0.0.22.0.4
    INET address 203.0.113.34
        State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
        Preference 0, metric 0, MTU 1500 bytes
        Broadcast address 203.0.113.255
        Destination: 203.0.113.0/8
        System flags: <Is-Preferred>
    INET address 198.51.100.4
        State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
        Preference 0, metric 0, MTU 1500 bytes
        Broadcast address 191.255.255.255
        Destination: 192.0.2.0/2
        System flags: <Primary Is-Default Is-Preferred Is-Primary>
    INET6 address fe80::200:ff:fe22:4
        State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
        Preference 0, metric 0, MTU 1500 bytes
        Destination: fe80::/64
        System flags: <Is-Preferred>
    INET6 address fec0::a:22:0:4
        State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
        Preference 0, metric 0, MTU 1500 bytes
        Destination: fec0::/64
        System flags: <Is-Default Is-Preferred Is-Primary>
em0.0
    Index: 3, Refcount: 2, State: <Up Broadcast Multicast> Change: <>
    0 metric, 0 up/down transitions, reth state 0, full-duplex
    Link layer: Ethernet Encapsulation: Ethernet Bandwidth: 100Mbps
    Link address #0 0.80.f9.26.0.c0
    INET address 192.168.178.11
        State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
        Preference 0, metric 0, MTU 1500 bytes
        Broadcast address 192.168.178.127
        Destination: 192.168.178.0/25
        System flags: <Is-Preferred Is-Primary>

```

show interfaces routing-instance

Syntax	show interfaces routing-instance (<i>instance-name</i> all) <brief detail extensive terse>
Release Information	Command introduced in Junos OS Release 9.1.
Description	Display information about the interfaces configured for either a specific routing instance or for all of the routing instances.
Options	all —Display information about all of the interfaces configured for all of the routing instances on the router. <i>instance-name</i> —Display information about the interfaces configured for the specified routing instance. brief detail extensive terse —(Optional) Display the specified level of output.
Required Privilege Level	view
List of Sample Output	show interfaces routing-instance terse on page 576 show interfaces routing-instance all on page 576 show interfaces routing-instance extensive on page 577
Output Fields	The output fields from the show interfaces routing-instance command are identical to those produced by the show interfaces <i>interface-name</i> command. For a description of output fields, see the other chapters in this manual.

Sample Output

show interfaces routing-instance terse

```
user@host> show interfaces routing-instance sample terse
Interface      Admin  Link   Proto  Local          Remote
ge-0/0/0.0     up     up     inet   192.168.4.28/24
```

Sample Output

show interfaces routing-instance all

```
user@host> show interfaces terse routing-instance all
Interface  Admin  Link  Proto  Local          Remote Instance
at-0/0/1   up     up    inet   203.0.113.1/24
ge-0/0/0.0 up     up    inet   192.168.4.28/24      sample-a
at-0/1/0.0 up     up    inet6  fe80::a:0:0:4/64    sample-b
so-0/0/0.0 up     up    inet   203.0.113.1/32
```

show interfaces routing-instance extensive

```

user@hostshow interfaces fe-0/1/3 routing-instance instance2 extensive
Logical interface fe-0/1/3.0 (Index 70) (SNMP ifIndex 53) (Generation 211)
  Flags: SNMP-Traps Encapsulation: ENET2
  Traffic statistics:
    Input bytes :                0
    Output bytes :               42
    Input packets:                0
    Output packets:              1
  IPv6 transit statistics:
    Input bytes :                0
    Output bytes :               0
    Input packets:               0
    Output packets:              0
  Local statistics:
    Input bytes :                0
    Output bytes :               42
    Input packets:               0
    Output packets:              1
  Transit statistics:
    Input bytes :                0                0 bps
    Output bytes :               0                0 bps
    Input packets:               0                0 pps
    Output packets:              0                0 pps
  IPv6 transit statistics:
    Input bytes :                0
    Output bytes :               0
    Input packets:               0
    Output packets:              0
  Protocol inet, MTU: 1500, Generation: 252, Route table: 4
    Flags: Is-Primary
    Addresses, Flags: Is-Default Is-Preferred Is-Primary
    Destination: 192.0.2/24, Local: 192.0.2.51, Broadcast: 192.0.2.255,
    Generation: 263

```

show network-access aaa statistics

Syntax	<code>show network-access aaa statistics</code> <code><accounting (detail)></code> <code><address-assignment (client pool <i>pool-name</i>)></code> <code><dynamic-requests></code> <code><radius></code>
Release Information	Command introduced in Junos OS Release 9.1. Option address-assignment introduced in Junos OS Release 10.0. Option radius introduced in Junos OS Release 11.4. Option detail introduced in Junos OS Release 13.3.
Description	Display AAA accounting, address-assignment, dynamic request statistics, and RADIUS settings and statistics.
Options	accounting (detail) —(Optional) Display AAA accounting statistics. The detail keyword displays additional accounting information address-assignment (client pool <i>pool-name</i>) —(Optional) Display AAA address-assignment client and pool statistics. dynamic-requests —(Optional) Display AAA dynamic requests. radius —(Optional) Display RADIUS settings and statistics.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"><i>Verifying and Managing Subscriber AAA Information</i>
List of Sample Output	show network-access aaa statistics accounting on page 584 show network-access aaa statistics accounting detail on page 585 show network-access aaa statistics address-assignment client on page 585 show network-access aaa statistics address-assignment pool on page 585 show network-access aaa statistics dynamic-requests on page 586 show network-access aaa statistics radius on page 586
Output Fields	Table 33 on page 579 lists the output fields for the show network-access aaa statistics command. Output fields are listed in the approximate order in which they appear.

Table 33: show network-access aaa statistics Output Fields

Field Name	Field Description	Level of Output
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. <p>Does not include requests sent from backup accounting.</p>	All levels
Accounting request failures	<p>Number of accounting requests that failed to be sent or queued from a client to a RADIUS accounting server.</p> <p>Does not include requests sent from backup accounting.</p>	detail
Accounting request success	<p>Number of accounting requests successfully sent or queued from a client to a RADIUS accounting server.</p> <p>Does not include requests sent from backup accounting.</p>	detail
Account on requests	<p>Number of accounting on requests sent from a client to a RADIUS accounting server.</p>	detail
Accounting start requests	<p>Number of accounting start requests sent from a client to a RADIUS accounting server.</p>	detail
Accounting interim requests	<p>Number of accounting interim requests sent from a client to a RADIUS accounting server.</p>	detail
Accounting stop requests	<p>Number of accounting stop requests sent from a client to a RADIUS accounting server.</p> <p>Does not include requests sent from backup accounting.</p>	detail
Accounting request timeouts	<p>Number of accounting requests to the accounting server that timed out. This field was named Timed out requests in releases before Junos OS Release 16.1.</p> <p>Does not include requests sent from backup accounting.</p>	All levels
Accounting Response failures	<p>Number of accounting requests not acknowledged (NAK) by the accounting server.</p> <p>Does not include requests sent from backup accounting.</p>	All levels

Table 33: show network-access aaa statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
Accounting response success	Number of accounting requests acknowledged by the accounting server. Does not include requests sent from backup accounting.	All levels
Account on responses	Number of accounting on requests acknowledged by the RADIUS accounting server.	detail
Accounting start responses	Number of accounting start requests acknowledged by the RADIUS accounting server.	detail
Accounting interim responses	Number of accounting interim requests acknowledged by the RADIUS accounting server.	detail
Accounting stop responses	Number of accounting stop requests acknowledged by the RADIUS accounting server. Does not include requests sent from backup accounting.	detail
Accounting rollover requests	Number of accounting requests coming to a RADIUS accounting server after a previous server timing out.	detail
Accounting unknown requests	Number of unknown accounting requests sent from a client to a RADIUS accounting server (for example, when the header has invalid or unsupported information).	detail
Accounting radius pending requests	Number of accounting requests sent from a client to a RADIUS accounting server that are waiting for a response from the server.	detail
Accounting malformed responses	Number of accounting responses from a RADIUS accounting server that have invalid or unexpected attributes.	detail
Accounting retransmissions	Number of accounting requests made by a client to the RADIUS sever that were retransmitted. Does not include requests sent from backup accounting.	detail
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).	detail

Table 33: show network-access aaa statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
Accounting packets dropped	Number of accounting responses from a RADIUS accounting server that are dropped by a client.	detail
Accounting backup record creation requests	Number of accounting stop requests from a client to a RADIUS accounting server that were forwarded to be backed up.	detail
Accounting backup replay request success	Number of backup accounting stop requests successfully created by clients after each timeout for replay to a RADIUS accounting server.	detail
Accounting backup request failures	Number of backup accounting requests that failed to be sent or queued from a client to a RADIUS accounting server.	detail
Accounting backup request success	Number of backup accounting requests successfully sent or queued from a client to a RADIUS accounting server.	detail
Accounting backup timeouts	Number of backup accounting requests that timed out after being sent to a RADIUS accounting server.	detail
Accounting backup in-flight requests	<p>Number of backup accounting requests that were successfully sent or queued to a RADIUS accounting server for which no response or error has been received yet.</p> <p>Backup requests are replayed only in the following circumstances:</p> <ul style="list-style-type: none"> • When the request being replayed receives a positive response, the next request can be replayed. • When the request being replayed receives a timeout response, it can be replayed again. <p>Consequently this intermediate timer displays 1 or 0. The value eventually drops to 0 as requests are responded to positively or fail due to error.</p>	detail
Accounting backup responses success	Number of backup records that were successfully acknowledged with a positive response from a RADIUS accounting server.	detail

Table 33: show network-access aaa statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
Accounting backup radius requests	<p>Number of backup requests sent to UDP level.</p> <p>This is a RADIUS-level counter and increments rapidly based on the configured retries and timeouts and the RADIUS-level retransmissions. An observation that the value is increasing is more significant than the exact value of the counter.</p>	detail
Accounting backup radius responses	<p>Number of responses received at the UDP level for backup requests.</p> <p>This is a RADIUS-level counter and increments rapidly based on the configured retries and timeouts and the RADIUS-level retransmissions. Observation that the value is increasing is more significant than the exact value of the counter.</p>	detail
Accounting backup radius timeouts	<p>Number of backup requests that timed out after being sent to UDP.</p> <p>This is a RADIUS-level counter and increments rapidly based on the configured retries and timeouts and the RADIUS-level retransmissions. Observation that the value is increasing is more significant than the exact value of the counter.</p>	detail
Accounting backup radius pending requests	<p>Number of backup requests sent to a RADIUS accounting server that are waiting for a response from the server.</p> <p>This is an intermediate state counter that eventually drops to zero as requests are responded to or failed due to error.</p>	detail
Accounting backup radius retransmissions	<p>Sum of backup request retransmissions for each RADIUS accounting server.</p> <p>This is a RADIUS-level counter and increments rapidly based on the configured retries and timeouts and the RADIUS-level retransmissions. Observation that the value is increasing is more significant than the exact value of the counter.</p>	detail
Accounting backup malformed responses	Sum of malformed responses received for backup requests sent to each RADIUS accounting server at the UDP level.	detail
Accounting backup bad authenticators	Sum of responses received for backup accounting requests for each RADIUS accounting server where authenticators were mismatched.	detail

Table 33: show network-access aaa statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
Accounting backup responses dropped	Sum of responses for backup accounting requests for each RADIUS accounting server that were dropped due to various sanity checks.	detail
Accounting backup rollover requests	Sum of backup accounting requests rolled over for each RADIUS accounting server.	detail
Accounting backup unknown responses	Sum of unknown responses for backup accounting requests for each RADIUS accounting server.	detail
Client	Client type; for example, DHCP, Mobile IP, PPP.	none specified
Out of Memory	Number of times an address was not given to the client due to memory issues.	none specified
No Matches	Number of times there were no network matches for the pool.	none specified
Pool Name	Name of the address-assignment pool for this client.	none specified
Out of Addresses	Number of times there were no available addresses in the pool.	none specified
Address total	Number of addresses in the pool.	none specified
Addresses in use	Number of addresses in use.	none specified
Address Usage (percent)	Percentage of total addresses in use.	none specified
Pool drain configured	Configuration state of active drain for the specified local address pool, yes or no .	none specified
Pool Usage	Percentage of allocated addresses in the specified address pool.	none specified
processed successfully	Number of dynamic requests processed successfully by the AAA framework.	All levels
errors during processing	Number of dynamic requests that resulted in processing errors by the AAA framework.	All levels
Link Name	Name of the secondary address-assignment pool to which the primary pool is linked.	

Table 33: show network-access aaa statistics Output Fields (*continued*)

Field Name	Field Description	Level of Output
silently dropped	Number of dynamic requests dropped by the AAA framework due to multiple back-to-back or duplicate requests.	All levels
RADIUS Server	IPv4 or IPv6 address of the RADIUS server to which the router is sending requests.	All levels
Profile	Name of the RADIUS profile associated with the RADIUS server. A RADIUS server can be associated with more than one RADIUS profile.	All levels
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.	All levels
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.	All levels
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.	All levels
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.	All levels

Sample Output

show network-access aaa statistics accounting

```

user@host> show network-access aaa statistics accounting
Accounting module statistics
Accounting module statistics
Requests received: 5000
Accounting request timeouts: 2000
Accounting response failures: 0
Accounting response success: 3000

```

show network-access aaa statistics accounting detail

```

user@host> show network-access aaa statistics accounting detail
Accounting module statistics
Accounting module statistics
  Requests received: 5000
  Accounting request failures: 0
  Accounting request success: 5000
    Account on requests: 0
    Accounting start requests: 3000
    Accounting interim requests: 0
    Accounting stop requests: 2000
  Accounting request timeouts: 2000
  Accounting response failures: 0
  Accounting response success: 3000
    Account on responses: 0
    Accounting start responses: 3000
    Accounting interim responses: 0
    Accounting stop responses: 0
  Accounting rollover requests: 0
  Accounting unknown responses: 0
  Accounting radius pending requests: 0
  Accounting malformed responses: 0
  Accounting retransmissions: 6000
  Accounting bad authenticators: 0
  Accounting packets dropped: 0

  Accounting backup record creation requests: 3000
  Accounting backup request replay success: 9808
  Accounting backup request failures: 0
  Accounting backup request success: 3006
  Accounting backup timeouts: 6
  Accounting backup in-flight requests: 0
  Accounting backup responses success: 3000
  Accounting backup radius requests: 3006
  Accounting backup radius responses: 3000
  Accounting backup radius timeouts: 99
  Accounting backup radius pending requests: 0
  Accounting backup radius retransmissions: 99
  Accounting backup malformed responses: 0
  Accounting backup bad authenticators: 0
  Accounting backup responses dropped: 0
  Accounting backup rollover requests: 0
  Accounting backup unknown responses: 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
Pool drain configured: yes
```

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
198.51.100.239     prof1        1000         0         1000   14
                  prof2        500          17         432    0
198.51.100.211     myprof       200          0         200    27
203.0.113.254      pppoe-auth   111          0          1       0
2001:db8:0:f101::2 xyz-profile11 1000         10         135    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"> <i>Verifying and Managing Subscriber AAA Information</i>
List of Sample Output	show network-access aaa statistics authentication on page 589 show network-access aaa statistics authentication detail on page 589
Output Fields	Table 34 on page 587 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 34: 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

Table 34: show network-access aaa statistics authentication Output Fields (*continued*)

Field Name	Field Description	Level of Output
Malformed reply	Number of malformed replies received from the RADIUS authentication server.	Detail
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 subscribers

Syntax	<pre>show network-access aaa subscribers <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>> <statistics> <username> <session-id <i>session-id-number</i> detail></pre>
Release Information	<p>Command introduced in Junos OS Release 9.1.</p> <p>Command updated with session-id <i>session-id-number</i> detail in Junos OS Release 17.3.</p>
Description	Display subscriber-specific AAA statistics.
Options	<p>logical-system <i>logical-system-name</i>—(Optional) List subscribers in the specific logical system.</p> <p>routing-instance <i>routing-instance-name</i>—(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>statistics—(Optional) Display statistics for the subscriber events.</p> <p>username—(Optional) Display information for the specified subscriber.</p> <p>session-id <i>session-id-number</i> detail—(Optional) Display information for the specified session ID.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> <i>Verifying and Managing Subscriber AAA Information</i>
List of Sample Output	<p>show network-access aaa subscribers logical-system on page 592</p> <p>show network-access aaa subscribers logical-system routing-instance on page 592</p> <p>show network-access aaa subscribers statistics username on page 592</p> <p>show network-access aaa subscribers username on page 593</p> <p>show network-access aaa subscribers session-id 26 detail on page 593</p>
Output Fields	<p>Table 35 on page 590 lists the output fields for the show network-access aaa subscribers command. Output fields are listed in the approximate order in which they appear.</p>

Table 35: 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.

Table 35: show network-access aaa subscribers Output Fields (*continued*)

Field Name	Field Description
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.
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.
Stripped username	Username of the subscriber session.
AAA Logical system/Routing instance	AAA framework for the subscriber of logical system or routing instance.
Target Logical system/Routing instance	Target framework for the subscriber of logical system or routing instance.

Table 35: show network-access aaa subscribers Output Fields (*continued*)

Field Name	Field Description
Access-profile	Profile of the subscriber.
Accounting Session ID	ID of the subscriber session for accounting.
Multi Accounting Session ID	ID of the subscriber session for multiple accounting.
IP Address	IPv4 address of the subscriber.
IPv6 Address	IPv6 address of the subscriber.
IPv6 Prefix	IPv6 prefix of the subscriber.
Authentication State	State of subscriber session authentication.
Accounting State	State of subscriber session accounting.
Provisioning Type	Type of subscriber provisioning.

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
user61@example.net      ppp         default
00010e020304.1231      dhcp        isp-bos-metro-12:isp-cmborg-12
user54@example.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
user54@example.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 user80@example.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              on/volume
GamingBurst       time         6000 secs  on/volume

```

show network-access aaa subscribers session-id 26 detail

The following command output is seen when only an IPv4 client is associated with the session:

```

user@host> show network-access aaa subscribers session-id 26 detail
Type: dhcp
Stripped username: my-customer
AAA Logical system/Routing instance: default:default
Target Logical system/Routing instance: default:default
Access-profile: AccessProfile
Session ID: 26
Accounting Session ID: 26
Multi Accounting Session ID: 0
IP Address: 20.0.0.2
Authentication State: AuthStateActive
Accounting State: Acc-Interim-Sent
Provisioning Type: None

```

The following command output is seen when IPv6 client logs in (after IPv4 association) and is associated with the same session ID:

```

user@host> show network-access aaa subscribers session-id 26 detail
Type: dhcp
Stripped username: my-customer
AAA Logical system/Routing instance: default:default
Target Logical system/Routing instance: default:default
Access-profile: AccessProfile
Session ID: 26
Accounting Session ID: 26
Multi Accounting Session ID: 0
IP Address: 20.0.0.2
IPv6 Address: 3000:0:0:8003::2

```

IPv6 Prefix: 3ffe:ffff:0:4::/64
Authentication State: AuthStateActive
Accounting State: Acc-Interim-Sent
Provisioning Type: None

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 595
Output Fields	Table 36 on page 595 lists the output fields for the show network-access address-assignment pool command. Output fields are listed in the approximate order in which they appear.

Table 36: 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     00:00:5e:00:53:01 DHCP
192.168.2.2     00:00:5e:00:53:02 DHCP

```

192.168.2.3	00:00:5e:00:53:03	DHCP
192.168.2.4	00:00:5e:00:53:04	DHCP

show ppp interface

Syntax	<code>show ppp interface <i>interface-name</i></code> <code><extensive terse></code>
Release Information	Command introduced in Junos OS Release 7.5.
Description	Display information about PPP interfaces.
Options	<i>interface-name</i> —Name of a logical interface. extensive terse —(Optional) Display the specified level of output.
Required Privilege Level	view
List of Sample Output	show ppp interface on page 605 show ppp interface extensive on page 605 show ppp interface terse on page 605
Output Fields	Table 37 on page 597 lists the output fields for the show ppp interface command. Output fields are listed in the approximate order in which they appear.

Table 37: show ppp interface Output Fields

Field Name	Field Description	Level of Output
Session	Name of the logical interface on which the session is running.	All levels
Type	Session type: PPP.	All levels
Phase	PPP process phase: Authenticate , Pending , Establish , LCP , Network , Disabled , and Tunneled .	All levels
Session flags	Special conditions present in the session: Bundled , TCC , No-keepalives , Looped , Monitored , and NCP-only .	All levels
protocol State	Protocol state information. See specific protocol state fields for information.	None specified
AUTHENTICATION	Challenge-Handshake Authentication Protocol (CHAP) authentication state information or Password Authentication Protocol (PAP) state information. See the Authentication field description for further information.	None specified

Table 37: show ppp interface Output Fields (*continued*)

Field Name	Field Description	Level of Output
Keepalive settings	<p>Keepalive settings for the PPP sessions on the L2TP network server (LNS). LNS based PPP sessions are supported only on service interfaces (si).</p> <ul style="list-style-type: none"> • Interval—Time in seconds between successive keepalive requests. Keepalive aging timeout is calculated as a product of the interval and Down-count values. If the keepalive aging timeout is greater than 180 seconds, the keepalive packets are handled by the Routing Engine. If the aging timeout is less than or equal to 180 seconds, the packets are handled by the Packet Forwarding Engine. • Up-count—The number of keepalive packets a destination must receive to change a link's status from down to up. • Down-count—The number of keepalive packets a destination must fail to receive before the network takes down a link. 	extensive
RE Keepalive statistics	<p>Keepalive statistics for the packets handled by the Routing Engine.</p> <ul style="list-style-type: none"> • LCP echo req Tx—LCP echo requests sent from the Routing Engine. • LCP echo req Rx—LCP echo requests received at the Routing Engine. • LCP echo rep Tx—LCP echo responses sent from the Routing Engine. • LCP echo rep Rx—LCP echo responses received at the Routing Engine. • LCP echo req timeout—Number of keepalive packets where the keepalive aging timer has expired. • LCP Rx echo req Magic Num Failures—LCP echo requests where the magic numbers shared between the PPP peers during LCP negotiation did not match. • LCP Rx echo rep Magic Num Failures—LCP echo responses where the magic numbers shared between the PPP peers during LCP negotiation did not match. 	extensive

Table 37: show ppp interface Output Fields (*continued*)

Field Name	Field Description	Level of Output
LCP	<p>LCP information:</p> <ul style="list-style-type: none"> • State—LCP protocol state (all platforms except M120 and M320 routers): <ul style="list-style-type: none"> • Ack-rcvd—A Configure-Request has been sent and a Configure-Ack has been received. • Ack-sent—A Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received. • Closed—Link is not available for traffic. • Opened—Link is administratively available for traffic. • Req-sent—An attempt has been made to configure the connection. • State—LCP protocol state (M120 and M320 routers): <ul style="list-style-type: none"> • Ack-rcvd—A Configure-Request has been sent and a Configure-Ack has been received. • Ack-sent—A Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received. • Closed—Link is available (up), but no Open has occurred. • Closing—A Terminate-Request has been sent but a Terminate-Ack has not yet been received. • Opened—Link is administratively available for traffic. A Configure-Ack has been both sent and received. • Req-sent—An attempt has been made to configure the connection. A Configure-Request has been sent but a Configure-Ack has not yet been received. • Starting—An administrative Open has been initiated, but the lower layer is still unavailable (Down). • Stopped—The system is waiting for a Down event after the This-Layer-Finished action, or after sending a Terminate-Ack. • Stopping—A Terminate-Request has been sent but a Terminate-Ack has not yet been received. • Last started—LCP state start time. • Last completed—LCP state completion time. 	extensive

Table 37: show ppp interface Output Fields (*continued*)

Field Name	Field Description	Level of Output
	<ul style="list-style-type: none"> • Negotiated options: <ul style="list-style-type: none"> • ACFC—Address and-Control Field Compression. A configuration option that provides a method to negotiate the compression of the Data Link Layer Address and Control fields. • Asynchronous map—Asynchronous control character map. A configuration option used on asynchronous links such as telephone lines to identify control characters that must be replaced by a two-character sequence to prevent them from being interpreted by equipment used to establish the link. • Authentication protocol—Protocol used for authentication. This option provides a method to negotiate the use of a specific protocol for authentication. It requires a peer to authenticate itself before allowing network-layer protocol packets to be exchanged. By default, authentication is not required. • Authentication algorithm—Type of authentication algorithm. The Message Digest algorithm (MD5) is the only algorithm supported. • Endpoint discriminator class—For multilink PPP (MLPPP), a configuration option that identifies the system transmitting the packet. This option advises a system that the peer on this link could be the same as the peer on another existing link. • Magic number—A configuration option that provides a method to detect looped-back links and other data-link layer anomalies. By default, the magic number is not negotiated. • MRU—Maximum receive unit. A configuration option that may be sent to inform the peer that the implementation can receive larger packets, or to request that the peer send smaller packets. The default value is 1500 octets. • MRRU—For multilink PPP, the maximum receive reconstructed unit. A configuration option that specifies the maximum number of octets in the Information fields of reassembled packets. • Multilink header suspendable classes—For MLPPP, an LCP option that advises the peer that the implementation wishes to receive fragments with a format given by the code number, with the maximum number of suspendable classes given. • Multilink header format classes—For MLPPP, an LCP option that advises the peer that the implementation wishes to receive fragments with a format given by the code number. • PFC—Protocol-Field-Compression. A configuration option that provides a method to negotiate the compression of the PPP Protocol field. • short sequence—For MLPPP, an option that advises the peer that the implementation wishes to receive fragments with short, 12-bit sequence numbers. 	

Table 37: show ppp interface Output Fields (*continued*)

Field Name	Field Description	Level of Output
Authentication	<p>CHAP or PAP authentication state information. For CHAP authentication:</p> <ul style="list-style-type: none"> • Chap-ans-rcvd—Packet was sent from the peer, indicating that the peer received the Chap-resp-sent packet. • Chap-ans-sent—Packet was sent from the authenticator, indicating that the authenticator received the peer's Chap-resp-rcvd packet. • Chap-chal-rcvd—Challenge packet has been received by the peer. • Chap-chal-sent—Challenge packet has been sent by the authenticator to begin the CHAP protocol or has been transmitted at any time during the Network-Layer Protocol (NCP) phase to ensure that the connection has not been altered. • Chap-resp-rcvd—CHAP response packet has been received by the authenticator. • Chap-resp-sent—CHAP response packet has been sent to the authenticator. • Closed—Link is not available for authentication. • Failure—Authenticator compares the response value in the response packet from the peer with its own response value, but the value does not match. Authentication fails. • Success—Authenticator compares the response value in the response packet from the peer with its own response value, and the value matches. Authentication is successful. <p>For PAP authentication:</p> <ul style="list-style-type: none"> • Pap-resp-sent—PAP response sent to peer (ACK/NACK). • Pap-req-rcvd—PAP request packet received from peer. • Pap-resp-rcvd—PAP response received from the peer (ACK/NACK). • Pap-req-sent—PAP request packet sent to the peer. • Closed—Link is not available for authentication. • Failure—Authenticator compares the response value in the response packet from the peer with its own response value, but the value does not match. Authentication fails. • Success—Authenticator compares the response value in the response packet from the peer with its own response value, and the value matches. Authentication is successful. 	None specified

Table 37: show ppp interface Output Fields (*continued*)

Field Name	Field Description	Level of Output
IPCP	<p>Internet Protocol Control Protocol (IPCP) information.</p> <ul style="list-style-type: none"> • State—(All platforms except M120 and M320 routers) One of the following values: <ul style="list-style-type: none"> • Ack-rcvd—A Configure-Request has been sent and a Configure-Ack has been received. • Ack-sent—A Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received. • Closed—Link is not available for traffic. • Opened—Link is administratively available for traffic. • Req-sent—An attempt has been made to configure the connection. • State—(M120 and M320 routers) One of the following values: <ul style="list-style-type: none"> • Ack-rcvd—A Configure-Request has been sent and a Configure-Ack has been received. • Ack-sent—A Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received. • Closed—Link is available (up), but no Open has occurred. • Closing—A Terminate-Request has been sent but a Terminate-Ack has not yet been received. • Opened—Link is administratively available for traffic. A Configure-Ack has been both sent and received. • Req-sent—An attempt has been made to configure the connection. A Configure-Request has been sent but a Configure-Ack has not yet been received. • Starting—An administrative Open has been initiated, but the lower layer is still unavailable (Down). • Stopped—The system is waiting for a Down event after the This-Layer-Finished action, or after sending a Terminate-Ack. • Stopping—A Terminate-Request has been sent but a Terminate-Ack has not yet been received. • Last started—IPCP state start time. • Last completed—IPCP state authentication completion time. • Negotiated options: <ul style="list-style-type: none"> • compression protocol—Negotiate the use of a specific compression protocol. By default, compression is not enabled. • local address—Desired local address of the sender of a Configure-Request. If all four octets are set to zero, the peer provides the IP address. • primary DNS server—Negotiate with the remote peer to select the address of the primary DNS server to be used on the local end of the link. • primary WINS server—Negotiate with the remote peer to select the address of the primary WINS server to be used on the local end of the link. • remote address—IP address of the remote end of the link in dotted quad notation. • secondary DNS server—Negotiate with the remote peer to select the address of the secondary DNS server to be used on the local end of the link. • secondary WINS server—Negotiate with the remote peer to select the address of the secondary WINS server to be used on the local end of the link. • Negotiation mode—PPP Network Control Protocol (NCP) negotiation mode configured for IPCP: Active or Passive 	extensive

Table 37: show ppp interface Output Fields (*continued*)

Field Name	Field Description	Level of Output
IPV6CP	<p>Internet Protocol version 6 Control Protocol (IPv6CP) information.</p> <ul style="list-style-type: none"> • State—(All platforms except M120 and M320 routers) One of the following values: <ul style="list-style-type: none"> • Ack-rcvd—A Configure-Request has been sent and a Configure-Ack has been received. • Ack-sent—A Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received. • Closed—Link is not available for traffic. • Opened—Link is administratively available for traffic. • Req-sent—An attempt has been made to configure the connection. • State—(M120 and M320 routers) One of the following values: <ul style="list-style-type: none"> • Ack-rcvd—A Configure-Request has been sent and a Configure-Ack has been received. • Ack-sent—A Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received. • Closed—Link is available (up), but no Open has occurred. • Closing—A Terminate-Request has been sent but a Terminate-Ack has not yet been received. • Opened—Link is administratively available for traffic. A Configure-Ack has been both sent and received. • Req-sent—An attempt has been made to configure the connection. A Configure-Request has been sent but a Configure-Ack has not yet been received. • Starting—An administrative Open has been initiated, but the lower layer is still unavailable (Down). • Stopped—The system is waiting for a Down event after the This-Layer-Finished action, or after sending a Terminate-Ack. • Stopping—A Terminate-Request has been sent but a Terminate-Ack has not yet been received. • Last started—IPv6CP state start time. • Last completed—IPv6CP state authentication completion time. • Negotiated options: <ul style="list-style-type: none"> • local interface identifier—Desired local address of the sender of a Configure-Request. If all four octets are set to zero, the peer provides the IP address. • remote interface identifier—IP address of the remote end of the link in dotted quad notation. • Negotiation mode—PPP Network Control Protocol (NCP) negotiation mode configured for IPv6CP: Active or Passive 	extensive

Table 37: show ppp interface Output Fields (*continued*)

Field Name	Field Description	Level of Output
OSINLCP State	<p>OSI Network Layer Control Protocol (OSINLCP) protocol state information (all platforms except M120 and M320 routers):</p> <ul style="list-style-type: none"> • State: <ul style="list-style-type: none"> • Ack-rcvd—Configure-Request has been sent and Configure-Ack has been received. • Ack-sent—Configure-Request and Configure-Ack have both been sent, but Configure-Ack has not yet been received. • Closed—Link is not available for traffic. • Opened—Link is administratively available for traffic. • Req-sent—Attempt has been made to configure the connection. • Last started—OSINLCP state start time. • Last completed—OSINLCP state completion time. 	extensive
TAGCP	<p>TAGCP information.</p> <ul style="list-style-type: none"> • State—(All platforms except M120 and M320 routers) One of the following values: <ul style="list-style-type: none"> • Ack-rcvd—A Configure-Request has been sent and a Configure-Ack has been received. • Ack-sent—A Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received. • Closed—Link is not available for traffic. • Opened—Link is administratively available for traffic. • Req-sent—An attempt has been made to configure the connection. • State—(M120 and M320 routers) One of the following values: <ul style="list-style-type: none"> • Ack-rcvd—A Configure-Request has been sent and a Configure-Ack has been received. • Ack-sent—A Configure-Request and a Configure-Ack have both been sent, but a Configure-Ack has not yet been received. • Closed—Link is available (up), but no Open has occurred. • Closing—A Terminate-Request has been sent but a Terminate-Ack has not yet been received. • Opened—Link is administratively available for traffic. A Configure-Ack has been both sent and received. • Req-sent—An attempt has been made to configure the connection. A Configure-Request has been sent but a Configure-Ack has not yet been received. • Starting—An administrative Open has been initiated, but the lower layer is still unavailable (Down). • Stopped—The system is waiting for a Down event after the This-Layer-Finished action, or after sending a Terminate-Ack. • Stopping—A Terminate-Request has been sent but a Terminate-Ack has not yet been received. • Last started—TAGCP state start time. • Last completed—TAGCP state authentication completion time. 	extensive none

Sample Output

show ppp interface

```
user@host> show ppp interface si-1/3/0.0
Session si-1/3/0.0, Type: PPP, Phase: Authenticate
Session flags: Monitored
LCP State: Opened
AUTHENTICATION: CHAP State: Chap-resp-sent, Chap-ans-sent
IPCP State: Closed, OSINLCP State: Closed
```

show ppp interface extensive

```
user@host> show ppp interface si-0/0/3.0 extensive

Session si-0/0/3.0, Type: PPP, Phase: Network
Keepalive settings: Interval 30 seconds, Up-count 1, Down-count 3
RE Keepalive statistics:
LCP echo req Tx      : 657 (last sent 00:50:10 ago)
LCP echo req Rx      : 0 (last seen: never)
LCP echo rep Tx      : 0
LCP echo rep Rx      : 657
LCP echo req timeout : 0
LCP Rx echo req Magic Num Failures : 0
LCP Rx echo rep Magic Num Failures : 0
LCP
State: Opened
Last started: 2007-01-29 10:43:50 PST
Last completed: 2007-01-29 10:43:50 PST
Negotiated options:
Authentication protocol: PAP, Magic number: 2341124815, MRU: 4470
Authentication: PAP
State: Success
Last started: 2007-01-29 10:43:50 PST
Last completed: 2007-01-29 10:43:50 PST
IPCP
State: Opened
Last started: 2007-01-29 10:43:50 PST
Last completed: 2007-01-29 10:43:50 PST
Negotiated options:
Local address: 203.0.113.21, Remote address: 203.0.113.22
Negotiation mode: Active
IPV6CP
State: Opened
Last started: 2007-01-29 10:43:50 PST
Last completed: 2007-01-29 10:43:50 PST
Negotiated options:
Local interface identifier: 2a0:a522:64:d319, Remote interface identifier: 0:0:0:c
Negotiation mode: Passive
```

show ppp interface terse

```
user@host> show ppp interface si-1/3/0 terse
Session name  Session type  Session phase  Session flags
si-1/3/0.0    PPP           Authenticate    Monitored
```

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.
 Command introduced in Junos OS Release 15.1R3 on MX Series routers for enhanced subscriber management.

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, 192.0.2.0). If you specify the IP address as a prefix with a netmask (for example, 192.0.2.0/32), 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 one of the following client types:

- **dhcp**—DHCP clients only.
- **dot1x**—Dot1x clients only.
- **essm**—ESSM clients only.
- **fwauth**—FwAuth (authenticated across a firewall) clients only.
- **l2tp**—L2TP clients only.
- **mlppp**—MLPPP clients only.
- **ppp**—PPP clients only.
- **pppoe**—PPPoE clients only.
- **static**—Static clients only.
- **vlan**—VLAN clients only.
- **vlan-oob**—VLAN out-of-band (ANCP-triggered) clients only.
- **vpls-pw**—VPLS pseudowire clients only.
- **xauth**—Xauth clients only.

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 65,535.

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: Because of display limitations, logical system and routing instance output values are truncated when necessary.

Required Privilege Level

view

Related Documentation

- [show subscribers summary on page 632](#)
- *Verifying and Managing Agent Circuit Identifier-Based Dynamic VLAN Configuration*
- *Verifying and Managing Configurations for Dynamic VLANs Based on Access-Line Identifiers*
- *Verifying and Managing Junos OS Enhanced Subscriber Management*

List of Sample Output

[show subscribers \(IPv4\) on page 615](#)
[show subscribers \(IPv6\) on page 615](#)

[show subscribers \(IPv4 and IPv6 Dual Stack\) on page 615](#)
[show subscribers \(Single Session DHCP Dual Stack\) on page 615](#)
[show subscribers \(Single Session DHCP Dual Stack detail\) on page 616](#)
[show subscribers \(LNS on MX Series Routers\) on page 616](#)
[show subscribers \(L2TP Switched Tunnels\) on page 616](#)
[show subscribers client-type dhcp detail on page 616](#)
[show subscribers client-type vlan-oob detail on page 617](#)
[show subscribers count on page 617](#)
[show subscribers address detail \(IPv6\) on page 617](#)
[show subscribers detail \(IPv4\) on page 618](#)
[show subscribers detail \(IPv6\) on page 618](#)
[show subscribers detail \(pseudowire Interface for GRE Tunnel\) on page 618](#)
[show subscribers detail \(IPv6 Static Demux Interface\) on page 619](#)
[show subscribers detail \(L2TP LNS Subscribers on MX Series Routers\) on page 619](#)
[show subscribers detail \(L2TP Switched Tunnels\) on page 619](#)
[show subscribers detail \(Tunneled Subscriber\) on page 620](#)
[show subscribers detail \(IPv4 and IPv6 Dual Stack\) on page 620](#)
[show subscribers detail \(ACI Interface Set Session\) on page 621](#)
[show subscribers detail \(PPPoE Subscriber Session with ACI Interface Set\) on page 621](#)
[show subscribers extensive on page 621](#)
[show subscribers extensive \(Passive Optical Network Circuit Interface Set\) on page 622](#)
[show subscribers extensive \(DNS Addresses from Access Profile or Global Configuration\) on page 622](#)
[show subscribers extensive \(DNS Addresses from RADIUS\) on page 623](#)
[show subscribers extensive \(IPv4 DNS Addresses from RADIUS, IPv6 from Access Profile or Global Configuration\) on page 623](#)
[show subscribers extensive \(RPF Check Fail Filter\) on page 624](#)
[show subscribers extensive \(L2TP LNS Subscribers on MX Series Routers\) on page 624](#)
[show subscribers extensive \(IPv4 and IPv6 Dual Stack\) on page 624](#)
[show subscribers extensive \(ADF Rules \) on page 625](#)
[show subscribers extensive \(Effective Shaping-Rate\) on page 626](#)
[show subscribers extensive \(Subscriber Session Using PCEF Profile\) on page 626](#)
[show subscribers aci-interface-set-name detail \(Subscriber Sessions Using Specified ACI Interface Set\) on page 627](#)
[show subscribers agent-circuit-identifier detail \(Subscriber Sessions Using Specified ACI Substring\) on page 628](#)
[show subscribers interface extensive on page 628](#)
[show subscribers logical-system terse on page 629](#)
[show subscribers physical-interface count on page 629](#)
[show subscribers routing-instance inst1 count on page 629](#)
[show subscribers stacked-vlan-id detail on page 629](#)
[show subscribers stacked-vlan-id vlan-id detail \(Combined Output\) on page 629](#)
[show subscribers stacked-vlan-id vlan-id interface detail \(Combined Output for a Specific Interface\) on page 630](#)
[show subscribers user-name detail on page 630](#)
[show subscribers vlan-id on page 630](#)
[show subscribers vlan-id detail on page 630](#)
[show subscribers vpi vci extensive \(PPPoE-over-ATM Subscriber Session\) on page 631](#)
[show subscribers address detail \(Enhanced Subscriber Management\) on page 631](#)

Output Fields Table 38 on page 610 lists the output fields for the **show subscribers** command. Output fields are listed in the approximate order in which they appear.

Table 38: 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, GRE, L2TP, PPP, PPPoE, STATIC-INTERFACE, VLAN).
IP Address	Subscriber IPv4 address.
IP Netmask	Subscriber IP netmask. (MX Series) This field displays 255.255.255.255 by default. For tunneled or terminated PPP subscribers only, this field displays the actual value of Framed-IP-Netmask when the SDB_FRAMED_PROTOCOL attribute in the session database is equal to AUTHD_FRAMED_PROTOCOL_PPP. This occurs in the use case where the LNS generates access-internal routes when it receives Framed-IP-Netmask from RADIUS during authorization. When it receives Framed-Pool from RADIUS, the pool mask is ignored and the default /32 mask is used.
Primary DNS Address	IP address of primary DNS server. This field is displayed with the extensive option only when the address is provided by RADIUS.
Secondary DNS Address	IP address of secondary DNS server. This field is displayed with the extensive option only when the address is provided by RADIUS.
IPv6 Primary DNS Address	IPv6 address of primary DNS server. This field is displayed with the extensive option only when the address is provided by RADIUS.
IPv6 Secondary DNS Address	IPv6 address of secondary DNS server. This field is displayed with the extensive option only when the address is provided by RADIUS.
Domain name server inet	IP addresses for the DNS server, displayed in order of configuration. This field is displayed with the extensive option only when the addresses are derived from the access profile or the global access configuration.

Table 38: show subscribers Output Fields (*continued*)

Field Name	Field Description
Domain name server inet6	IPv6 addresses for the DNS server, displayed in order of configuration. This field is displayed with the extensive option only when the addresses are derived from the access profile or the global access configuration.
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.
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	(Enhanced subscriber management for MX Series routers) Name of the enhanced subscriber management logical interface, in the form demux0.nnnn (for example, demux0.3221225472), to which access-internal and framed subscriber routes are mapped.
Interface Type	Whether the subscriber interface is Static or Dynamic .

Table 38: show subscribers Output Fields (*continued*)

Field Name	Field Description
Interface Set	<p>Internally generated name of the dynamic ACI or ALI interface set used by the subscriber session. The prefix of the name indicates the string received in DHCP or PPPoE control packets on which the interface set is based. For ALI interface sets, the prefix indicates that the value is configured as a trusted option to identify the subscriber line.</p> <p>The name of the interface set uses one of the following prefixes:</p> <ul style="list-style-type: none"> • aci—ACI; for example, aci-1033-demux0.3221225524. This is the only prefix allowed for ACI interface sets. • ari—ARI; for example, ari-1033-demux0.3221225524. • aci+ari—Both the ACI and ARI; for example, aci+ari-1033-demux0.3221225524. • noids—Neither the ACI nor the ARI were received; for example, noids-1033-demux0.3221225524. <p>NOTE: ACI interface sets are configured with the agent-circuit-identifier autoconfiguration stanza. ALI interface sets are configured with the line-identity autoconfiguration stanza.</p> <p>Besides dynamic ACI and ALI interface sets, this field can be an interface set based on a substring of the ARI string. This occurs when the dynamic profile includes the predefined variable \$junos-pon-id-interface-set-name, and the profile is applied for a passive optical network (PON). The ARI string is inserted by the optical line terminal (OLT). The final substring in the string, unique for the PON, identifies individual subscriber circuits, and is used as the name of the interface set.</p>
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> .

Table 38: show subscribers Output Fields (*continued*)

Field Name	Field Description
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	<p>For the dhcp client type, 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.</p> <p>For the vlan-oob client type, the agent circuit ID or access-loop circuit identifier that identifies the subscriber line based on the subscriber-facing DSLAM interface on which the subscriber request originates.</p>
Agent Remote ID	<p>For the dhcp client type, 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.</p> <p>For the vlan-oob client type, the agent remote ID or access-loop remote identifier that identifies the subscriber line based on the NAS-facing DSLAM interface on which the subscriber request originates.</p>
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 Input Service Set	Input service set in access dynamic profile.
IPv4 Output Service Set	Output service set in access dynamic profile.
PCEF Profile	PCEF profile in access dynamic profile.
PCEF Rule/Rulebase	PCC rule or rulebase used in dynamic profile.
Dynamic configuration	Values for variables that are passed into the dynamic profile from RADIUS.
Service activation time	Time at which the first family in this service became active.
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.

Table 38: show subscribers Output Fields (*continued*)

Field Name	Field Description
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-Ipv6-Prefix AAA attribute. This field is displayed only when the predefined variable \$junos-ipv6-address is used in the dynamic profile.
IPv6 Framed Interface Id	Interface ID assigned by the Framed-Interface-Id AAA attribute.
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).

Table 38: show subscribers Output Fields (*continued*)

Field Name	Field Description
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 10                   WHOLESALE-CLIENT default:default
demux0.1073741824   203.0.113.10        RETAILER1-CLIENT test1:retailer1
demux0.1073741825   203.0.113.3         RETAILER2-CLIENT test1:retailer2
demux0.1073741826   203.0.113.3         RETAILER2-CLIENT test1:retailer2

```

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     203.0.113.13        dualstackuser1@example1.com
*                  2001:db8:1::/48
*                  2001:db8:1:1::/64
pp0.1073741837     203.0.113.33        dualstackuser2@example1.com
*                  2001:db8:1:2:5::/64

```

show subscribers (Single Session DHCP Dual Stack)

```
user@host> show subscribers
```

```

Interface          IP Address/VLAN ID  User Name          LS:RI
demux0.1073741364  192.168.10.10       dual-stack-retail35 default:default
                  2001:db8::100:0:0:0/74 default:default
                  2001:db8:3ffe:0:4::/64

```

show subscribers (Single Session DHCP Dual Stack detail)

```
user@host> show subscribers id 27 detail
Type: DHCP
User Name: dual-stack-retail33
IP Address: 10.10.0.53
IPv6 Address: 2001:db8:3000:0:0:8003::2
IPv6 Prefix: 2001:db8:3ffe:0:4::/64
Logical System: default
Routing Instance: default
Interface: ae0.3221225472
Interface type: Static
Underlying Interface: ae0.3221225472
Dynamic Profile Name: dhcp-retail-18
MAC Address: 00:00:5E:00:53:02
State: Active
DHCP Relay IP Address: 10.10.0.1
Radius Accounting ID: 27
Session ID: 27
PFE Flow ID: 2
Stacked VLAN Id: 2000
VLAN Id: 1
Login Time: 2014-05-15 10:12:10 PDT
DHCP Options: len 60
00 08 00 02 00 00 00 01 00 0a 00 03 00 01 00 00 64 01 01 02
00 06 00 04 00 03 00 19 00 03 00 0c 00 00 00 00 00 00 00 00
00 00 00 00 00 19 00 0c 00 00 00 00 00 00 00 00 00 00 00 00
```

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     192.0.2.0           user@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    user@example.com default:default
si-2/1/0.1073741843 Tunnel-switched    user@example.com default:default
```

show subscribers client-type dhcp detail

```
user@host> show subscribers client-type dhcp detail
Type: DHCP
IP Address: 203.0.113.29
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux
MAC Address: 00:00:5e:00:53:98
State: Active
Radius Accounting ID: user :2304
Login Time: 2009-08-25 14:43:52 PDT
```

```

Type: DHCP
IP Address: 203.0.113.27
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: 00:00:5e:00:53:f3
State: Active
Radius Accounting ID: 1234 :2560
Login Time: 2009-08-25 14:43:56 PDT

```

show subscribers client-type vlan-oob detail

```

user@host> show subscribers client-type vlan-oob detail
Type: VLAN-00B
User Name: L2WS.line-aci-1.line-ari-1
Logical System: default
Routing Instance: ISP1
Interface: demux0.1073744127
Interface type: Dynamic
Underlying Interface: ge-1/0/0
Dynamic Profile Name: Prof_L2WS
Dynamic Profile Version: 1
State: Active
Radius Accounting ID: 1234
Session ID: 77
VLAN Id: 126
Core-Facing Interface: ge-2/1/1
VLAN Map Id: 6
Inner VLAN Map Id: 2001
Agent Circuit ID: line-aci-1
Agent Remote ID: line-ari-1
Login Time: 2013-10-29 14:43:52 EDT

```

show subscribers count

```

user@host> show subscribers count
Total Subscribers: 188, Active Subscribers: 188

```

show subscribers address detail (IPv6)

```

user@host> show subscribers address 203.0.113.137 detail
Type: PPPoE
User Name: pppoeTerV6User1Svc
IP Address: 203.0.113.137
IP Netmask: 255.0.0.0
IPv6 User Prefix: 2001:db8:0:c88::/32
Logical System: default
Routing Instance: default
Interface: pp0.1073745151
Interface type: Dynamic
Underlying Interface: demux0.8201
Dynamic Profile Name: pppoe-client-profile
MAC Address: 00:00:5e:00:53:53
Session Timeout (seconds): 31622400
Idle Timeout (seconds): 86400
State: Active
Radius Accounting ID: example 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: 203.0.113.29
IP Netmask: 255.255.0.0
Primary DNS Address: 192.0.2.0
Secondary DNS Address: 192.0.2.1
Primary WINS Address: 192.0.2.3
Secondary WINS Address: 192.0.2.4
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:00:5e:00:53:98
State: Active
Radius Accounting ID: example :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:ffff:1::/32
Logical System: default
Routing Instance: default
Interface: ge-3/1/3.2
Interface type: Static
MAC Address: 00:00:5e:00:53:03
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 (pseudowire Interface for GRE Tunnel)

```
user@host> show subscribers detail
Interface      IP Address/VLAN ID  User Name  LS:RI
ps0.3221225484 30.1.0.2
ps0.3221225485 30.1.0.3
demux0.3221225486 1                                default:default
```


demux0.3221225487	1	default:default
demux0.3221225488	100.16.0.1	default:default
demux0.3221225489	100.16.0.2	default:default

show subscribers detail (IPv6 Static Demux Interface)

```

user@host> show subscribers detail
Type: STATIC-INTERFACE
User Name: user@example.net
IPv6 Prefix: 2001:db8:3:4:5:6:7:aa/32
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: user@example.net
IP Address: 203.0.113.58
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: user@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: 203.0.113.51
Remote IP Address: 192.0.2.0
Radius Accounting ID: 21
Session ID: 21
Login Time: 2013-01-18 03:01:11 PST

Type: L2TP

```

```
User Name: user@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: 203.0.113.31
Remote IP Address: 192.0.2.1
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: 203.0.113.13
IPv6 Prefix: 2001:db8:1::/32
IPv6 User Prefix: 2001:db8:1:1::/32
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: dualStack-Profile1
MAC Address: 00:00:5e:00:53:02
State: Active
Radius Accounting ID: 2
Session ID: 2
Login Time: 2011-11-30 00:18:05 PST

Type: DHCP
IPv6 Prefix: 2001:db8:1::/32
Logical System: default
Routing Instance: ASP-1
```

```

Interface: pp0.1073741825
Interface type: Static
MAC Address: 00:00:5e:00:53:02
State: Active
Radius Accounting ID: test :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: 203.0.113.15
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: 00:00:5e:00:53:02
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:ffff:1::/32

```

```
Logical System: default
Routing Instance: default
Interface: ge-3/1/3.2
Interface type: Static
MAC Address: 00:00:5e:00:53:03
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 (Passive Optical Network Circuit Interface Set)

```
user@host> show subscribers client-type dhcp extensive
Type: DHCP
IP Address: 192.0.2.136
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073741842
Interface type: Dynamic
Interface Set: ot101.xyz101-202
Underlying Interface: demux0.1073741841
Dynamic Profile Name: dhcp-profile
MAC Address: 00:10:94:00:00:02
State: Active
Radius Accounting ID: jnpr :19
Session ID: 19
VLAN Id: 1100
Agent Remote ID: ABCD01234|100M|AAAA01234|ot101.xyz101-202

Login Time: 2017-03-29 10:30:46 PDT
DHCP Options: len 97
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 02 33 04 00 00
17 70 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 32 2f
32 2d 31 2d 31 37 05 01 06 0f 21 2c 52 2b 02 29 41 42 43 44
30 31 32 33 34 7c 31 30 30 4d 7c 41 41 41 41 30 31 32 33 34
7c 6f 74 6c 30 31 2e 78 79 7a 31 30 31 2d 32 30 32
IP Address Pool: POOL-V4
```

show subscribers extensive (DNS Addresses from Access Profile or Global Configuration)

```
user@host> show subscribers extensive
Type: DHCP
User Name: test-user@example-com
IP Address: 192.0.2.119
IP Netmask: 255.255.255.255
Domain name server inet: 198.51.100.1 198.51.100.2
IPv6 Address: 2001:db8::1:11
Domain name server inet6: 2001:db8:5001::12 2001:db8:3001::12
Logical System: default
Routing Instance: default
Interface: ge-2/0/3.0
Interface type: Static
Underlying Interface: ge-2/0/3.0
```

```

MAC Address: 00:00:5E:00:53:00
State: Active
Radius Accounting ID: 5
Session ID: 5
Login Time: 2017-01-31 11:16:21 IST
DHCP Options: len 53
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 03 33 04 00 00
00 3c 0c 16 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 35 2f
31 32 2d 30 2d 30 37 05 01 06 0f 21 2c
IP Address Pool: v4-pool

```

show subscribers extensive (DNS Addresses from RADIUS)

```

user@host> show subscribers extensive
Type: DHCP
User Name: test-user@example-com
IP Address: 192.0.2.119
IP Netmask: 255.255.255.255
Primary DNS Address: 198.51.100.1
Secondary DNS Address: 198.51.100.2
IPv6 Address: 2001:db8::1:11
IPv6 Primary DNS Address: 2001:db8:5001::12
IPv6 Secondary DNS Address: 2001:db8:3001::12
Logical System: default
Routing Instance: default
Interface: ge-2/0/3.0
Interface type: Static
Underlying Interface: ge-2/0/3.0
MAC Address: 00:00:5E:00:53:00
State: Active
Radius Accounting ID: 5
Session ID: 5
Login Time: 2017-01-31 11:16:21 IST
DHCP Options: len 53
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 03 33 04 00 00
00 3c 0c 16 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 35 2f
31 32 2d 30 2d 30 37 05 01 06 0f 21 2c
IP Address Pool: v4-pool

```

show subscribers extensive (IPv4 DNS Addresses from RADIUS, IPv6 from Access Profile or Global Configuration)

```

user@host> show subscribers extensive
Type: DHCP
User Name: test-user@example-com
IP Address: 192.0.2.119
IP Netmask: 255.255.255.255
Primary DNS Address: 198.51.100.1
Secondary DNS Address: 198.51.100.2
IPv6 Address: 2001:db8::1:11
Domain name server inet6: 2001:db8:5001::12 2001:db8:3001::12
Logical System: default
Routing Instance: default
Interface: ge-2/0/3.0
Interface type: Static
Underlying Interface: ge-2/0/3.0
MAC Address: 00:00:5E:00:53:00
State: Active
Radius Accounting ID: 5
Session ID: 5
Login Time: 2017-01-31 11:16:21 IST

```

```
DHCP Options: len 53
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 03 33 04 00 00
00 3c 0c 16 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 35 2f
31 32 2d 30 2d 30 37 05 01 06 0f 21 2c
IP Address Pool: v4-pool
```

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: user@example.net
IP Address: 203.0.113.58
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: 203.0.113.13
IPv6 Prefix: 2001:db8:1::/32
IPv6 User Prefix: 2001:db8:1:1::/32
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: dualStack-Profile1
MAC Address: 00:00:5e:00:53:02
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: 2001:db8:2016:1:1::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: 2001:db8:1::/32
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Static
MAC Address: 00:00:5e:00:53:02
State: Active
Radius Accounting ID: test :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
IPv6 Delegated Network Prefix Length: 48

```

show subscribers extensive (ADF Rules)

```

user@host> show subscribers extensive
...
Service Session ID: 12
Service Session Name: SERVICE-PROFILE
State: Active
Family: inet
  ADF IPv4 Input Filter Name: __junos_adf_12-demux0.3221225474-inet-in
    Rule 0: 010101000b0101020b020200201811
      from {
        source-address 203.0.113.232;
        destination-address 198.51.100.0/24;
        protocol 17;
      }
      then {
        accept;
      }
    }

```

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 extensive (Subscriber Session Using PCEF Profile)

```
user@host> show subscribers extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.3221225517
Interface type: Dynamic
Underlying Interface: ge-1/0/3
Dynamic Profile Name: svlan-dhcp
State: Active
Session ID: 59
PFE Flow ID: 71
Stacked VLAN Id: 0x8100.1
VLAN Id: 0x8100.2
Login Time: 2017-03-28 08:23:08 PDT

Type: DHCP
User Name: pcefuser
IP Address: 5.0.0.26
IP Netmask: 255.0.0.0
Logical System: default
Routing Instance: default
Interface: demux0.3221225518
Interface type: Dynamic
Underlying Interface: demux0.3221225517
Dynamic Profile Name: dhcp-client-prof
MAC Address: 00:11:01:00:00:01
State: Active
Radius Accounting ID: 60
Session ID: 60
PFE Flow ID: 73
Stacked VLAN Id: 1
VLAN Id: 2
Login Time: 2017-03-28 08:23:08 PDT
Service Sessions: 1
DHCP Options: len 9
35 01 01 37 04 01 03 3a 3b
IP Address Pool: pool-ipv4
IPv4 Input Service Set: tdf-service-set
IPv4 Output Service Set: tdf-service-set
```



```

PCEF Profile: pcef-prof-1
PCEF Rule/Rulebase: default
Dynamic configuration:
  junos-input-service-filter: svc-filt-1
  junos-input-service-set: tdf-service-set
  junos-output-service-filter: svc-filt-1
  junos-output-service-set: tdf-service-set
  junos-pcef-profile: pcef-prof-1
  junos-pcef-rule: default

Service Session ID: 61
Service Session Name: pcef-serv-prof
State: Active
Family: inet
IPv4 Input Service Set: tdf-service-set
IPv4 Output Service Set: tdf-service-set
PCEF Profile: pcef-prof-1
PCEF Rule/Rulebase: limit-fb
Service Activation time: 2017-03-28 08:31:19 PDT
Dynamic configuration:
  pcef-prof: pcef-prof-1
  pcef-rule1: limit-fb
  svc-filt: svc-filt-1
  svc-set: tdf-service-set

```

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: 203.0.113.17
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:
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: 203.0.113.17
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: 00:00:5e:00:53:52
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: user@test.example.com
Logical System: default
Routing Instance: testnet
Interface: demux0.1073741826
Interface type: Dynamic
Dynamic Profile Name: profile-vdemux-relay-23qos
MAC Address: 00:00:5e:00:53:04
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: user@test.example.com
IP Address: 192.0.2.0
IP Netmask: 255.255.255.0
Logical System: default
Routing Instance: testnet
Interface: demux0.1073741826
```

```

Interface type: Static
MAC Address: 00:00:5e:00:53:04
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  203.0.113.3         RETAILER1-CLIENT  test1:retailer1
demux0.1073741826  203.0.113.4         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: 203.0.113.37
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: 00:00:5e:00:53:01
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: 203.0.113.2
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: pp0.0
Interface type: Static
MAC Address: 00:00:5e:00:53:02
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 address detail (Enhanced Subscriber Management)

```

user@host> show subscribers address 203.0.113.111 detail
Type: DHCP
User Name: simple_filters_service
IP Address: 203.0.113.111
IP Netmask: 255.0.0.0
Logical System: default
Routing Instance: default
Interface: demux0.3221225482
Interface type: Dynamic
Underlying Interface: demux0.3221225472
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:00:5e:00:53:0f
State: Active
Radius Accounting ID: 11
Session ID: 11
PFE Flow ID: 15
Stacked VLAN Id: 210
VLAN Id: 209
Login Time: 2014-03-24 12:53:48 PDT
Service Sessions: 1
DHCP Options: len 3
35 01 01

```

show subscribers summary

Syntax show subscribers summary
 <all>
 <detail | extensive | terse>
 <count>
 <physical-interface *physical-interface-name*>
 <logical-system *logical-system* pic | port | routing-instance *routing-instance* | slot>

Release Information Command introduced in Junos OS Release 10.2.

Description Display summary information for subscribers.

Options **none**—Display summary information by state and client type for all subscribers.

all—(Optional) Display summary information by state, client type, and LS:RI.

detail | extensive | terse—(Not supported on MX Series routers) (Optional) Display the specified level of output.

count—(Not supported on MX Series routers) (Optional) Display the count of total subscribers and active subscribers for any specified option.

logical-system *logical-system*—(Optional) Display subscribers whose logical system matches the specified logical system.

physical-interface *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.

pic—(M120, M320, and MX Series routers only) (Optional) Display a count of subscribers by PIC number and the total number of subscribers.

port—(M120, M320, and MX Series routers only) (Optional) Display a count of subscribers by port number and the total number of subscribers.

routing-instance *routing-instance*—(Optional) Display subscribers whose routing instance matches the specified routing instance.

slot—(M120, M320, and MX Series routers only) (Optional) Display a count of subscribers by FPC slot number and the total number of subscribers.



NOTE: Due to display limitations, logical system and routing instance output values are truncated when necessary.

Required Privilege Level view

Related Documentation • [show subscribers on page 606](#)

List of Sample Output [show subscribers summary on page 634](#)
[show subscribers summary all on page 634](#)
[show subscribers summary physical-interface on page 635](#)
[show subscribers summary physical-interface pic on page 635](#)
[show subscribers summary physical-interface port on page 635](#)
[show subscribers summary physical-interface slot on page 636](#)
[show subscribers summary pic on page 636](#)
[show subscribers summary pic \(Aggregated Ethernet Interfaces\) on page 636](#)
[show subscribers summary port on page 636](#)
[show subscribers summary port extensive on page 636](#)
[show subscribers summary slot on page 637](#)
[show subscribers summary terse on page 637](#)

Output Fields [Table 39 on page 633](#) lists the output fields for the **show subscribers summary** command. Output fields are listed in the approximate order in which they appear.

Table 39: show subscribers summary Output Fields

Field Name	Field Description	Level of Output
Subscribers by State	Number of subscribers summarized by state. The summary information includes the following: <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. 	detail none
Subscribers by Client Type	Number of subscribers summarized by client type. Client types can include DHCP, GRE, L2TP, PPP, PPPOE, STATIC-INTERFACE, VLAN, and VLAN-OOB. Also displays the total number of subscribers for all client types (Total).	detail extensive none
Subscribers by LS:RI	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).	detail none
Subscribers by Connection Type	Number of subscribers summarized by connection type, Cross-connected or Terminated .	extensive
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. For aggregated Ethernet interfaces, the output of the summary (pic port slot) options prefixes the interface name with ae0:.	All levels

Table 39: show subscribers summary Output Fields (*continued*)

Field Name	Field Description	Level of Output
Count	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.	detail extensive none
Total Subscribers	Total number of subscribers for all physical interfaces, all PICS, all ports, or all LS:RI slots.	detail extensive none
IP Address/VLAN ID	Subscriber IP address or VLAN ID associated with the subscriber in the form <i>tpid.vlan-id</i>	terse
User Name	Name of subscriber.	terse
LS:RI	Logical system and routing instance associated with the subscriber.	terse

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
VLAN-OOB    2
TOTAL      193
```

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-5/0/1       201
ge-5/0/2       301

Total Subscribers: 502
```

show subscribers summary port extensive

```
user@host> show subscribers summary port extensive
Interface: ge-5/0/1
Count: 201
Detail:
Subscribers by Client Type
  DHCP: 100
  PPPoE: 100
  VLAN-00B: 1
Subscribers by Connection Type
  Terminated: 200
  Cross-connected: 1

Interface: ge-5/0/2
Count: 301
Detail:
```

```
Subscribers by Client Type
  DHCP: 200
  PPPoE: 100
  VLAN-OOB: 1
Subscribers by Connection Type
  Terminated: 300
  Cross-connected: 1

Total Subscribers: 502
```

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                 default:default
demux0.1073741824   203.0.113.10        WHOLESALER-CLIENT default:default
demux0.1073741825   203.0.113.13        RETAILER1-CLIENT  test1:retailer1
demux0.1073741826   203.0.113.213       RETAILER2-CLIENT  test1:retailer2
```

show vpls connections

Syntax	<code>show vpls connections</code> <code><brief extensive></code> <code><down up up-down></code> <code><history></code> <code><instance <i>instance-name</i> local-site <i>local-site-name</i> remote-site <i>remote-site-name</i>></code> <code><instance-history></code> <code><logical-system (all <i>logical-system-name</i>)></code> <code><status></code> <code><summary></code>
Release Information	Command introduced before Junos OS Release 7.4. instance-history option introduced in Junos OS Release 12.3R2.
Description	(T Series and M Series routers, except for the M160 router) Display virtual private LAN service (VPLS) connection information.
Options	none —Display information about all VPLS connections for all routing instances. brief extensive —(Optional) Display the specified level of output. down up up-down —(Optional) Display nonoperational, operational, or both types of connections. history —(Optional) Display information about connection history. instance <i>instance-name</i> —(Optional) Display the VPLS connections for the specified routing instance only. instance-history —(Optional) Display information about connection history for a particular instance. local-site <i>local-site-name</i> —(Optional) Display the VPLS connections for the specified local site name or ID only. remote-site <i>remote-site-name</i> —(Optional) Display the VPLS connections for the specified remote site name or ID only. Label block size information is always shown as 0 when using this option. logical-system (all <i>logical-system-name</i>) —(Optional) Perform this operation on all logical systems or on a particular logical system. status —(Optional) Display information about the connection and interface status. summary —(Optional) Display summary of all VPLS connections information.
Required Privilege Level	view

List of Sample Output [show vpls connections on page 643](#)
[show vpls connections \(with FEC128 and FEC129 in the same routing-instance\) on page 645](#)
[show vpls connections \(with multiple pseudowires\) on page 646](#)
[show vpls connections extensive \(Static VPLS Neighbors\) on page 647](#)

Output Fields Table 40 on page 639 lists the output fields for the **show vpls connections** command. Output fields are listed in the approximate order in which they appear.

Table 40: show vpls connections Output Fields

Field Name	Field Description
Instance	Name of the VPLS instance.
Local site	Name of the local site.
VPLS-id	Identifier for the VPLS site.
Number of local interfaces	Number of interfaces configured for the local site.
Number of local interfaces up	Number of interfaces configured for the local site that are currently up.
IRB interface present	Indicates whether or not an integrated routing and bridging (IRB) interface is present (yes or no).
Intf	<p>List of all of the interfaces configured for the local site. The types of interfaces can include VPLS virtual loopback tunnel interfaces and label-switched interfaces. Any interface that supports VPLS could be listed here.</p> <p>Virtual loopback tunnel interfaces are displayed using the vt-fpc/pic/port.nnnnn format. Label-switched interfaces are displayed using the lsi.nnnnn format. In both cases, nnnnn is a dynamically generated virtual port used to transport and receive packets from other provider edge (PE) routers in the VPLS domain.</p> <p>Each interface might include the following information:</p> <ul style="list-style-type: none"> • Identification as a VPLS interface • Name of the associated VPLS routing instance • Local site number • Remote site number • VPLS neighbor address • VPLS identifier
Interface flags	<p>Flag associated with the interface. Can include the following:</p> <ul style="list-style-type: none"> • VC-Down—The virtual circuit associated with this interface is down.
Label-base	First label in a block of labels. A remote PE router uses this first label when sending traffic toward the advertising PE router.

Table 40: show vpls connections Output Fields (*continued*)

Field Name	Field Description
Offset	Displays the VPLS Edge (VE) block offset in the Layer 2 VPN NLRI. The VE block offset is used to identify a label block from which a particular label value is selected to setup a pseudowire for a remote site. The block offset value itself indicates the starting VE ID that maps to the label base contained in the VPLS NLRI advertisement.
Size	Label block size. A configurable value that represents the number of label blocks required to cover all the pseudowires for the remote peer. Acceptable configuration values are: 2 , 4 , 8 and 16 . The default value is 2 . A value of 0 will be displayed when using the remote-site option.
Range	Label block range. A value that keeps track of the numbers of remote sites discovered within each label block.
Preference	Preference value advertised for a VPLS site. When multiple PE routers are assigned the same VE ID for multihoming, you might need to specify that a particular PE router acts as the designated forwarder by configuring the site preference value. The site preference indicates the degree of preference for a particular customer site. The site preference is one of the tie-breaking criteria used in a designated forwarder election.
status-vector	Bit vector advertising the state of local PE-CE circuits to remote PE routers. A bit value of 0 indicates that the local circuit and LSP tunnel to the remote PE router are up, whereas a value of 1 indicates either one or both are down.
connection-site	Name of the connection site.
Neighbor	IP address and VPLS identifier for the VPLS neighbor. If multiple pseudowires have been configured, the IP address will also show the PW-specific <i>vpls-id-list</i> , for example, 203.0.113.144 (vpls-id 200).
Type	Type of connection: loc (local) or rmt (remote).

Table 40: show vpls connections Output Fields (*continued*)

Field Name	Field Description
St	<p>Status of the VPLS connection (corresponds with Legend for Connection Status):</p> <ul style="list-style-type: none"> • EI—The local VPLS interface is configured with an encapsulation that is not supported. • EM—The encapsulation type received on this VPLS connection from the neighbor does not match the local VPLS connection interface encapsulation type. • VC-Dn—The virtual circuit is currently down. • CM—The two routers do not agree on a control word, which causes a control word mismatch. • CN—The virtual circuit is not provisioned properly. • OR—The label associated with the virtual circuit is out of range. • OL—No advertisement has been received for this virtual circuit from the neighbor. There is no outgoing label available for use by this virtual circuit. • LD—All of the CE-facing interfaces to the local site are down. Therefore, the connection to the local site is signaled as down to the other PE routers. No pseudowires can be established. • RD—All the interfaces to the remote neighbor are down. Therefore, the remote site has been signaled as down to the other PE routers. No pseudowires can be established. • LN—The local site has lost path selection to the remote site and therefore no pseudowires can be established from this local site. • RN—The remote site has lost path selection to a local site or other remote site and therefore no pseudowires are established to this remote site. In a multihoming configuration, one multihomed PE site displays the state LN, and the other multihomed PE site displays the state RN in the following circumstances: <ul style="list-style-type: none"> • The multihomed links are both configured to be the backup site. • The two multihomed PE routers have the same site ID, but have a peering relationship with a route reflector (RR) that has a different site ID. • XX—The VPLS connection is down for an unknown reason. This is a programming error. • MM—The MTU for the local site and the remote site do not match. • BK—The router is using a backup connection. • PF—Profile parse failure. • RS—The remote site is in a standby state. • NC—The interface encapsulation is not configured as an appropriate CCC, TCC, or VPLS encapsulation. • WE—The encapsulation configured for the interface does not match the encapsulation configured for the associated connection within the VPLS routing instance.

Table 40: show vpls connections Output Fields (*continued*)

Field Name	Field Description
	<ul style="list-style-type: none"> • NP—The router detects that interface hardware is not present. The hardware might be offline, a PIC might not be of the desired type, or the interface might be configured in a different routing instance. • -->—Only the outbound connection is up. • <--—Only the inbound connection is up. • Up—The VPLS connection is operational. • Dn—The VPLS connection is down. • CF—The router cannot find enough bandwidth to the remote router to satisfy the VPLS connection bandwidth requirement. • SC—The local site identifier matches the remote site identifier. No pseudowire can be established between these two sites. You should configure different values for the local and remote site identifiers. • LM—The local site identifier is not the minimum designated, meaning it is not the lowest. There is another local site with a lower site identifier. Pseudowires are not being established to this local site, and the associated local site identifier is not being used to distribute VPLS label blocks. However, this is not an error state. Traffic continues to be forwarded to the PE router interfaces connected to the local sites when the local sites are in this state. • RM—The remote site identifier is not the minimum designated, meaning it is not the lowest. There is another remote site connected to the same PE router which has lower site identifier. The PE router cannot establish a pseudowire to this remote site and the associated remote site identifier cannot be used to distribute VPLS label blocks. However, this is not an error state. Traffic can continue to be forwarded to the PE router interface connected to this remote site when the remote site is in this state. • IL—The incoming packets for the VPLS connection have no MPLS label. • MI—The configured mesh group identifier is in use by another system in the network. • ST—The router has switched to a standby connection. • PB—Profile busy. • SN—The VPLS neighbor is static.
Time last up	Time connection was last in the Up condition.
# Up trans	Number of transitions from Down to Up condition.
Status	Status of the (local or remote circuit) local interface: <ul style="list-style-type: none"> • Up—Operational • Dn—Down • NP—Not present • DS—Disabled • WE—Wrong encapsulation • UN—Uninitialized
Encapsulation	Type of encapsulation: VPLS .
Remote PE	Address of the remote provider edge router.

Table 40: show vpls connections Output Fields (*continued*)

Field Name	Field Description
Negotiated control-word	Whether a control word has been negotiated: Yes or No .
Incoming label	Name of the incoming label.
Outgoing label	Name of the outgoing label.
Negotiated PW status TLV	Indicates whether or not the pseudowire status TLV has been negotiated for the VPLS connection.
Local interface	Provides the following information about the local interface configured for the VPLS neighbor: <ul style="list-style-type: none"> • Name of the local interface • Status—Interface status (Up or Down) • Encapsulation—Interface encapsulation (for example, ETHERNET) • Description—Includes the VPLS instance name, the VPLS neighbor address, and the VPLS identifier
Time	Date and time of VPLS connection event.
Event	Type of event.
Interface/Lbl/PE	Interface, label, or PE router.
Connection History	Each entry can include the date, time, year, and the connection event. Connection events include any of a variety of events related to VPLS connections, such as route changes, label updates, and interfaces going down or coming up.

Sample Output

show vpls connections

```
user@host> show vpls connections
```

```
Layer-2 VPN connections:
```

```
Legend for connection status (St)
```

```

EI -- encapsulation invalid      NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch    WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down  NP -- interface hardware not present
CM -- control-word mismatch    -< -- only outbound connection is up
CN -- circuit not provisioned  >- -- only inbound connection is up
OR -- out of range            Up -- operational
OL -- no outgoing label       Dn -- down
LD -- local site signaled down CF -- call admission control failure
RD -- remote site signaled down SC -- local and remote site ID collision
LN -- local site not designated LM -- local site ID not minimum designated
RN -- remote site not designated RM -- remote site ID not minimum designated
XX -- unn connection status  IL -- no incoming label
MM -- MTU mismatch           MI -- Mesh-Group ID not available
BK -- Backup connection      ST -- Standby connection

```

PF -- Profile parse failure PB -- Profile busy

Legend for interface status

Up -- operational

Dn -- down

Instance: vpls-1

Local site: 1 (11)

Number of local interfaces: 1

Number of local interfaces up: 1

IRB interface present: no

lt-1/3/0.10496

vt-1/3/0.1048588 1 Intf - vpls vpls-1 local site 11 remote site 1

vt-1/2/0.1048591 2 Intf - vpls vpls-1 local site 11 remote site 2

vt-1/2/0.1048585 3 Intf - vpls vpls-1 local site 11 remote site 3

vt-1/2/0.1048587 4 Intf - vpls vpls-1 local site 11 remote site 4

vt-1/2/0.1048589 5 Intf - vpls vpls-1 local site 11 remote site 5

vt-1/3/0.1048586 6 Intf - vpls vpls-1 local site 11 remote site 6

vt-1/3/0.1048590 7 Intf - vpls vpls-1 local site 11 remote site 7

vt-1/3/0.1048584 8 Intf - vpls vpls-1 local site 11 remote site 8

Label-base	Offset	Size	Range	Preference
800256	1	16	16	100

Timer Values:

Startup wait time: 120 seconds

New site wait-time: 20 seconds

Collision detect time: 30 seconds

Reclaim wait time: 748 milliseconds

connection-site	Type	St	Time last up	# Up trans
1	rmt	Up	Apr 28 13:28:24 2009	2

Remote PE: 192.0.2.1, Negotiated control-word: No

Incoming label: 800256, Outgoing label: 800026

Local interface: vt-1/3/0.1048588, Status: Up, Encapsulation: VPLS

Description: Intf - vpls vpls-1 local site 11 remote site 1

Connection History:

Apr 28 13:28:24 2009 status update timer

Apr 28 13:28:24 2009 PE route down

Apr 28 13:24:27 2009 status update timer

Apr 28 13:24:27 2009 loc intf up vt-1/3/0.1048588

Apr 28 13:24:27 2009 PE route changed

Apr 28 13:24:27 2009 Out lbl Update 800026

Apr 28 13:24:27 2009 In lbl Update 800256

Apr 28 13:24:27 2009 loc intf down

2	rmt	Up	Apr 28 13:28:24 2009	2
---	-----	----	----------------------	---

Remote PE: 192.0.2.71, Negotiated control-word: No

Incoming label: 800257, Outgoing label: 800034

Local interface: vt-1/2/0.1048591, Status: Up, Encapsulation: VPLS

Description: Intf - vpls vpls-1 local site 11 remote site 2

Connection History:

Apr 28 13:28:24 2009 status update timer

Apr 28 13:28:24 2009 PE route down

Apr 28 13:24:28 2009 status update timer

Apr 28 13:24:28 2009 loc intf up vt-1/2/0.1048591

Apr 28 13:24:28 2009 PE route changed

```

Apr 28 13:24:28 2009 Out lbl Update      800034
Apr 28 13:24:28 2009 In lbl Update       800257
Apr 28 13:24:28 2009 loc intf down

```

show vpls connections (with FEC128 and FEC129 in the same routing-instance)

```

user@host> show vpls connections
Instance: fec129
  L2vpn-id: 1:1
  Local-id: 203.0.113.0
FEC129-VPLS State:
  Mesh-group connections: __ves__
    Remote-id      Type  St   Time last up      # Up trans
    203.0.3.3      rmt  Up   Sep 19 09:59:56 2017      1
      Remote PE: 203.0.3.3, Negotiated control-word: No
      Incoming label: 262155, Outgoing label: 262164
      Negotiated PW status TLV: No
      Local interface: lsi.1048844, Status: Up, Encapsulation: ETHERNET
      Description: Intf - vpls fec129 local-id 81.4.4.4 remote-id 203.0.3.3
  neighbor 203.0.3.3
    Flow Label Transmit: No, Flow Label Receive: No
    203.0.2.2      rmt  Up   Sep 19 09:59:52 2017      1
      Remote PE: 203.0.2.2, Negotiated control-word: No
      Incoming label: 262154, Outgoing label: 262157
      Negotiated PW status TLV: No
      Local interface: lsi.1048846, Status: Up, Encapsulation: ETHERNET
      Description: Intf - vpls fec129 local-id 81.4.4.4 remote-id 203.0.2.2
  neighbor 203.0.2.2
    Flow Label Transmit: No, Flow Label Receive: No
    203.0.1.1      rmt  Up   Sep 19 09:59:48 2017      1
      Remote PE: 203.0.1.1, Negotiated control-word: No
      Incoming label: 262156, Outgoing label: 262157
      Negotiated PW status TLV: No
      Local interface: lsi.1048845, Status: Up, Encapsulation: ETHERNET
      Description: Intf - vpls fec129 local-id 81.4.4.4 remote-id 203.0.1.1
  neighbor 203.0.1.1
    Flow Label Transmit: No, Flow Label Receive: No

LDP-VPLS State
  Mesh-group connections: MG1
    Neighbor      Type  St   Time last up      # Up trans
    203.0.6.6(vpls-id 1)  rmt  Up   Sep 17 19:17:11 2017      1
      Remote PE: 203.0.6.6, Negotiated control-word: No
      Incoming label: 262423, Outgoing label: 262145
      Negotiated PW status TLV: No
      Local interface: lsi.1049859, Status: Up, Encapsulation: ETHERNET
      Description: Intf - vpls bgp-vpls neighbor 203.0.6.6 vpls-id 1
    Flow Label Transmit: No, Flow Label Receive: No
    203.0.7.7(vpls-id 1)  rmt  Up   Sep 17 19:17:04 2017      1
      Remote PE: 203.0.7.7, Negotiated control-word: No
      Incoming label: 262424, Outgoing label: 262145
      Negotiated PW status TLV: No
      Local interface: lsi.1049857, Status: Up, Encapsulation: ETHERNET
      Description: Intf - vpls bgp-vpls neighbor 203.0.7.7 vpls-id 1
    Flow Label Transmit: No, Flow Label Receive: No
  Mesh-group connections: MG2
    Neighbor      Type  St   Time last up      # Up trans
    203.0.5.5(vpls-id 1)  rmt  Up   Sep 17 19:17:00 2017      1
      Remote PE: 203.0.5.5, Negotiated control-word: No
      Incoming label: 262425, Outgoing label: 299872
      Negotiated PW status TLV: No

```

Local interface: lsi.1049856, Status: Up, Encapsulation: ETHERNET
 Description: Intf - vpls bgp-vpls neighbor 203.0.5.5 vpls-id 1
 Flow Label Transmit: No, Flow Label Receive: No

show vpls connections (with multiple pseudowires)

```
user@host> show vpls connections
Layer-2 VPN connections:
```

Legend for connection status (St)

EI -- encapsulation invalid	NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch	WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down	NP -- interface hardware not present
CM -- control-word mismatch	-> -- only outbound connection is up
CN -- circuit not provisioned	<- -- only inbound connection is up
OR -- out of range	Up -- operational
OL -- no outgoing label	Dn -- down
LD -- local site signaled down	CF -- call admission control failure
RD -- remote site signaled down	SC -- local and remote site ID collision
LN -- local site not designated	LM -- local site ID not minimum designated
RN -- remote site not designated	RM -- remote site ID not minimum designated
XX -- unknown connection status	IL -- no incoming label
MM -- MTU mismatch	MI -- Mesh-Group ID not available
BK -- Backup connection	ST -- Standby connection
PF -- Profile parse failure	PB -- Profile busy
RS -- remote site standby	SN -- Static Neighbor
LB -- Local site not best-site	RB -- Remote site not best-site
VM -- VLAN ID mismatch	

Legend for interface status

Up -- operational
 Dn -- down

Instance: vpls

VPLS-id: 100

Mesh-group connections: __ves__

Neighbor	Type	St	Time last up	# Up trans
10.255.114.3 (vpls-id 100)	rmt	Up	Apr 11 23:38:38 2013	1
Remote PE: 10.255.114.3, Negotiated control-word: No				
Incoming label: 262145, Outgoing label: 262145				
Negotiated PW status TLV: No				
Local interface: lsi.1049090, Status: Up, Encapsulation: ETHERNET				
Description: Intf - vpls h-vpls neighbor 10.255.114.3 vpls-id 100				

Mesh-group connections: spokes

Neighbor	Type	St	Time last up	# Up trans
10.255.114.4 (vpls-id 200)	rmt	Up	Apr 11 23:39:25 2013	1
Remote PE: 10.255.114.4, Negotiated control-word: No				
Incoming label: 262148, Outgoing label: 304224				
Negotiated PW status TLV: Yes				
local PW status code: 0x00000000, Neighbor PW status code: 0x00000000				
Local interface: lsi.1049091, Status: Up, Encapsulation: ETHERNET				
Description: Intf - vpls h-vpls neighbor 10.255.114.4 vpls-id 200				
10.255.114.4 (vpls-id 201)	rmt	Up	Apr 11 23:39:25 2013	1
Remote PE: 10.255.114.4, Negotiated control-word: No				
Incoming label: 262149, Outgoing label: 304225				
Negotiated PW status TLV: Yes				
local PW status code: 0x00000000, Neighbor PW status code: 0x00000000				
Local interface: lsi.1049096, Status: Up, Encapsulation: ETHERNET				
Description: Intf - vpls h-vpls neighbor 10.255.114.4 vpls-id 201				

show vpls connections extensive (Static VPLS Neighbors)

```
user@host> show vpls connections extensive instance red
```

```
Layer-2 VPN connections:
```

```
Legend for connection status (St)
```

```
EI -- encapsulation invalid      NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch     WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down   NP -- interface hardware not present
CM -- control-word mismatch     -> -- only outbound connection is up
CN -- circuit not provisioned   <- -- only inbound connection is up
OR -- out of range             Up -- operational
OL -- no outgoing label        Dn -- down
LD -- local site signaled down  CF -- call admission control failure
RD -- remote site signaled down SC -- local and remote site ID collision
LN -- local site not designated LM -- local site ID not minimum designated
RN -- remote site not designated RM -- remote site ID not minimum designated
XX -- unnn connection status   IL -- no incoming label
MM -- MTU mismatch            MI -- Mesh-Group ID not available
BK -- Backup connection        ST -- Standby connection
PF -- Profile parse failure    PB -- Profile busy
RS -- remote site standby     SN -- Static Neighbor
```

```
Legend for interface status
```

```
Up -- operational
Dn -- down
```

```
Instance: static
```

```
VPLS-id: 1
```

```
Number of local interfaces: 1
```

```
Number of local interfaces up: 1
```

```
ge-0/0/5.0
```

```
lsi.1049344 Intf - vpls static neighbor 10.255.114.3 vpls-id
```

```
1
```

```
Neighbor          Type St    Time last up      # Up trans
10.255.114.3(vpls-id 1)(SN) rmt Up    Mar  4 08:48:41 2010      1
```

```
Remote PE: 10.255.114.3, Negotiated control-word: No
```

```
Incoming label: 29696, Outgoing label: 29697
```

```
Negotiated PW status TLV: No
```

```
Local interface: lsi.1049344, Status: Up, Encapsulation: ETHERNET
```

```
Description: Intf - vpls static neighbor 10.255.114.3 vpls-id 1
```

```
Connection History:
```

```
Mar  4 08:48:41 2010 status update timer
```

```
Mar  4 08:48:41 2010 PE route changed
```

```
Mar  4 08:48:41 2010 Out lbl Update 29697
```

```
Mar  4 08:48:41 2010 In lbl Update 29696
```

```
Mar  4 08:48:41 2010 loc intf up lsi.1049344
```

```
user@PE1> show vpls connections extensive (Multihoming with FEC 129)
```

```
Layer-2 VPN connections:
```

```
Legend for connection status (St)
```

```
EI -- encapsulation invalid      NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch     WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down   NP -- interface hardware not present
CM -- control-word mismatch     -> -- only outbound connection is up
CN -- circuit not provisioned   <- -- only inbound connection is up
OR -- out of range             Up -- operational
OL -- no outgoing label        Dn -- down
LD -- local site signaled down  CF -- call admission control failure
```

```

RD -- remote site signaled down  SC -- local and remote site ID collision
LN -- local site not designated  LM -- local site ID not minimum designated
RN -- remote site not designated  RM -- remote site ID not minimum designated
XX -- unknown connection status  IL -- no incoming label
MM -- MTU mismatch               MI -- Mesh-Group ID not available
BK -- Backup connection          ST -- Standby connection
PF -- Profile parse failure       PB -- Profile busy
RS -- remote site standby         SN -- Static Neighbor
LB -- Local site not best-site    RB -- Remote site not best-site
VM -- VLAN ID mismatch

```

Legend for interface status

Up -- operational

Dn -- down

Instance: green

L2vpn-id: 100:100

Local-id: 192.0.2.2

Number of local interfaces: 2

Number of local interfaces up: 2

ge-0/3/1.0

ge-0/3/3.0

lsi.101711873

Intf - vpls green local-id 192.0.2.2 remote-id

192.0.2.4 neighbor 192.0.2.4

Remote-id	Type	St	Time last up	# Up trans
192.0.2.4	rmt	Up	Jan 31 13:49:52 2012	1

Remote PE: 192.0.2.4, Negotiated control-word: No

Incoming label: 262146, Outgoing label: 262146

Local interface: lsi.101711873, Status: Up, Encapsulation: ETHERNET

Description: Intf - vpls green local-id 192.0.2.2 remote-id 192.0.2.4

neighbor 192.0.2.4

Connection History:

Jan 31 13:49:52 2012	status update timer	
Jan 31 13:49:52 2012	PE route changed	
Jan 31 13:49:52 2012	Out lbl Update	262146
Jan 31 13:49:52 2012	In lbl Update	262146
Jan 31 13:49:52 2012	loc intf up	lsi.101711873

Multi-home:

Local-site	Id	Pref	State
test	1	100	Up

Number of interfaces: 1

Number of interfaces up: 1

ge-0/3/1.0

Received multi-homing advertisements:

Remote-PE	Pref	flag	Description
192.0.2.4	100	0x0	

show vpls flood event-queue

Syntax show vpls flood event-queue

Release Information Command introduced in Junos OS Release 8.0.

Description Display the pending events in the VPLS flood queue.

Options This command has no options.

Required Privilege Level view

List of Sample Output [show vpls flood event-queue on page 649](#)

Output Fields [Table 41 on page 649](#) lists the output fields for the **show vpls flood event-queue** command. Output fields are listed in the approximate order in which they appear.

Table 41: show vpls flood event-queue Output Fields

Field Name	Field Description
Current Pending Event	Provides information on the current event in the VPLS flood event queue.
Name	Name of the event.
Owner Name	Name of the interface associated with the flood event.
Pending Op	Pending operation for the event.
Last Error	Name of the last error encountered.
Number of Retries	Number of attempts made to update the event queue.
Pending Event List	List of the events awaiting processing.
Event Name	Name of the event.
Pending Op	Pending operation for the event.
Event Identifier	Name of the interface associated with the flood event.

Sample Output

show vpls flood event-queue

```
user@host> show vpls flood event-queue
```

Current Pending Event

Name: Flood Nexthop

Owner Name:ge-4/3/0.0

Pending Op: ADD

Last Error:ENOMEM

Number of Retries:3

Pending Event List:

Event Name	Pending Op	Event Identifier
Flood Nexthop	ADD	ge-4/3/0.0
Flood Route	ADD	ge-4/3/0.0

show vpls flood instance

Syntax	show vpls flood instance <brief detail extensive> <instance-name> <logical-system <i>logical-system-name</i> >
Release Information	Command introduced in Junos OS Release 8.0.
Description	Display VPLS information related to the flood process.
Options	<p>none—Display VPLS information related to the flood process for all routing instances.</p> <p>brief detail extensive—(Optional) Display the specified level of output.</p> <p>instance-name—(Optional) Display VPLS information related to the flood process for the specified routing instance.</p> <p>logical-system <i>logical-system-name</i>—(Optional) Display VPLS information related to the flood process for the specified logical system.</p>
Required Privilege Level	view
List of Sample Output	show vpls flood instance on page 652 show vpls flood instance logical-system-name on page 652 show vpls flood instance detail on page 652
Output Fields	<p>Table 42 on page 651 lists the output fields for the show vpls flood instance command. Output fields are listed in the approximate order in which they appear.</p>

Table 42: show vpls flood instance Output Fields

Field Name	Field Description
Logical system	Name of the logical system.
Name	Name of the VPLS routing instance.
CEs	Number of CE routers connected to the VPLS instance.
VEs	Number of VE routers connected to the VPLS instance.
Flood routes	List of all flood routes associated with the VPLS instance.
Prefix	Prefix for the route.
Type	Type of route.

Table 42: show vpls flood instance Output Fields (*continued*)

Field Name	Field Description
Owner	VPLS routing instance or interface associated with the route.
NhType	Next-hop type. For example, flood for a flood route.
Nhindex	Next-hop index number for the route.

Sample Output

show vpls flood instance

```

user@host> show vpls flood instance

Logical system: __example_ls1__
Name: green
CEs: 1
VEs: 1
Flood Routes:
  Prefix  Type      Owner      NhType      NhIndex
  default ALL_CE_FLOOD green       flood       383
  0x47/16 CE_FLOOD  fe-1/2/1.0 flood       388

```

show vpls flood instance logical-system-name

```

user@host:__example_ls1__> show vpls flood instance example_ls1

Logical system: __example_ls1__
Name: green
CEs: 1
VEs: 1
Flood Routes:
  Prefix  Type      Owner      NhType      NhIndex
  default ALL_CE_FLOOD green       flood       383
  0x47/16 CE_FLOOD  fe-1/2/1.0 flood       388

```

show vpls flood instance detail

```

user@host:__example_ls1__> show vpls flood instance detail

Logical system: __example_ls1__
Name: green
CEs: 1
VEs: 1
Flood Routes:
  Prefix  Type      Owner      NhType      NhIndex
  default ALL_CE_FLOOD green       flood       383
  0x47/16 CE_FLOOD  fe-1/2/1.0 flood       388

```

show vpls flood route

Syntax show vpls flood route
 (all-ce-flood instance-name *instance-name* <logical-system-name *logical-system-name*>
 |
 ce-flood interface *interface-name*)

Release Information Command introduced in Junos OS Release 8.0.

Description Display VPLS route information related to the flood process for either the specified routing instance or the specified interface.

Options **all-ce-flood**—Display the flood next-hop route for all customer edge routers for traffic coming from the core of the network.

ce-flood interface *interface-name*—Display the flood next-hop route for traffic coming from the specified customer edge interface.

instance-name *instance-name*—Display the flood routes for the specified instance.

logical-system-name *logical-system-name*—(Optional) Specify the logical system whose flood routes you want to display. You can only specify the default logical system name for VPLS. The default logical system name is **__example_ls1__** (the name must be entered in the command with the underscore characters).

Required Privilege Level view

List of Sample Output [show vpls flood route all-ce-flood on page 654](#)
[show vpls flood route ce-flood on page 654](#)

Output Fields [Table 43 on page 653](#) lists the output for the **show vpls flood route** command. Output fields are listed in the approximate order in which they appear.

Table 43: show vpls flood route Output Fields

Field Name	Field Description
Flood route prefix	Prefix for the flood route.
Flood route type	Type of flood route (either CE_FLOOD or ALL_CE_FLOOD).
Flood route owner	VPLS routing instance or interface associated with the flood route.
Nexthop type	Next-hop type. For example, flood for a flood route.
Nexthop index	Next-hop index number for the route.
Interfaces flooding to	Interfaces to which VPLS routes are being flooded.

Table 43: show vpls flood route Output Fields (*continued*)

Field Name	Field Description
Name	Name of the interface.
Type	Type of VPLS router (CE or VE).
Nh type	Next-hop type.
Index	Index number for the flood route.

Sample Output

show vpls flood route all-ce-flood

```
user@host: __example_lsi__> show vpls flood route all-ce-flood logical-system-name
__example_lsi__instance-name green
```

```
Flood route prefix: default
Flood route type: ALL_CE_FLOOD
Flood route owner: green
Nexthop type: flood
Nexthop index: 383
  Interfaces Flooding to:
    Name      Type      NhType      Index
    fe-1/2/1.0  CE
```

show vpls flood route ce-flood

```
user@host: __example_lsi__> show vpls flood route ce-flood interface fe-1/2/1.0
```

```
Flood route prefix: 0x47/16
Flood route type: CE_FLOOD
Flood route owner: fe-1/2/1.0
Nexthop type: flood
Nexthop index: 388
  Interfaces Flooding to:
    Name      Type      NhType      Index
    lsi.49152  VE      indr      262142
```

show vpls mac-table

Syntax	<pre>show vpls mac-table <age> <brief detail extensive summary> <bridge-domain <i>bridge-domain-name</i>> <instance <i>instance-name</i>> <interface <i>interface-name</i>> <logical-system (all <i>logical-system-name</i>)> <mac-address> <vlan-id <i>vlan-id-number</i>></pre>
Release Information	<p>Command introduced in Junos OS Release 8.5.</p> <p>Command introduced in Junos OS Release 15.1.</p>
Description	Display learned virtual private LAN service (VPLS) media access control (MAC) address information.
Options	<p>none—Display all learned VPLS MAC address information.</p> <p>age— (Optional) Display age of a single mac-address.</p> <p>brief detail extensive summary—(Optional) Display the specified level of output.</p> <p>bridge-domain <i>bridge-domain-name</i>—(Optional) Display learned VPLS MAC addresses for the specified bridge domain.</p> <p>instance <i>instance-name</i>—(Optional) Display learned VPLS MAC addresses for the specified instance.</p> <p>interface <i>interface-name</i>—(Optional) Display learned VPLS MAC addresses for the specified instance.</p> <p>logical-system (all <i>logical-system-name</i>)—(Optional) Display learned VPLS MAC addresses for all logical systems or for the specified logical system.</p> <p>mac-address—(Optional) Display the specified learned VPLS MAC address information..</p> <p>vlan-id <i>vlan-id-number</i>—(Optional) Display learned VPLS MAC addresses for the specified VLAN.</p>
Required Privilege Level	view
List of Sample Output	<p>show vpls mac-table on page 657</p> <p>show vpls mac-table (with Layer 2 Services over GRE Interfaces) on page 657</p> <p>show vpls mac-table (with VXLAN enabled) on page 657</p> <p>show vpls mac-table age (for GE interface) on page 658</p> <p>show vpls mac-table age (for AE interface) on page 658</p> <p>show vpls mac-table count on page 658</p>

[show vpls mac-table detail on page 659](#)

[show vpls mac-table extensive on page 659](#)

Output Fields [Table 44 on page 656](#) describes the output fields for the **show vpls mac-table** command. Output fields are listed in the approximate order in which they appear.

Table 44: show vpls mac-table Output fields

Field Name	Field Description
Age	Age of a single mac-address.
Routing instance	Name of the routing instance.
Bridging domain	Name of the bridging domain.
MAC address	MAC address or addresses learned on a logical interface.
MAC flags	Status of MAC address learning properties for each interface: <ul style="list-style-type: none"> • S—Static MAC address configured. • D—Dynamic MAC address learned. • SE—MAC accounting is enabled. • NM—Nonconfigured MAC.
Logical interface	Name of the logical interface.
MAC count	Number of MAC addresses learned on a specific routing instance or interface.
Learning interface	Logical interface or logical Label Switched Interface (LSI) the address is learned on.
Base learning interface	Base learning interface of the MAC address. This field is introduced in Junos OS Release 14.2.
Learn VLAN ID/VLAN	VLAN ID of the routing instance or bridge domain in which the MAC address was learned.
VXLAN ID/VXLAN	VXLAN Network Identifier (VNI)
Layer 2 flags	Debugging flags signifying that the MAC address is present in various lists.
Epoch	Spanning Tree Protocol epoch number identifying when the MAC address was learned. Used for debugging.
Sequence number	Sequence number assigned to this MAC address. Used for debugging.
Learning mask	Mask of Packet Forwarding Engines where this MAC address was learned. Used for debugging.
IPC generation	Creation time of the logical interface when this MAC address was learned. Used for debugging.

Sample Output

show vpls mac-table

```
user@host> show vpls mac-table
MAC flags (S -static MAC, D -dynamic MAC,
           SE -Statistics enabled, NM -Non configured MAC)

Routing instance : vpls_ldp1
VLAN : 223
  MAC          MAC      Logical
  address      flags    interface
  00:00:5e:00:53:5d  D      ge-0/2/5.400

MAC flags (S -static MAC, D -dynamic MAC,
           SE -Statistics enabled, NM -Non configured MAC)

Routing instance : vpls_red
VLAN : 401
  MAC          MAC      Logical
  address      flags    interface
  00:00:5e:00:53:12  D      lsi.1051138
  00:00:5e:00:53:f0  D      lsi.1051138
```

show vpls mac-table (with Layer 2 Services over GRE Interfaces)

```
user@host> show vpls mac-table
MAC flags (S -static MAC, D -dynamic MAC, L -locally learned
           SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance : vpls_4site:1000
Bridging domain : __vpls_4site:1000__, MAC          MAC      Logical
  address      flags    interface
  00:00:5e:00:53:f4  D,SE    ge-4/2/0.1000
  00:00:5e:00:53:33  D,SE    lsi.1052004
  00:00:5e:00:53:32  D,SE    lsi.1048840
  00:00:5e:00:53:14  D,SE    lsi.1052005
  00:00:5e:00:53:f7  D,SE    gr-1/2/10.10
```

show vpls mac-table (with VXLAN enabled)

```
user@host> show vpls mac-table
MAC flags (S -static MAC, D -dynamic MAC, L -locally learned
           SE -Statistics enabled, NM -Non configured MAC, R -Remote PE MAC)

Routing instance : vpls_4site:1000
Bridging domain : __vpls_4site:1000__, VLAN : 4094,4093
VXLAN: Id : 300, Multicast group: 233.252.0.1
  MAC          MAC      Logical
  address      flags    interface
  00:00:5e:00:53:f4  D,SE    ge-4/2/0.1000
  00:00:5e:00:53:33  D,SE    lsi.1052004
  00:00:5e:00:53:32  D,SE    lsi.1048840
  00:00:5e:00:53:14  D,SE    lsi.1052005
  00:00:5e:00:53:f7  D,SE    vtep.1052010
  00:00:5e:00:53:3f  D,SE    vtep.1052011
```

show vpls mac-table age (for GE interface)

```
user@host> show vpls mac-table age 00:00:5e:00:53:1a instance vpls_instance_1
MAC Entry Age information
Current Age: 4 seconds
```

show vpls mac-table age (for AE interface)

```
user@host> show vpls mac-table age 000:00:5e:00:53:1a instance vpls_instance_1
MAC Entry Age information
Current Age on FPC1: 102 seconds
Current Age on FPC2: 94 seconds
```

show vpls mac-table count

```
user@host> show vpls mac-table count
0 MAC address learned in routing instance __example_private1__
```

MAC address count per interface within routing instance:

Logical interface	MAC count
lc-0/0/0.32769	0
lc-0/1/0.32769	0
lc-0/2/0.32769	0
lc-2/0/0.32769	0
lc-0/3/0.32769	0
lc-2/1/0.32769	0
lc-9/0/0.32769	0
lc-11/0/0.32769	0
lc-2/2/0.32769	0
lc-9/1/0.32769	0
lc-11/1/0.32769	0
lc-2/3/0.32769	0
lc-9/2/0.32769	0
lc-11/2/0.32769	0
lc-11/3/0.32769	0
lc-9/3/0.32769	0

MAC address count per learn VLAN within routing instance:

Learn VLAN ID	MAC count
0	0

1 MAC address learned in routing instance vpls_ldp1

MAC address count per interface within routing instance:

Logical interface	MAC count
lsi.1051137	0
ge-0/2/5.400	1

MAC address count per learn VLAN within routing instance:

Learn VLAN ID	MAC count
0	1

1 MAC address learned in routing instance vpls_red

MAC address count per interface within routing instance:

Logical interface	MAC count
ge-0/2/5.300	1

MAC address count per learn VLAN within routing instance:

Learn VLAN ID	MAC count
0	1

show vpls mac-table detail

```

user@host> show vpls mac-table detail
MAC address: 00:00:5e:00:53:5d
  Routing instance: vpls_ldp1
  Learning interface: ge-0/2/5.400
  Layer 2 flags: in_ifd, in_ifl, in_vlan, kernel
  Epoch: 0                               Sequence number: 1
  Learning mask: 0x1                      IPC generation: 0

MAC address: 00:00:5e:00:53:5d
  Routing instance: vpls_red
  Learning interface: ge-0/2/5.300
  Layer 2 flags: in_ifd, in_ifl, in_vlan, kernel
  Epoch: 0                               Sequence number: 1
  Learning mask: 0x1                      IPC generation: 0

```

show vpls mac-table extensive

```

user@host> show vpls mac-table extensive

MAC address: 00:00:5e:00:53::00
  Routing instance: vpls_1
  Bridging domain: __vpls_1__, VLAN : NA
  Learning interface: lsi.1049165
  Base learning interface: lsi.1049165
  Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
  Epoch: 0                               Sequence number: 1
  Learning mask: 0x00000001

MAC address: 00:00:5e:00:53:01
  Routing instance: vpls_1
  Bridging domain: __vpls_1__, VLAN : NA
  Learning interface: lsi.1049165
  Base learning interface: lsi.1049165
  Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
  Epoch: 0                               Sequence number: 1
  Learning mask: 0x00000001

MAC address: 00:00:5e:00:53:02
  Routing instance: vpls_1
  Bridging domain: __vpls_1__, VLAN : NA
  Learning interface: lsi.1049165
  Base learning interface: lsi.1049165
  Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
  Epoch: 0                               Sequence number: 1
  Learning mask: 0x00000001

MAC address: 00:00:5e:00:53:03
  Routing instance: vpls_1
  Bridging domain: __vpls_1__, VLAN : NA
  Learning interface: lsi.1049165
  Base learning interface: lsi.1049165
  Layer 2 flags: in_hash,in_ifd,in_ifl,in_vlan,in_rtt,kernel,in_ifbd
  Epoch: 0                               Sequence number: 1
  Learning mask: 0x00000001

```

show vpls statistics

Syntax	show vpls statistics <instance <i>instance-name</i> > <logical-system (all <i>logical-system-name</i>)>
Release Information	Command introduced before Junos OS Release 7.4.
Description	(T Series and M Series routers, except for the M160 router) Display virtual private LAN service (VPLS) statistics.
Options	<p>none—Display VPLS statistics for all routing instances.</p> <p>instance <i>instance-name</i>—(Optional) Display VPLS statistics for a specific VPLS routing instance only.</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>
Required Privilege Level	view
List of Sample Output	show vpls statistics on page 661 show vpls statistics instance on page 662
Output Fields	Table 45 on page 660 lists the output fields for the show vpls statistics command. Output fields are listed in the approximate order in which they appear.

Table 45: show vpls statistics Output Fields

Field Name	Field Description
Instance	Name of the VPLS instance.
Local interface	Name of the local VPLS virtual loopback tunnel interface, vt-fpc/pic/port.nnnnn , where nnnnn is a dynamically generated virtual port used to transport and receive packets from other provider edge (PE) routers in the VPLS domain.
Index	Number associated with the next hop.
Remote provider edge router	Address of the remote provider edge router.
Multicast packets	Number of multicast packets received.
Multicast bytes	Number of multicast bytes received.
Flood packets	Number of VPLS flood packets received.

Table 45: show vpls statistics Output Fields (*continued*)

Field Name	Field Description
Flood bytes	Number of VPLS flood bytes received.
Current MAC count	Number of MAC addresses learned by the interface and the configured maximum limit on the number of MAC addresses that can be learned.

Sample Output

show vpls statistics

```
user@host> show vpls statistics
```

```
VPLS statistics:
```

```
Instance: green
```

```
Local interface: fe-2/2/1.0, Index: 69
Multicast packets:      1
Multicast bytes   :      60
Flooded packets   :      18
Flooded bytes    :    2556
Current MAC count:      1
```

```
Local interface: lt-0/3/0.2, Index: 72
Multicast packets:      3
Multicast bytes   :    153
Flooded packets   :      1
Flooded bytes    :      51
Current MAC count:      1
```

```
Local interface: lsi.32769, Index: 75
Current MAC count:      0
```

```
Local interface: lsi.32771, Index: 77
Remote PE: 10.255.14.222
Current MAC count:      2
```

```
Instance: red
```

```
Local interface: vt-0/3/0.32768, Index: 74
Multicast packets:      0
Multicast bytes   :      0
Flooded packets   :      0
Flooded bytes    :      0
Current MAC count:      0
```

```
Local interface: vt-0/3/0.32770, Index: 76
Multicast packets:      0
Multicast bytes   :      0
Flooded packets   :      0
Flooded bytes    :      0
Current MAC count:      0
```

show vpls statistics instance

```
user@host> show vpls statistics instance red
```

Layer-2 VPN Statistics:

Instance: red

Local interface: vt-3/2/0.32768, Index: 73

Remote provider edge router: 10.255.17.35

Multicast packets: 0

Multicast bytes : 0

Flood packets : 0

Flood bytes : 0

Current MAC count: 1 (Limit 20)