JUNIPER NETWORKS | Engineering Simplicity

Junos® OS

Broadband Subscriber Management Wholesale User Guide

Published
2026-01-13

JUNOS

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. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

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

Junos® OS Broadband Subscriber Management Wholesale User Guide
Copyright © 2026 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 https://support.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 This Guide | viii

1 **Configuring DHCP Layer 3 Wholesale Networks**

Subscriber Management DHCP Layer 3 Wholesale Overview | 2

Layer 2 and Layer 3 Wholesale Overview | **2**

Wholesale Network Configuration Options and Considerations | **3**

DHCP Layer 3 Wholesale Configuration Interface Support | **4**

Layer 3 Wholesale Configuration DHCP Support | **5**

Subscriber to Logical System and Routing Instance Relationship | **5**

RADIUS VSAs and Broadband Subscriber Management Wholesale Configuration Overview | **6**

Configuring DHCPv4 Layer 3 Wholesale Networks | 8

Broadband Subscriber Management DHCPv4 Layer 3 Wholesale Topology and Configuration Elements | **8**

DHCPv4 Layer 3 Wholesale Network Topology Overview | **10**

Configuring Loopback Interfaces for the DHCPv4 Layer 3 Wholesale Solution | **12**

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 | **15**

Configuring Access Components for the DHCP Layer 3 Wholesale Network Solution | **18**

- Configuring RADIUS Server Access | **18**
- Configuring a DHCP Wholesaler Access Profile | **19**
- Configuring DHCP Retailer Access Profiles | **20**

Configuring Dynamic Profiles for the DHCPv4 Layer 3 Wholesale Network Solution | **21**

- Configuring a Wholesale Dynamic Profile for use in the DHCPv4 Solution | **22**
- Configuring a Dynamic Profile for use by a Retailer in the DHCPv4 Solution | **23**

Configuring Separate Routing Instances for DHCPv4 Service Retailers | **25**

Configure Default Forwarding Options for the DHCPv4 Wholesale Network Solution | **28**

Example: Wholesaler Dynamic Profile for a DHCPv4 Wholesale Network | 31

Example: Retailer Dynamic Profile for a DHCPv4 Wholesale Network | 31

Example: Default Forwarding Options Configuration for the DHCPv4 Wholesale Network | 32

Example: Retailer Routing Instances for a DHCPv4 Wholesale Network | 34

Configuring DHCPv6 Layer 3 Wholesale Networks | 37

Broadband Subscriber Management DHCPv6 Layer 3 Wholesale Topology and Configuration Elements | 37

DHCPv6 Layer 3 Wholesale Network Topology Overview | 39

Configuring Loopback Interfaces for the DHCPv6 Layer 3 Wholesale Solution | 41

Configuring VLANs for the DHCPv6 Layer 3 Wholesale Network Solution | 42

- Configuring Static Customer VLANs for the DHCPv6 Layer 3 Wholesale Network Solution | 42
- Configuring Dynamic Customer VLANs for the DHCPv6 Layer 3 Wholesale Network Solution | 44

Configuring Access Components for the DHCP Layer 3 Wholesale Network Solution | 46

- Configuring RADIUS Server Access | 47
- Configuring a DHCP Wholesaler Access Profile | 47
- Configuring DHCP Retailer Access Profiles | 48

Configuring Dynamic Profiles for the DHCPv6 Layer 3 Wholesale Network Solution | 50

- Configuring a Wholesale Dynamic Profile for use in the DHCPv6 Solution | 50
- Configuring a Dynamic Profile for use by Each Retailer in the DHCPv6 Solution | 51

Configuring Separate Routing Instances for DHCPv6 Service Retailers | 53

Configuring Address Server Elements for the DHCPv6 Layer 3 Wholesale Solution | 54

- Configuring a DHCPv6 Address Assignment Pool | 55
- Configuring Extended DHCPv6 Local Server | 57

Example: Retailer Dynamic Profile for a DHCPv6 Wholesale Network | 59

Example: Retailer Routing Instances for a DHCPv6 Wholesale Network | 60

Example: DHCPv6 Address Assignment Pool That Provides Full 128-bit IPV6 Addresses for a DHCPv6 Wholesale Network | 61

Example: DHCPv6 Address Assignment Pool That Provides 74-bit IPV6 Prefixes for a DHCPv6 Wholesale Network | 61

Example: Extended DHCPv6 Local Server for a DHCPv6 Wholesale Network | 62

2 Configuring PPPoE Layer 3 Wholesale Networks

Subscriber Management PPPoE Wholesale Overview | 65

Layer 2 and Layer 3 Wholesale Overview | 65

PPPoE Layer 3 Wholesale Configuration Interface Support | 66

Subscriber to Logical System and Routing Instance Relationship | 67

RADIUS VSAs and Broadband Subscriber Management Wholesale Configuration Overview | 67

Configuring PPPoE Layer 3 Wholesale Networks | 69

Broadband Subscriber Management PPPoE Layer 3 Wholesale Topology and Configuration Elements | 69

PPPoE Layer 3 Wholesale Network Topology Overview | 71

Configuring Loopback Interfaces for the PPPoE Layer 3 Wholesale Solution | 73

Configuring Static Customer VLANs for the PPPoE Layer 3 Wholesale Network Solution | 75

Configuring Access Components for the PPPoE Wholesale Network Solution | 76

- Configuring RADIUS Server Access | 76
- Configuring a PPPoE Wholesaler Access Profile | 77
- Configuring PPPoE Retailer Access Profiles | 78

Configuring Dynamic Profiles for the PPPoE Layer 3 Wholesale Network Solution | 80

- Configuring a Wholesale Dynamic Profile for use in the PPPoE Solution | 80

Configuring Separate Routing Instances for PPPoE Service Retailers | 82

Example: Wholesaler Dynamic Profile for a PPPoE Wholesale Network | 84

Example: Retailer Routing Instances for a PPPoE Wholesale Network | 85

3 Configuring Layer 2 Wholesale Networks

Subscriber Management Layer 2 Wholesale Overview | 87

Layer 2 and Layer 3 Wholesale Overview | 87

Wholesale Network Configuration Options and Considerations | 88

RADIUS VSAs and Broadband Subscriber Management Wholesale Configuration Overview | 89

Extensible Subscriber Services Manager | 91

Extensible Subscriber Services Manager Overview | 91

Understanding the Dictionary File | 92

Configuring Layer 2 Wholesale Networks | 93

Broadband Subscriber Management Layer 2 Wholesale Topology and Configuration Elements | 93

Layer 2 Wholesale Network Topology Overview | 94

Configuring a Retail Dynamic Profile for Use in the Layer 2 Wholesale Solution | 96

Stacking and Rewriting VLAN Tags for the Layer 2 Wholesale Solution | 99

Configuring VLAN Interfaces for the Layer 2 Wholesale Solution | 102

Configuring Encapsulation for Layer 2 Wholesale VLAN Interfaces | 105

Configuring Direct ISP-Facing Interfaces for the Layer 2 Wholesale Solution | 107

Configuring Separate Access Routing Instances for Layer 2 Wholesale Service Retailers | 108

Configuring Access Components for the Layer 2 Wholesale Network Solution | 111

Configuring RADIUS Server Access | 111

Configuring a Layer 2 Wholesaler Access Profile | 112

Example: Retailer Dynamic Profile for a Layer 2 Wholesale Network | 113

Example: Access Interface for a Layer 2 Wholesale Network | 114

Example: Retailer Access Routing Instances for a Layer 2 Wholesale Network | 114

Example: Retailer Direct ISP-Facing Interface for a Layer 2 Wholesale Network | 116

4 **Configuring ANCP-Triggered Layer 2 Wholesale Services**

ANCP-Triggered Layer 2 Wholesale Service Overview | 118

Layer 2 Wholesale with ANCP-Triggered VLANs Overview | 118

Configuring ANCP-Triggered Layer 2 Wholesale Services | 138

Configuring ANCP Neighbors | 138

Configuring the ANCP Agent for ANCP-Triggered, Autosensed Dynamic VLANs | 140

Configuring a Username for Authentication of Out-of-Band Triggered Dynamic VLANs | 141

Configuring Out-of-Band ANCP Messages to Trigger Dynamic VLAN Instantiation | 142

Triggering ANCP OAM to Simulate ANCP Port Down and Port Up Messages | 143

Configuring the ANCP Agent to Dampen the Effects of Short-Term Adjacency Losses | **146**

Reestablishing Pending Access Line Sessions for Layer 2 Wholesale | **147**

Configuring Multiple Non-Overlapping VLAN Ranges for Core-Facing Physical Interfaces | **147**

Clearing ANCP Access Loops | **148**

Configuring Flat-File Accounting for Layer 2 Wholesale Services | 150

Flat-File Accounting Overview | **150**

Configuring Flat-File Accounting for Layer 2 Wholesale | **154**

Configuring Flat-File Accounting for Extensible Subscriber Services Management | **159**

Configuring Service Accounting in Local Flat Files | **164**

Configuring Five-Level and Four-Level Heterogeneous Networks | 169

Five-Level and Four-Level Heterogeneous Networks | **169**

- CoS Node Shaping in Four-Level and Five-Level Heterogeneous Networks | **169**
- CuTTB Use Case Topology and CoS Hierarchy | **174**
- FTTB/FTTH Use Case Topology and CoS Hierarchy | **179**
- Automatic Creation of Business Subscriber Interface Sets | **184**
- How to Configure the Automatic Creation of Business Subscriber Interface Sets | **186**
- Dynamic Level 2 and Level 3 Interface Set Naming with Predefined Variables | **186**

OLT Migration to Using PON TLVs Instead of DSL TLVs | **192**

- Support for OLT Migration to PON TLVs | **192**
- How to Configure Preference for DSL or PON TLVs When an OLT Sends Both | **193**

5 **Configuration Statements and Operational Commands**

dynamic-profile (DHCP Local Server) | 196

Junos CLI Reference Overview | 198

About This Guide

Use this guide to understand how wholesaling enables service providers to resell broadband services and enable other providers to deploy their own services over the incumbent network. This guide discusses Layer 3 wholesale networks (DHCP and PPPoE) and Layer 2 wholesale networks (including ANCP-triggered wholesale services).

1

PART

Configuring DHCP Layer 3 Wholesale Networks

- Subscriber Management DHCP Layer 3 Wholesale Overview | **2**
- Configuring DHCPv4 Layer 3 Wholesale Networks | **8**
- Configuring DHCPv6 Layer 3 Wholesale Networks | **37**

CHAPTER 1

Subscriber Management DHCP Layer 3 Wholesale Overview

IN THIS CHAPTER

- Layer 2 and Layer 3 Wholesale Overview | 2
- Wholesale Network Configuration Options and Considerations | 3
- DHCP Layer 3 Wholesale Configuration Interface Support | 4
- Layer 3 Wholesale Configuration DHCP Support | 5
- Subscriber to Logical System and Routing Instance Relationship | 5
- RADIUS VSAs and Broadband Subscriber Management Wholesale Configuration Overview | 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 | 8

Broadband Subscriber Management PPPoE Layer 3 Wholesale Topology and Configuration Elements | 69

Broadband Subscriber Management Layer 2 Wholesale Topology and Configuration Elements | 93

Wholesale Network Configuration Options and Considerations

You can configure a wholesale network any number of ways using Juniper Networks hardware and Junos OS software. 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.

(Continued)

Wholesale Configuration Options	Considerations
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.

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*
- *Configuring a Subscriber Interface Using a Set of Static IP Demux Interfaces*

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*.

RELATED DOCUMENTATION

Extended DHCP Relay Agent Overview

DHCP Relay Proxy Overview

Understanding Differences Between Legacy DHCP and Extended DHCP

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 (primary) 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

Routing Instances Overview

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 1 on page 6 is required for a wholesale network to function.

Table 1: 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

CHAPTER 2

Configuring DHCPv4 Layer 3 Wholesale Networks

IN THIS CHAPTER

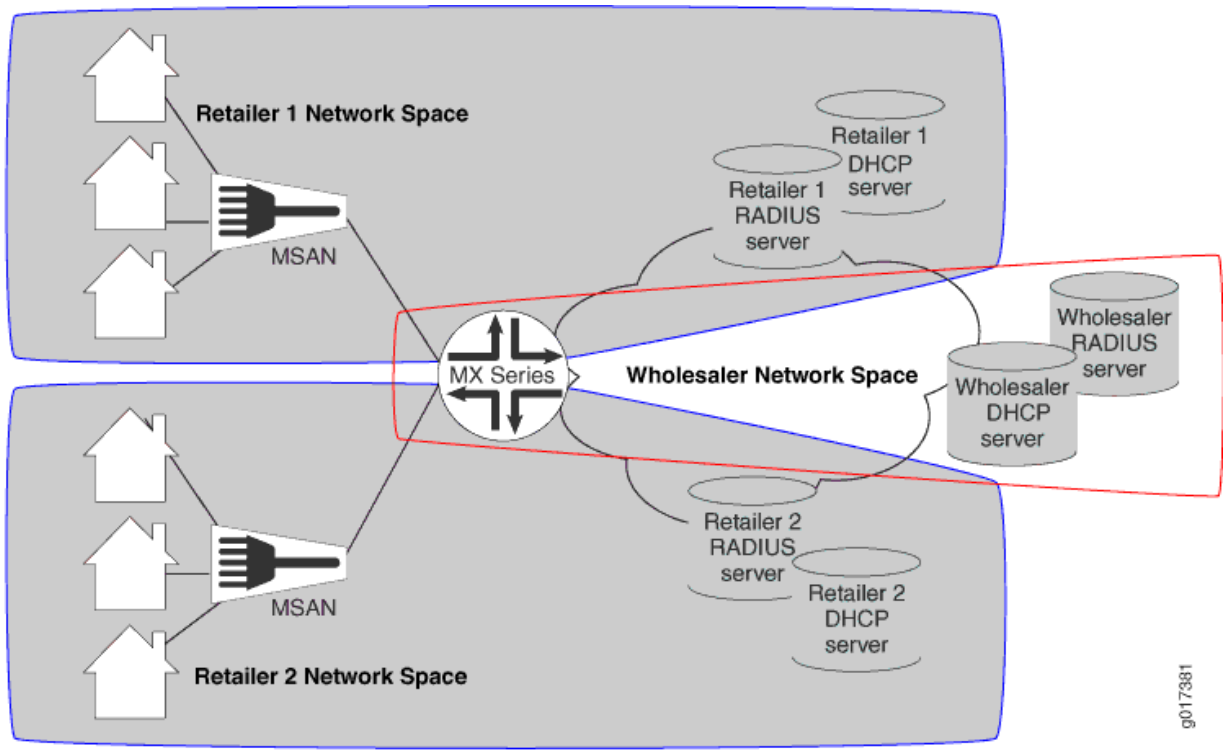
- Broadband Subscriber Management DHCPv4 Layer 3 Wholesale Topology and Configuration Elements | 8
- DHCPv4 Layer 3 Wholesale Network Topology Overview | 10
- Configuring Loopback Interfaces for the DHCPv4 Layer 3 Wholesale Solution | 12
- Configuring VLANs for the DHCPv4 Layer 3 Wholesale Network Solution | 13
- Configuring Access Components for the DHCP Layer 3 Wholesale Network Solution | 18
- Configuring Dynamic Profiles for the DHCPv4 Layer 3 Wholesale Network Solution | 21
- Configuring Separate Routing Instances for DHCPv4 Service Retailers | 25
- Configure Default Forwarding Options for the DHCPv4 Wholesale Network Solution | 28
- Example: Wholesaler Dynamic Profile for a DHCPv4 Wholesale Network | 31
- Example: Retailer Dynamic Profile for a DHCPv4 Wholesale Network | 31
- Example: Default Forwarding Options Configuration for the DHCPv4 Wholesale Network | 32
- Example: Retailer Routing Instances for a DHCPv4 Wholesale Network | 34

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 9 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

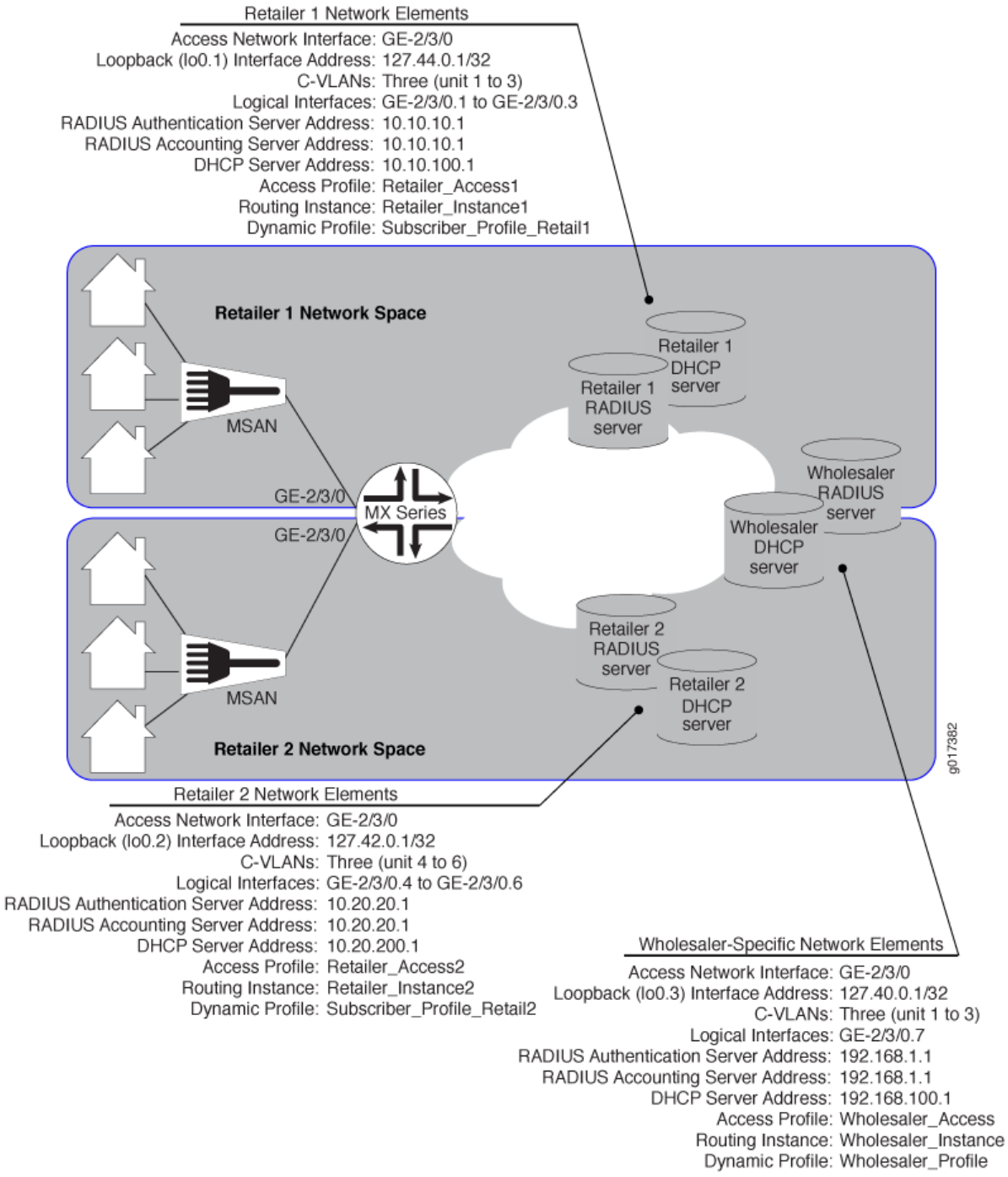
Layer 2 and Layer 3 Wholesale Overview | 2

DHCPv4 Layer 3 Wholesale Network Topology Overview | 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 | 2

Broadband Subscriber Management DHCPv4 Layer 3 Wholesale Topology and Configuration Elements | 8

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

IN THIS SECTION

- Configuring Static Customer VLANs for the DHCPv4 Layer 3 Wholesale Network Solution | 13
- Configuring Dynamic VLANs for the DHCPv4 Layer 3 Wholesale Network Solution | 15

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

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

IN THIS SECTION

- Configuring RADIUS Server Access | **18**
- Configuring a DHCP Wholesaler Access Profile | **19**
- Configuring DHCP Retailer Access Profiles | **20**

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

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
```

SEE ALSO

> *RADIUS Servers and Parameters for Subscriber Access*

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 *RADIUS Servers and Parameters for Subscriber Access*.

7. Configure subscriber accounting (RADIUS accounting).

   See *Configuring Per-Subscriber Session Accounting*.

SEE ALSO

> *Configuring Authentication and Accounting Parameters for Subscriber Access*
>
> *Specifying the Authentication and Accounting Methods for Subscriber Access*
>
> *RADIUS Servers and Parameters for Subscriber Access*
>
> *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 *RADIUS Servers and Parameters for Subscriber Access*.

7. Configure subscriber accounting (RADIUS accounting).

   See *Configuring Per-Subscriber Session Accounting*.

SEE ALSO

- *Configuring Authentication and Accounting Parameters for Subscriber Access*
- *Specifying the Authentication and Accounting Methods for Subscriber Access*
- *RADIUS Servers and Parameters for Subscriber Access*
- *Configuring Per-Subscriber Session Accounting*

Configuring Dynamic Profiles for the DHCPv4 Layer 3 Wholesale Network Solution

IN THIS SECTION

- Configuring a Wholesale Dynamic Profile for use in the DHCPv4 Solution | 22
- Configuring a Dynamic Profile for use by a Retailer in the DHCPv4 Solution | 23

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

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 demu0 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 demu0 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 *Example-Configuring DHCP with External Authentication Server*.

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 *Example-Configuring DHCP with External Authentication Server*.

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.

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 *Example-Configuring DHCP with External Authentication Server*.

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 *Example-Configuring DHCP with External Authentication Server*.

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*
- *Example-Configuring DHCP with External Authentication Server*
- *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 | 21

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 | 21

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 | 28

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 | 25

CHAPTER 3

Configuring DHCPv6 Layer 3 Wholesale Networks

IN THIS CHAPTER

- Broadband Subscriber Management DHCPv6 Layer 3 Wholesale Topology and Configuration Elements | **37**
- DHCPv6 Layer 3 Wholesale Network Topology Overview | **39**
- Configuring Loopback Interfaces for the DHCPv6 Layer 3 Wholesale Solution | **41**
- Configuring VLANs for the DHCPv6 Layer 3 Wholesale Network Solution | **42**
- Configuring Access Components for the DHCP Layer 3 Wholesale Network Solution | **46**
- Configuring Dynamic Profiles for the DHCPv6 Layer 3 Wholesale Network Solution | **50**
- Configuring Separate Routing Instances for DHCPv6 Service Retailers | **53**
- Configuring Address Server Elements for the DHCPv6 Layer 3 Wholesale Solution | **54**
- Example: Retailer Dynamic Profile for a DHCPv6 Wholesale Network | **59**
- Example: Retailer Routing Instances for a DHCPv6 Wholesale Network | **60**
- Example: DHCPv6 Address Assignment Pool That Provides Full 128-bit IPV6 Addresses for a DHCPv6 Wholesale Network | **61**
- Example: DHCPv6 Address Assignment Pool That Provides 74-bit IPV6 Prefixes for a DHCPv6 Wholesale Network | **61**
- Example: Extended DHCPv6 Local Server for a DHCPv6 Wholesale Network | **62**

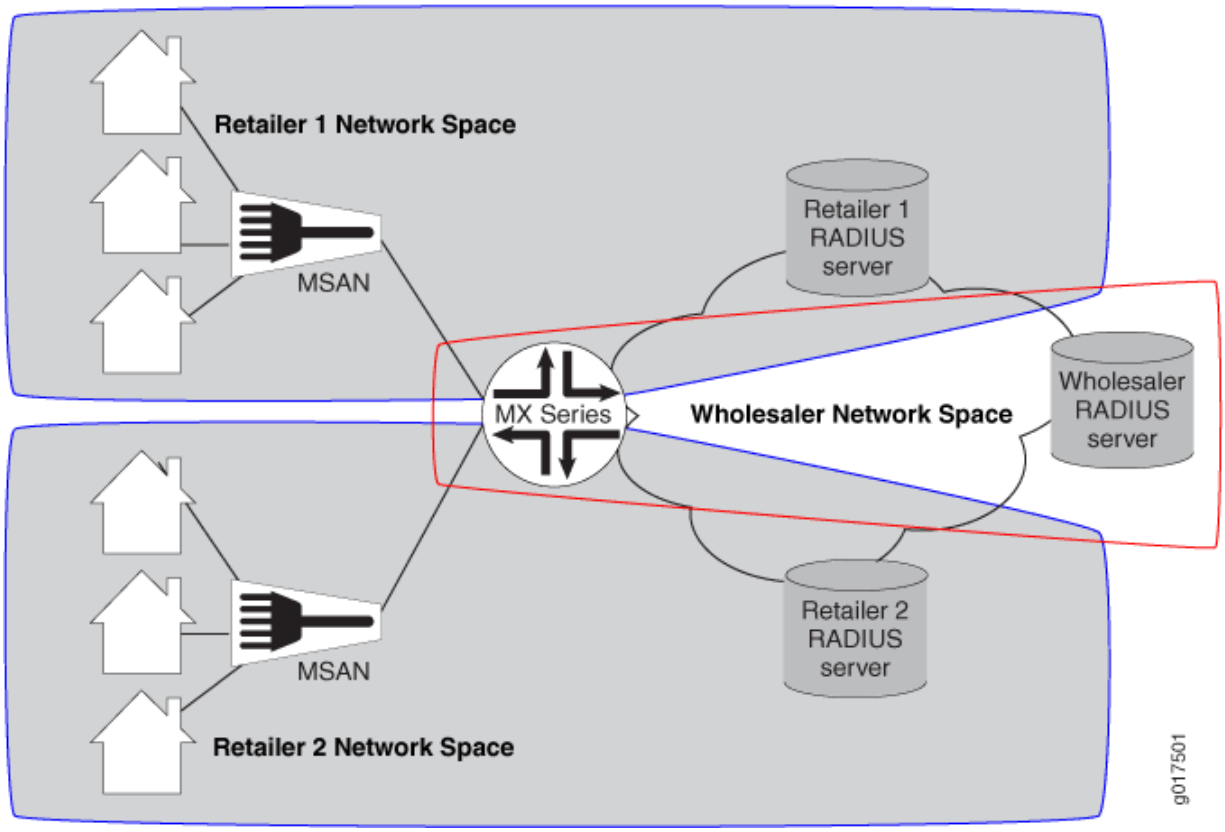
Broadband Subscriber Management DHCPv6 Layer 3 Wholesale Topology and Configuration Elements

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 38 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

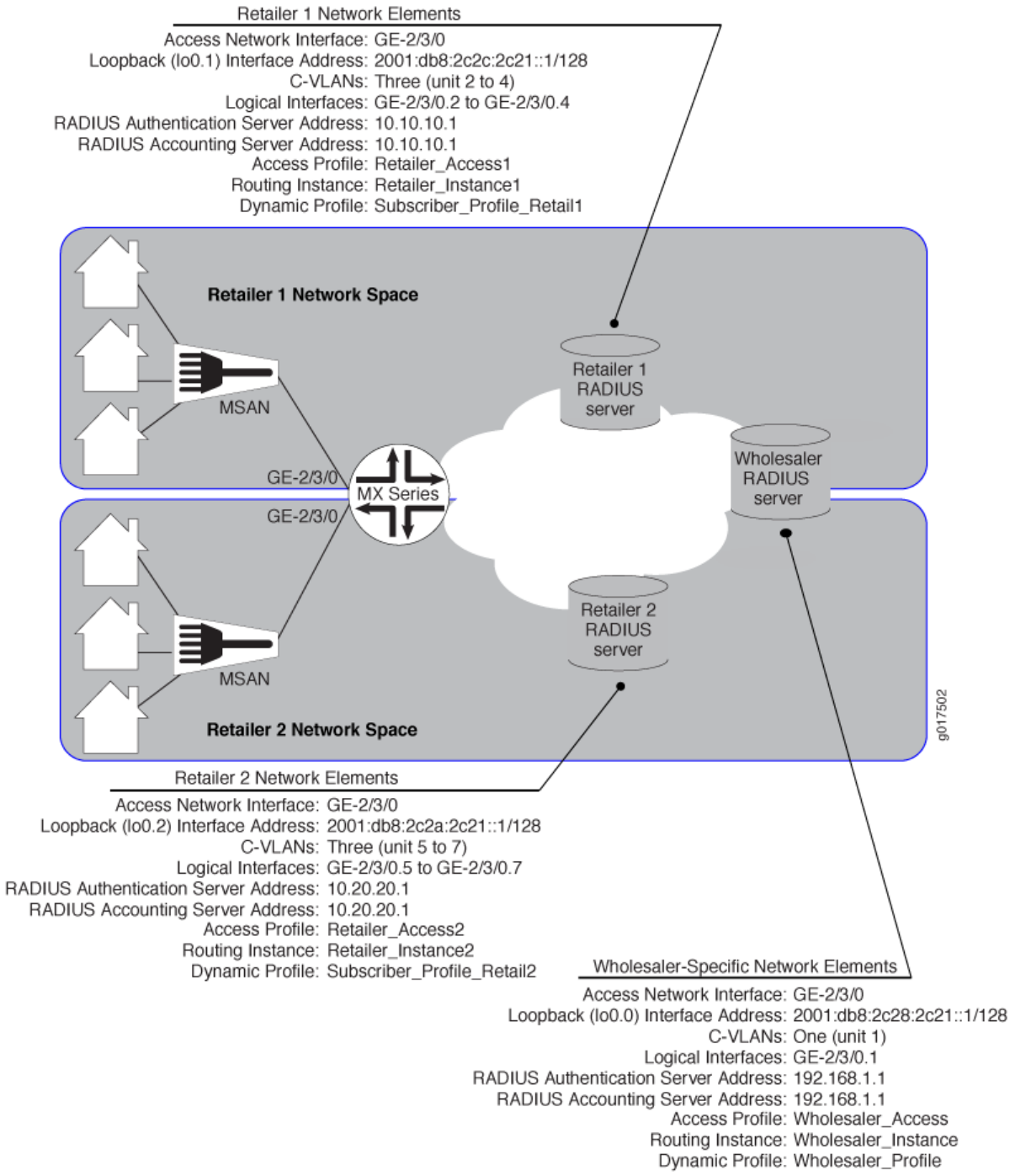
Layer 2 and Layer 3 Wholesale Overview | 2

DHCPv6 Layer 3 Wholesale Network Topology Overview | 39

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 40 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 | 2

Broadband Subscriber Management DHCPv4 Layer 3 Wholesale Topology and Configuration Elements | 8

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

IN THIS SECTION

- Configuring Static Customer VLANs for the DHCPv6 Layer 3 Wholesale Network Solution | 42
- Configuring Dynamic Customer VLANs for the DHCPv6 Layer 3 Wholesale Network Solution | 44

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

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

IN THIS SECTION

- Configuring RADIUS Server Access | 47
- Configuring a DHCP Wholesaler Access Profile | 47
- Configuring DHCP Retailer Access Profiles | 48

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

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
```

SEE ALSO

> *RADIUS Servers and Parameters for Subscriber Access*

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 *RADIUS Servers and Parameters for Subscriber Access*.

7. Configure subscriber accounting (RADIUS accounting).

   See *Configuring Per-Subscriber Session Accounting*.

SEE ALSO

> *Configuring Authentication and Accounting Parameters for Subscriber Access*
>
> *Specifying the Authentication and Accounting Methods for Subscriber Access*
>
> *RADIUS Servers and Parameters for Subscriber Access*
>
> *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 *RADIUS Servers and Parameters for Subscriber Access*.

7. Configure subscriber accounting (RADIUS accounting).

   See *Configuring Per-Subscriber Session Accounting*.

SEE ALSO

- *Configuring Authentication and Accounting Parameters for Subscriber Access*
- *Specifying the Authentication and Accounting Methods for Subscriber Access*
- *RADIUS Servers and Parameters for Subscriber Access*
- *Configuring Per-Subscriber Session Accounting*

Configuring Dynamic Profiles for the DHCPv6 Layer 3 Wholesale Network Solution

IN THIS SECTION

- Configuring a Wholesale Dynamic Profile for use in the DHCPv6 Solution | 50
- Configuring a Dynamic Profile for use by Each Retailer in the DHCPv6 Solution | 51

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

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 demu0 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-ipv6-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 demu0 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.

If the router connects directly to an ISP network (or ISP-controlled device), you must configure the routing instances as an access routing instance.

To define a retailer routing instance:

1. Create the retailer routing instance.

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

2. Specify the routing instance type for the retailer.

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

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

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

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

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

5. 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.

6. Repeat this procedure for other retailers.

Configuring Address Server Elements for the DHCPv6 Layer 3 Wholesale Solution

IN THIS SECTION

- Configuring a DHCPv6 Address Assignment Pool | 55
- Configuring Extended DHCPv6 Local Server | 57

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:

1. 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 | 50

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 | 53

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;
                }
            }
        }
    }
}
```

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 | 54

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 | 54

2

PART

Configuring PPPoE Layer 3 Wholesale Networks

- Subscriber Management PPPoE Wholesale Overview | **65**
- Configuring PPPoE Layer 3 Wholesale Networks | **69**

CHAPTER 4

Subscriber Management PPPoE Wholesale Overview

IN THIS CHAPTER

- Layer 2 and Layer 3 Wholesale Overview | 65
- PPPoE Layer 3 Wholesale Configuration Interface Support | 66
- Subscriber to Logical System and Routing Instance Relationship | 67
- RADIUS VSAs and Broadband Subscriber Management Wholesale Configuration Overview | 67

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 | **8**
- Broadband Subscriber Management PPPoE Layer 3 Wholesale Topology and Configuration Elements | **69**
- Broadband Subscriber Management Layer 2 Wholesale Topology and Configuration Elements | **93**

PPPoE Layer 3 Wholesale Configuration Interface Support

PPPoE Layer 3 wholesale requires the use of PPP interfaces. This means that you must specify the PP0 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*
- *Configuring Dynamic PPPoE Subscriber Interfaces*

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 (primary) 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

Routing Instances Overview

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 2 on page 68 is required for a wholesale network to function.

Table 2: 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

CHAPTER 5

Configuring PPPoE Layer 3 Wholesale Networks

IN THIS CHAPTER

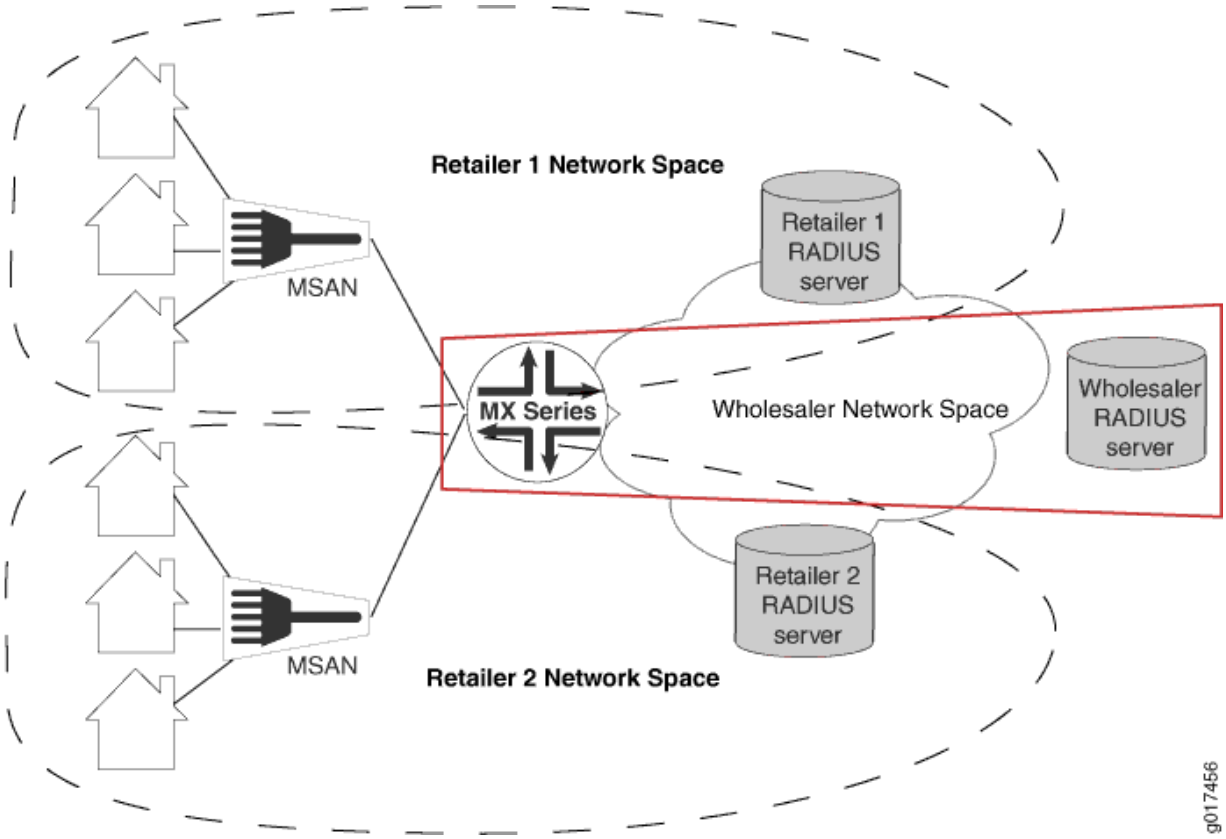
- Broadband Subscriber Management PPPoE Layer 3 Wholesale Topology and Configuration Elements | 69
- PPPoE Layer 3 Wholesale Network Topology Overview | 71
- Configuring Loopback Interfaces for the PPPoE Layer 3 Wholesale Solution | 73
- Configuring Static Customer VLANs for the PPPoE Layer 3 Wholesale Network Solution | 75
- Configuring Access Components for the PPPoE Wholesale Network Solution | 76
- Configuring Dynamic Profiles for the PPPoE Layer 3 Wholesale Network Solution | 80
- Configuring Separate Routing Instances for PPPoE Service Retailers | 82
- Example: Wholesaler Dynamic Profile for a PPPoE Wholesale Network | 84
- Example: Retailer Routing Instances for a PPPoE Wholesale Network | 85

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 70 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



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

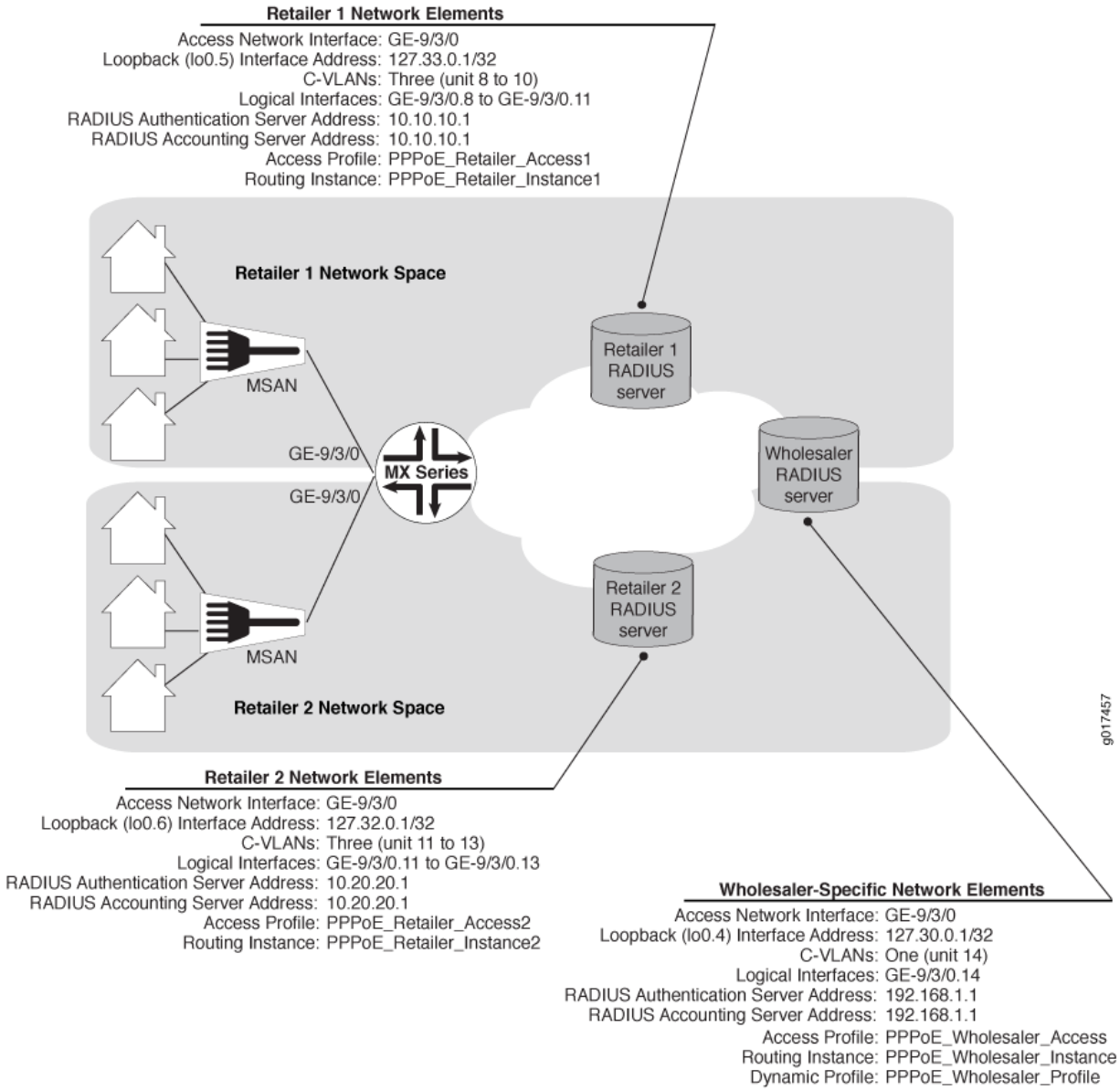
Layer 2 and Layer 3 Wholesale Overview | 2

PPPoE Layer 3 Wholesale Network Topology Overview | 71

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 72 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 | 2

Broadband Subscriber Management DHCPv4 Layer 3 Wholesale Topology and Configuration Elements | 8

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

IN THIS SECTION

- Configuring RADIUS Server Access | 76
- Configuring a PPPoE Wholesaler Access Profile | 77
- Configuring PPPoE Retailer Access Profiles | 78

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

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
```

SEE ALSO

> *RADIUS Servers and Parameters for Subscriber Access*

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 *RADIUS Servers and Parameters for Subscriber Access*.

7. Configure subscriber accounting (RADIUS accounting).

   See *Configuring Per-Subscriber Session Accounting*.

SEE ALSO

> *Configuring Authentication and Accounting Parameters for Subscriber Access*
>
> *Specifying the Authentication and Accounting Methods for Subscriber Access*
>
> *RADIUS Servers and Parameters for Subscriber Access*
>
> *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 *RADIUS Servers and Parameters for Subscriber Access*.

7. Configure subscriber accounting (RADIUS accounting).

   See *Configuring Per-Subscriber Session Accounting*.

SEE ALSO

- *Configuring Authentication and Accounting Parameters for Subscriber Access*
- *Specifying the Authentication and Accounting Methods for Subscriber Access*
- *RADIUS Servers and Parameters for Subscriber Access*
- *Configuring Per-Subscriber Session Accounting*

Configuring Dynamic Profiles for the PPPoE Layer 3 Wholesale Network Solution

IN THIS SECTION

- Configuring a Wholesale Dynamic Profile for use in the PPPoE Solution | 80

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

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.

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 | 80

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 | 82

PART 3

Configuring Layer 2 Wholesale Networks

- Subscriber Management Layer 2 Wholesale Overview | **87**
- Configuring Layer 2 Wholesale Networks | **93**

CHAPTER 6

Subscriber Management Layer 2 Wholesale Overview

IN THIS CHAPTER

- Layer 2 and Layer 3 Wholesale Overview | 87
- Wholesale Network Configuration Options and Considerations | 88
- RADIUS VSAs and Broadband Subscriber Management Wholesale Configuration Overview | 89
- Extensible Subscriber Services Manager | 91

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 | 8
- Broadband Subscriber Management PPPoE Layer 3 Wholesale Topology and Configuration Elements | 69
- Broadband Subscriber Management Layer 2 Wholesale Topology and Configuration Elements | 93

Wholesale Network Configuration Options and Considerations

You can configure a wholesale network any number of ways using Juniper Networks hardware and Junos OS software. 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.

(Continued)

Wholesale Configuration Options	Considerations
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 89 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

Extensible Subscriber Services Manager

IN THIS SECTION

- Extensible Subscriber Services Manager Overview | 91
- Understanding the Dictionary File | 92

Extensible Subscriber Services Manager Overview

Extensible Subscriber Services Manager (ESSM) is a background process that is part of the Intelligent Customer Extendable authentication, authorization, and accounting (ICE-AAA) framework, which supports customer extensible services for both business and residential subscribers. Services are classified as residential or business on the basis of the value specified for the RADIUS VSA (26-173) `ERX-Service-Activate-Type` that is received in the Access-Accept message.

Extensible Subscriber Services Manager uses the ICE-AAA framework, which comprises a dictionary, operation scripts, and RADIUS vendor-specific attributes (VSAs), to create business services for subscribers without modifying Junos OS. Extensible Subscriber Services Manager supports only the `ERX-Activate` service type.

Using the Extensible Subscriber Services Manager, you can create business services using the following sources:

- The dictionary that refers to or invokes the operation scripts.
- The operation scripts that you use to create subscriber-specific configuration
- The VSAs that the RADIUS server sends that contain configuration values for provisioning services

SEE ALSO

Understanding the Dictionary File | 92

show subscribers

show subscribers summary

Configuring Flat-File Accounting for Extensible Subscriber Services Management | 159

Understanding the Dictionary File

The XML-based dictionary specifies the action to be taken by ESSMD when it receives a service request. The dictionary contains provisioning, deprovisioning, and operation scripts. ESSMD parses the dictionary file during initialization and stores the parsed information in the database. Extensible Subscriber Services Manager acts on the extensible-subscriber-service requests on the basis of the services configured in the dictionary file.

During a commit operation, essmd verifies the path and the filename of the dictionary file. If the path or the filename is invalid, the commit operation fails and the error is logged in a system log message. Restarting the daemon or performing a graceful Routing Engine switchover (GRES) operation forces essmd to use the new dictionary. Ensure that you always configure a valid dictionary for essmd.

When loading the dictionary file after a successful commit operation, essmd validates whether:

- There are errors in parsing the dictionary file.
- The operation scripts specified in the dictionary file are available on the router.
- Any active services are modified.

If the validation fails, an error is logged in a system log message, and essmd continues to use the existing version of the dictionary file. Use the `request services extensible-subscriber-services reload-dictionary` command to reload the dictionary file after resolving the errors.

SEE ALSO

> *dictionary*
>
> *show extensible-subscriber-services dictionary*
>
> *show extensible-subscriber-services dictionary attributes*
>
> *show extensible-subscriber-services dictionary services*

CHAPTER 7

Configuring Layer 2 Wholesale Networks

IN THIS CHAPTER

- Broadband Subscriber Management Layer 2 Wholesale Topology and Configuration Elements | **93**
- Layer 2 Wholesale Network Topology Overview | **94**
- Configuring a Retail Dynamic Profile for Use in the Layer 2 Wholesale Solution | **96**
- Stacking and Rewriting VLAN Tags for the Layer 2 Wholesale Solution | **99**
- Configuring VLAN Interfaces for the Layer 2 Wholesale Solution | **102**
- Configuring Encapsulation for Layer 2 Wholesale VLAN Interfaces | **105**
- Configuring Direct ISP-Facing Interfaces for the Layer 2 Wholesale Solution | **107**
- Configuring Separate Access Routing Instances for Layer 2 Wholesale Service Retailers | **108**
- Configuring Access Components for the Layer 2 Wholesale Network Solution | **111**
- Example: Retailer Dynamic Profile for a Layer 2 Wholesale Network | **113**
- Example: Access Interface for a Layer 2 Wholesale Network | **114**
- Example: Retailer Access Routing Instances for a Layer 2 Wholesale Network | **114**
- Example: Retailer Direct ISP-Facing Interface for a Layer 2 Wholesale Network | **116**

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. 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.
- VLAN interface configuration
- RADIUS server access configuration
- Core network configuration

RELATED DOCUMENTATION

Layer 2 and Layer 3 Wholesale Overview | 2

Layer 2 Wholesale Network Topology Overview | 94

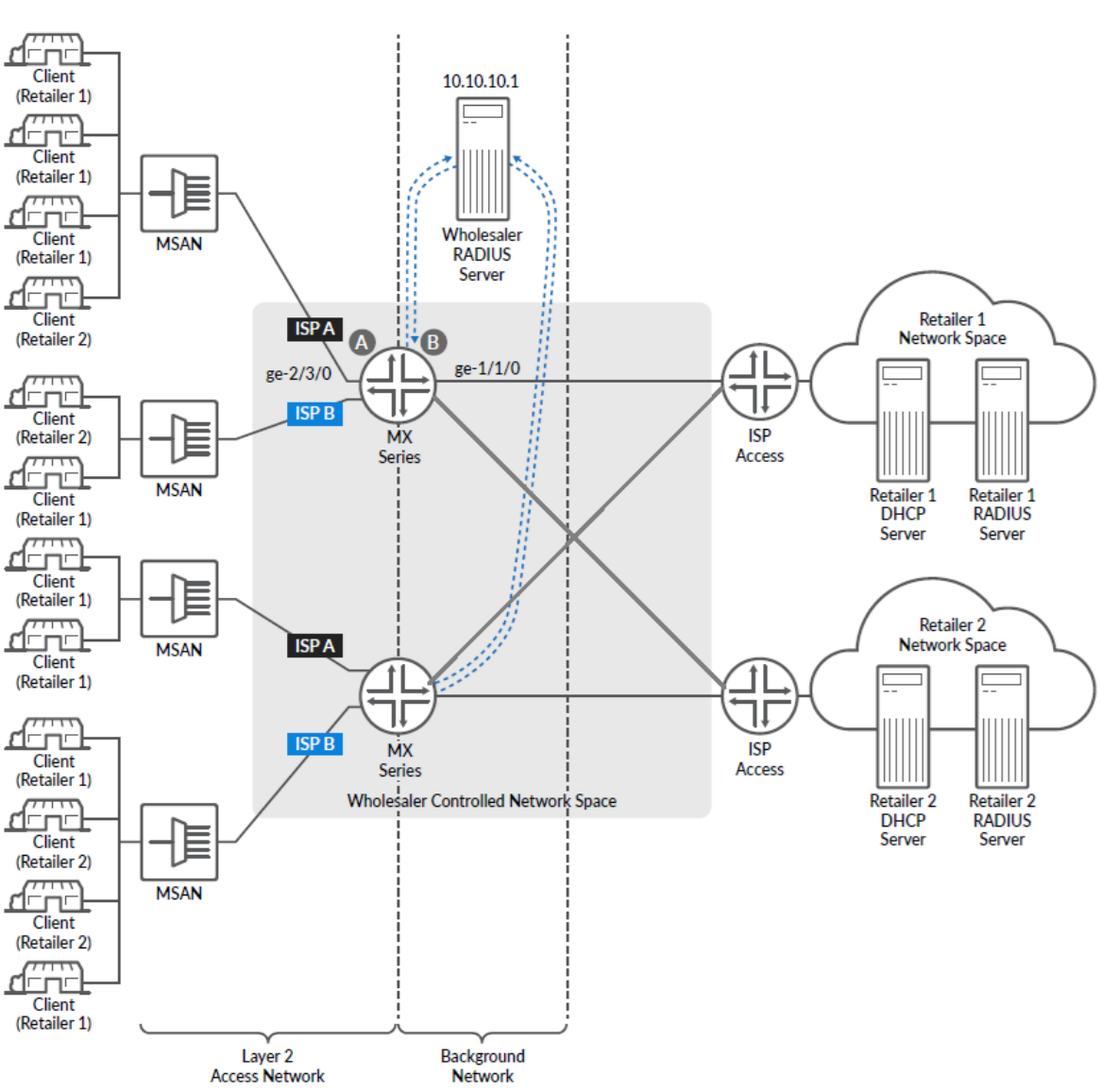
Layer 2 Wholesale Network Topology Overview

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 Layer 2 Network access routers.

The example 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.

Figure 7 on page 95 provides the reference topology for this configuration example.

Figure 7: Layer 2 Wholesale Network Reference Topology



RELATED DOCUMENTATION

Layer 2 and Layer 3 Wholesale Overview | 2

Broadband Subscriber Management Layer 2 Wholesale Topology and Configuration Elements | 93

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

To configure a dynamic profile for use with retailer access:

NOTE: To support Layer 2 access profiles the RADIUS server must provide VLAN authentication.

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# edit 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# edit unit $junos-interface-unit
```

6. (Optional) Define 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 an encapsulation for the physical interface.

7. Define the VLAN tag parameters 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 Broadband Subscriber VLANs and Interfaces User Guide.

```
[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 99 for details. For our example, we use:

```
[edit dynamic-profiles Subscriber_Profile_Retail1 interfaces “$junos-interface-ifd-name” unit
“$junos-interface-unit”]
user@host# set input-vlan-map swap-push
user@host# set input-vlan-map vlan-id "$junos-vlan-map-id"
user@host# set input-vlan-map inner-vlan-id "$junos-inner-vlan-map-id"
user@host# set output-vlan-map pop-swap
user@host# set output-vlan-map inner-tag-protocol-id 0x8100
```

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
```

The result is a dynamic subscriber profile that uses RADIUS authentication to assign the outer VLAN ID dynamically.

The dynamic profile is displayed in curly brace format:

```
[edit]
user@host# show dynamic-profiles
Subscriber_Profile_Retail1
    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-push;
                    vlan-id "$junos-vlan-map-id";
                    inner-vlan-id "$junos-inner-vlan-map-id";
                }
                output-vlan-map {
                    pop-swap;
                    inner-tag-protocol-id 0x8100;
                }
                family vpls;
            }
        }
    }
```

The need to authenticate the VLAN through RADIUS is specified by `"$junos-vlan-map-id"` and `"$junos-vlan-id"` parameters.

The outer VLAN ID is returned by the RADIUS server as part of the user name attribute, as shown:

```
Type: VLAN
User Name: user1.xe-0/1/0:2015
Logical System: default
Routing Instance: ISP02-Test
Interface: xe-0/1/0.3221225509
Interface type: Dynamic
Underlying Interface: xe-0/1/0
Core IFL Name: xe-0/1/3.0
Dynamic Profile Name: Subscriber_Profile_Retail1
Dynamic Profile Version: 1
State: Active
Radius Accounting ID: 43
Session ID: 43
PFE Flow ID: 87
VLAN Id: 2015
VLAN Map Id: 100
Inner VLAN Map Id: 201
Login Time: 2021-07-07 06:42:33 PDT
Dynamic configuration:
  junos-vlan-map-id: 100
```

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 4 on page 100 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 4: 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
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 5 on page 100 shows what rewrite operation combinations you can configure. "None" means that no rewrite operation is specified for the VLAN map.

Table 5: 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

Table 5: Applying Rewrite Operations to VLAN Maps *(Continued)*

Input VLAN Map	Output VLAN Map			
	none	push	pop	swap
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.

NOTE: To support Layer 2 access profiles the RADIUS server must provide VLAN authentication.

To configure a VLAN interface for dynamic client access:

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

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

2. Specify the encapsulation type for the VLAN interfaces.

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

3. 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
```

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

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

5. Specify that you want to configure stacked VLANs.

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

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

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

7. Define the VLAN ranges for the dynamic profile.

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

8. Move up two levels in the configuration hierarchy to define the VLAN authentication profile.

```
[edit interfaces ge-2/3/0 auto-configure stacked-vlan-ranges dynamic-profile
“Subscriber_Profile_Retail1”]
user@host# up 2
[edit interfaces ge-2/3/0 auto-configure stacked-vlan-ranges]
user@host# set authentication password abc123
user@host# set authentication username-include user-prefix user1
user@host# set authentication username-include interface-name
user@host# set access-profile access-profile-1
```

9. Define a simple access profile that specifies the RADIUS server used to provide VLAN authentication. Use the `top` command to position yourself at the edit hierarchy.

```
[edit]
user@host# set access profile access-profile-1 radius-server 10.10.10.1 secret abc123
```

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

The configuration of the VLAN Interface for the Layer 2 wholesale dynamic profile is displayed in curly brace format:

```
[edit]
user@host# show interfaces
ge-2/3/0 {
    flexible-vlan-tagging;
    auto-configure {
        stacked-vlan-ranges {
            dynamic-profile Subscriber_Profile_Retail1 {
                accept any;
                ranges {
                    any,any;
                }
            }
            authentication {
                password abc123;
                username-include {
                    user-prefix user1;
                    interface-name;
                }
            }
```

```
            access-profile access-profile-1;
        }
    }
}
```

RELATED DOCUMENTATION

Configuring Encapsulation for Layer 2 Wholesale VLAN Interfaces | 105

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 6 on page 105 provides the valid encapsulation combinations for both dynamic profiles and physical interfaces in the Layer 2 wholesale network.

Table 6: 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.

Table 6: Encapsulation Combinations for Layer 2 Wholesale Interfaces *(Continued)*

Dynamic Profile Encapsulation	Physical Interface Encapsulation	Usage Notes
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 | 96

Configuring VLAN Interfaces for the Layer 2 Wholesale Solution | 102

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 Separate Access Routing Instances for Layer 2 Wholesale Service Retailers | 108

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.

If the router connects directly to an ISP network (or ISP-controlled device), you must configure the routing instances as an access routing instance.

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 10.10.1.1:1
```

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.

Configuring Access Components for the Layer 2 Wholesale Network Solution

IN THIS SECTION

- Configuring RADIUS Server Access | 111
- Configuring a Layer 2 Wholesaler Access Profile | 112

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

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
```

SEE ALSO

RADIUS Servers and Parameters for Subscriber Access

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 Access Profile Options for Interactions with RADIUS Servers*.

7. Configure subscriber accounting (RADIUS accounting).

   See *Configuring Per-Subscriber Session Accounting*.

SEE ALSO

Configuring Authentication and Accounting Parameters for Subscriber Access

Specifying the Authentication and Accounting Methods for Subscriber Access

RADIUS Servers and Parameters for Subscriber Access

Configuring Per-Subscriber Session Accounting

Example: Retailer Dynamic Profile for a Layer 2 Wholesale Network

```
dynamic-profiles {
    Subscriber_Profile_Retail1 {
        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 | 2

Layer 2 Wholesale Network Topology Overview | 94

Configuring a Retail Dynamic Profile for Use in the Layer 2 Wholesale Solution | 96

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 | 2
- Layer 2 Wholesale Network Topology Overview | 94
- Configuring VLAN Interfaces for the Layer 2 Wholesale Solution | 102

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 | 2
- Layer 2 Wholesale Network Topology Overview | 94
- Configuring Separate Access Routing Instances for Layer 2 Wholesale Service Retailers | 108

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 | 2
- Layer 2 Wholesale Network Topology Overview | 94
- Configuring Direct ISP-Facing Interfaces for the Layer 2 Wholesale Solution | 107

4

PART

Configuring ANCP-Triggered Layer 2 Wholesale Services

- ANCP-Triggered Layer 2 Wholesale Service Overview | **118**
- Configuring ANCP-Triggered Layer 2 Wholesale Services | **138**
- Configuring Flat-File Accounting for Layer 2 Wholesale Services | **150**
- Configuring Five-Level and Four-Level Heterogeneous Networks | **169**

CHAPTER 8

ANCP-Triggered Layer 2 Wholesale Service Overview

IN THIS CHAPTER

- Layer 2 Wholesale with ANCP-Triggered VLANs Overview | **118**

Layer 2 Wholesale with ANCP-Triggered VLANs Overview

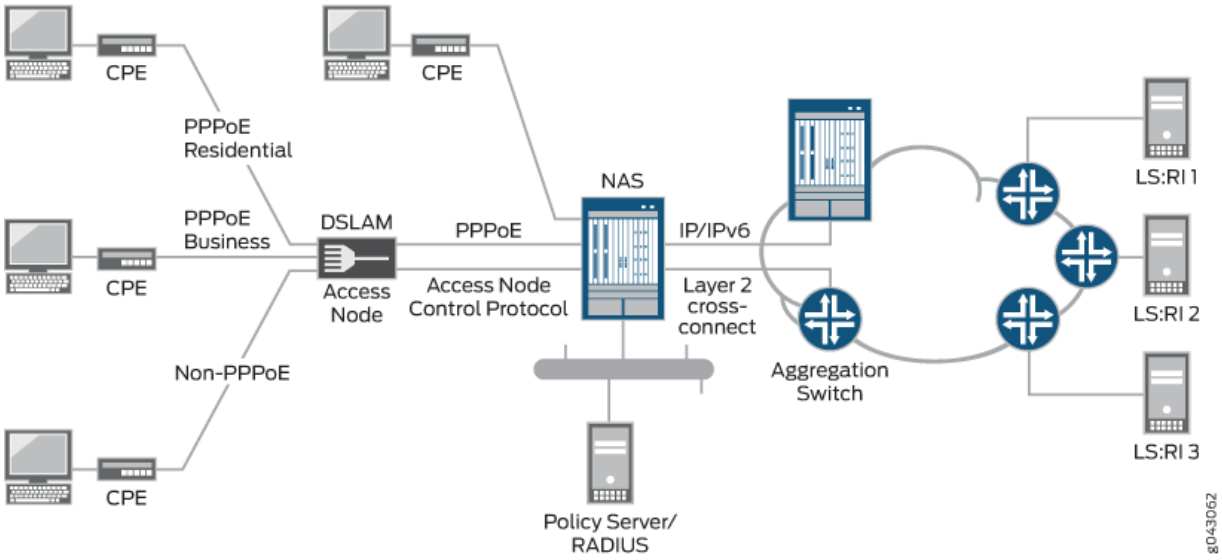
IN THIS SECTION

- RADIUS Authorization for ANCP-Triggered VLANs | **121**
- Instantiation of an ANCP-Triggered, Autosensed, Dynamic VLAN | **121**
- Weighted Load Balancing for Subscriber Sessions over Eligible Core-Facing Physical Interfaces | **122**
- RADIUS Interim Accounting Updates | **123**
- Removal of the Layer 2 Wholesale Service | **124**
- Interactions Between In-Band and Out-of-Band VLAN Autosensing | **125**
- Migration of Subscriber Ownership from Wholesaler to Retailer | **127**
- Migration of Subscriber Ownership from Retailer to Wholesaler | **128**
- Migration of Subscriber Ownership Between Retailers | **128**
- Modification of the Access Line Identifier or Port VLAN Identifier | **129**
- Disconnecting PPPoE Sessions and Automatically Attempting Reconnection as Layer 2 Wholesale Sessions | **130**
- Consequences of a State Transition in the Access-Facing Physical Interface | **131**
- Consequences of a State Transition from Up to Down in the Core-Facing Physical Interface | **133**
- Consequences of a State Transition from Down to Up in the Core-Facing Physical Interface | **134**
- Loss of ANCP TCP Adjacency | **135**

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 8 on page 119 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 8: 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

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

Tthe 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 thecleared 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.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

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 | **142**

Configuring the ANCP Agent for ANCP-Triggered, Autosensed Dynamic VLANs | **140**

Configuring the ANCP Agent

ANCP and the ANCP Agent Overview

Junos OS Predefined Variables

Juniper Networks VSAs Supported by the AAA Service Framework

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

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

CHAPTER 9

Configuring ANCP-Triggered Layer 2 Wholesale Services

IN THIS CHAPTER

- Configuring ANCP Neighbors | **138**
- Configuring the ANCP Agent for ANCP-Triggered, Autosensed Dynamic VLANs | **140**
- Configuring a Username for Authentication of Out-of-Band Triggered Dynamic VLANs | **141**
- Configuring Out-of-Band ANCP Messages to Trigger Dynamic VLAN Instantiation | **142**
- Triggering ANCP OAM to Simulate ANCP Port Down and Port Up Messages | **143**
- Configuring the ANCP Agent to Dampen the Effects of Short-Term Adjacency Losses | **146**
- Reestablishing Pending Access Line Sessions for Layer 2 Wholesale | **147**
- Configuring Multiple Non-Overlapping VLAN Ranges for Core-Facing Physical Interfaces | **147**
- Clearing ANCP Access Loops | **148**

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
```

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.

NOTE: The following physical interface types are supported: aggregated Ethernet (ae), Gigabit Ethernet (ge), 10-Gigabit Ethernet (xe), 100-Gigabit Ethernet (et), demux, and pseudowire (ps). The ps interface type was added in Junos OS Release 19.3R1.

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
```

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

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

ANCP and the ANCP Agent Overview

Layer 2 Wholesale with ANCP-Triggered VLANs Overview | **118**

Configuring Out-of-Band ANCP Messages to Trigger Dynamic VLAN Instantiation | **142**

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 (Interfaces)]
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 (Interfaces)]
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 | **142**

Configuring the ANCP Agent for ANCP-Triggered, Autosensed Dynamic VLANs | **140**

Layer 2 Wholesale with ANCP-Triggered VLANs Overview | **118**

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 | 118

Configuring the ANCP Agent for ANCP-Triggered, Autosensed Dynamic VLANs | 140

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 | 118

Triggering ANCP OAM to Test the Local Loop

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

ANCP and the ANCP Agent Overview

Layer 2 Wholesale with ANCP-Triggered VLANs Overview | 118

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 | 118

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];
...
```

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 | 118

CHAPTER 10

Configuring Flat-File Accounting for Layer 2 Wholesale Services

IN THIS CHAPTER

- Flat-File Accounting Overview | 150
- Configuring Flat-File Accounting for Layer 2 Wholesale | 154
- Configuring Flat-File Accounting for Extensible Subscriber Services Management | 159
- Configuring Service Accounting in Local Flat Files | 164

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.

NOTE: Starting in Junos OS Release 18.4R1, flat-file service accounting to a local file is no longer supported.

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 7 on page 151 lists the elements and their values in the sample header.

Table 7: 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

Table 7: Value of Elements in Sample Accounting Flat File XML Header *(Continued)*

Description	Header Element	Value
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 primary role occurs for both the new primary Routing Engine and the new backup Routing Engine or for only the new primary 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 primary role occurs, the new backup Routing Engine saves its files to the **/var/log/pfedBackup/** directory. The primary 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.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

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 | 159
- Configuring Flat-File Accounting for Layer 2 Wholesale | 154
- Configuring Service Accounting in Local Flat Files | 164
- 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 primary Routing Engine when a change in primary role 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-profileflat-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-profileflat-file-profile-name
```

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

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 | **150**
- Configuring Flat-File Accounting for Extensible Subscriber Services Management | **159**
- Layer 2 Wholesale with ANCP-Triggered VLANs Overview | **118**

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 form the primary 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 primary Routing Engine when a change in primary role 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
```

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

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 | 154

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.

NOTE: Starting in Junos OS Release 18.4R1, service accounting in local flat files is no longer supported. If included in a configuration, it is ignored.

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 primary Routing Engine when a change in primary role 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.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

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 | 150

CHAPTER 11

Configuring Five-Level and Four-Level Heterogeneous Networks

IN THIS CHAPTER

- Five-Level and Four-Level Heterogeneous Networks | 169
- OLT Migration to Using PON TLVs Instead of DSL TLVs | 192

Five-Level and Four-Level Heterogeneous Networks

IN THIS SECTION

- CoS Node Shaping in Four-Level and Five-Level Heterogeneous Networks | 169
- CuTTB Use Case Topology and CoS Hierarchy | 174
- FTTB/FTTH Use Case Topology and CoS Hierarchy | 179
- Automatic Creation of Business Subscriber Interface Sets | 184
- How to Configure the Automatic Creation of Business Subscriber Interface Sets | 186
- Dynamic Level 2 and Level 3 Interface Set Naming with Predefined Variables | 186

CoS Node Shaping in Four-Level and Five-Level Heterogeneous Networks

A heterogeneous subscriber access model has the following characteristics:

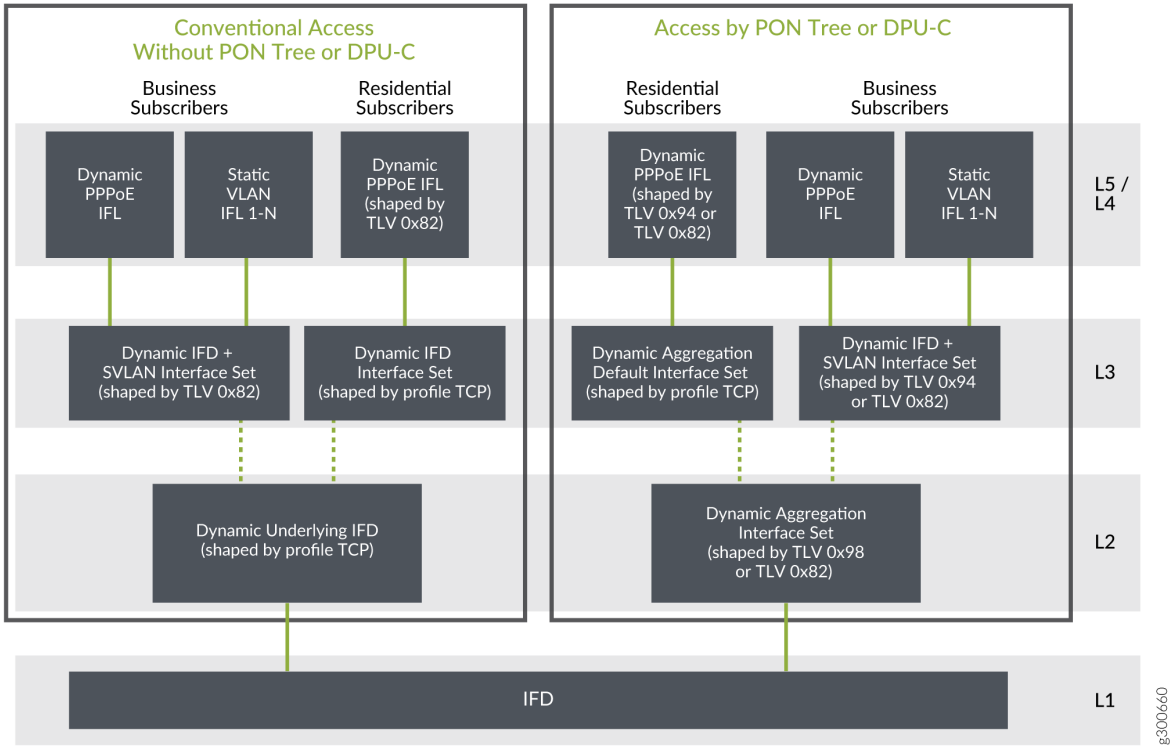
- It includes both residential subscribers and business subscribers. Both subscriber types are typically PPPoE subscribers.
- The access technologies can be conventional or shared media, or both. Shared media access includes bonded copper connections through a DPU-C or fiber connections through a DPU-P. DPU-C and

DPU-P are distribution units for the respective media type. Conventional access networks do not include either a DPU-C or DPU-P.

- Traffic shaping depends on hierarchical CoS. The network can use a four-level scheduler hierarchy, a five-level scheduler hierarchy, or both.

Figure 9 on page 170 summarizes how CoS shapes key nodes in the five-level scheduler hierarchy. Shaping is based either on the adjusted rates from the DSL and PON TLVs or on traffic control profiles in the dynamic client profile configuration. A CoS adjustment control profile specifies the source of the shaping rate applied to a given node.

Figure 9: Five-Level CoS Node Shaping Summary



The following lists describe the CoS scheduler nodes by access type and subscriber type for the five-level hierarchy in Figure 9 on page 170.

For conventional access, residential subscribers:

- Level 1 node—Corresponds to the access-facing physical interface.
- Level 2 node—Corresponds to a dynamic interface set that conserves L2 nodes. This parent interface set is based on the underlying physical interface. The name is derived from the predefined variable,

$junos-phy-ifd-underlying-intf-set-name, by appending “-underlying”. Traffic shaping is determined by a traffic control profile specified in the dynamic client profile.

- Level 3 node—Corresponds to a dynamic interface set that conserves Level 3 nodes. This child interface set is based on the physical interface. The name is derived from the predefined variable, $junos-phy-ifd-intf-set-name. Traffic shaping is determined by a traffic control profile specified in the dynamic client profile.
- Level 4 node—Corresponds to the subscriber’s PPPoE session logical interface. Traffic shaping is determined by the Actual-Data-Rate-Downstream TLV (0x82).
- Level 5 node—Corresponds to the scheduling queue for the subscriber.

For conventional access, business subscribers:

- Level 1 node—Corresponds to the access-facing physical interface.
- Level 2 node—Corresponds to a dynamic interface set that conserves L2 nodes. This parent interface set is based on the underlying physical interface. The name is derived from the predefined variable, $junos-phy-ifd-underlying-intf-set-name by appending “-underlying”. Traffic shaping is determined by a traffic control profile specified in the dynamic client profile.
- Level 3 node—Corresponds to a dynamic interface set that conserves L3 nodes. This child interface set is based on the physical interface and VLAN tag. The set name is derived in one of two ways:
  - If configured, it is provided by the Qos-Set-Name VSA (26–4874–130) in the Access-Accept from the RADIUS server.
  - It is created from the $junos-phy-ifd-interface-set-name predefined variable by appending the SVLAN tag to the value.

  Traffic shaping is determined by the Actual-Data-Rate-Downstream TLV (0x82).
- Level 4 node—Corresponds to the subscriber’s dynamic PPPoE session logical interface or static VLAN logical interface.
- Level 5 node—Corresponds to the scheduling queue for the subscriber.

For shared-media access, residential subscribers:

- Level 1 node—Corresponds to the access-facing physical interface.
- Level 2 node—Corresponds to a dynamic aggregation interface set that conserves L2 nodes. This parent interface set is based on the backhaul identifier from Access-Aggregation-Circuit-Id-ASCII TLV 0x03, which represents the PON tree connection. The name is derived from the predefined-variable, $junos-aggregation-interface-set-name. Traffic shaping is determined by the Actual-Data-Rate-Downstream TLV (0x82) for bonded copper connections and by the PON-Tree-Maximum-Data-Rate-Downstream TLV (0x98) for PON tree connections.

- Level 3 node—Corresponds to a dynamic aggregation interface set that conserves L3 nodes. This child interface set is based on the backhaul identifier from the Access-Aggregation-Circuit-Id-ASCII TLV (0x03), which represents the PON tree connection. The name is derived from the predefined variable, $junos-aggregation-interface-set-name by appending “-default”. Traffic shaping is determined by a traffic control profile specified in the dynamic client profile.

- Level 4 node—Corresponds to the subscriber’s PPPoE session logical interface. Traffic shaping is determined by the Actual-Data-Rate-Downstream TLV (0x82) for bonded copper connections and by the ONT/ONU-Peak-Data-Rate-Downstream TLV (0x94) for PON tree connections.

- Level 5 node—Corresponds to the scheduling queue for the subscriber.

For shared-media access, business subscribers:

- Level 1 node—Corresponds to the access-facing physical interface.

- Level 2 node—Corresponds to a dynamic aggregation interface set that conserves L2 nodes. This parent interface set is based on the backhaul identifier from the Access-Aggregation-Circuit-Id-ASCII TLV (0x03), which represents the PON tree connection. The name is derived from the predefined-variable, $junos-aggregation-interface-set-name. Traffic shaping is determined by the Actual-Data-Rate-Downstream TLV (0x82) for bonded copper connections and by the PON-Tree-Maximum-Data-Rate-Downstream TLV (0x98) for PON tree connections.

- Level 3 node—Corresponds to a dynamic interface set that conserves L3 nodes. This child interface set is based on the physical interface and VLAN tag. The set name is derived in one of two ways:

  - If configured, it is provided by the Qos-Set-Name VSA (26–4874–130) in the Access-Accept from the RADIUS server.

  - It is created from the $junos-phy-ifd-interface-set-name predefined variable by appending the SVLAN tag to the value.

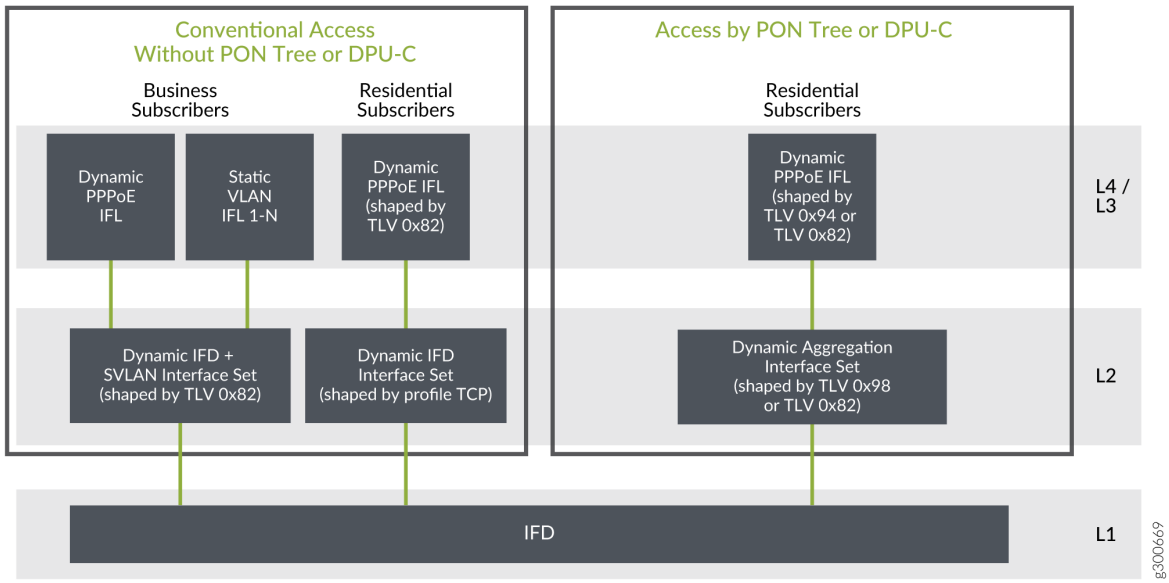
  Traffic shaping is determined by the Actual-Data-Rate-Downstream TLV (0x82) for bonded copper connections and by the ONT/ONU-Peak-Data-Rate-Downstream TLV (0x94) for PON tree connections.

- Level 4 node—Corresponds to the subscriber’s dynamic PPPoE session logical interface or static VLAN logical interface.

- Level 5 node—Corresponds to the scheduling queue for the subscriber.

Figure 10 on page 173 summarizes how CoS shapes key nodes in the four-level scheduler hierarchy. Shaping is based either on the adjusted rates resulting from the DSL and PON TLVs or on traffic control profiles in the dynamic client profile configuration. A CoS adjustment control profile specifies the source of the shaping rate applied to a given node.

Figure 10: Four-Level CoS Node Shaping Summary



The following lists describe the CoS scheduler nodes by access type and subscriber type for the four-level hierarchy in Figure 10 on page 173.

For conventional access, residential subscribers:

- Level 1 node—Corresponds to the access-facing physical interface.
- Level 2 node—Corresponds to a dynamic interface set that conserves Level 2 nodes. This interface set is based on the physical interface. The name is derived from the predefined variable, $junos-phy-ifd-intf-set-name. Traffic shaping is determined by a traffic control profile specified in the dynamic client profile.
- Level 3 node—Corresponds to the subscriber's PPPoE session logical interface. Traffic shaping is determined by the Actual-Data-Rate-Downstream TLV (0x82).
- Level 4 node—Corresponds to the scheduling queue for the subscriber.

For conventional access, business subscribers:

- Level 1 node—Corresponds to the access-facing physical interface.
- Level 2 node—Corresponds to a dynamic interface set that conserves L2 nodes. This interface set is based on the physical interface and VLAN tag. The set name is derived in one of two ways:
  - If configured, it is provided by the Qos-Set-Name VSA (26–4874–130) in the Access-Accept from the RADIUS server.

- It is created from the $junos-phy-ifd-interface-set-name predefined variable by appending the SVLAN tag to the value.

Traffic shaping is determined by the Actual-Data-Rate-Downstream TLV (0x82).

- Level 3 node—Corresponds to the subscriber's dynamic PPPoE session logical interface or static VLAN logical interface.
- Level 4 node—Corresponds to the scheduling queue for the subscriber.

For shared-media access, residential subscribers:

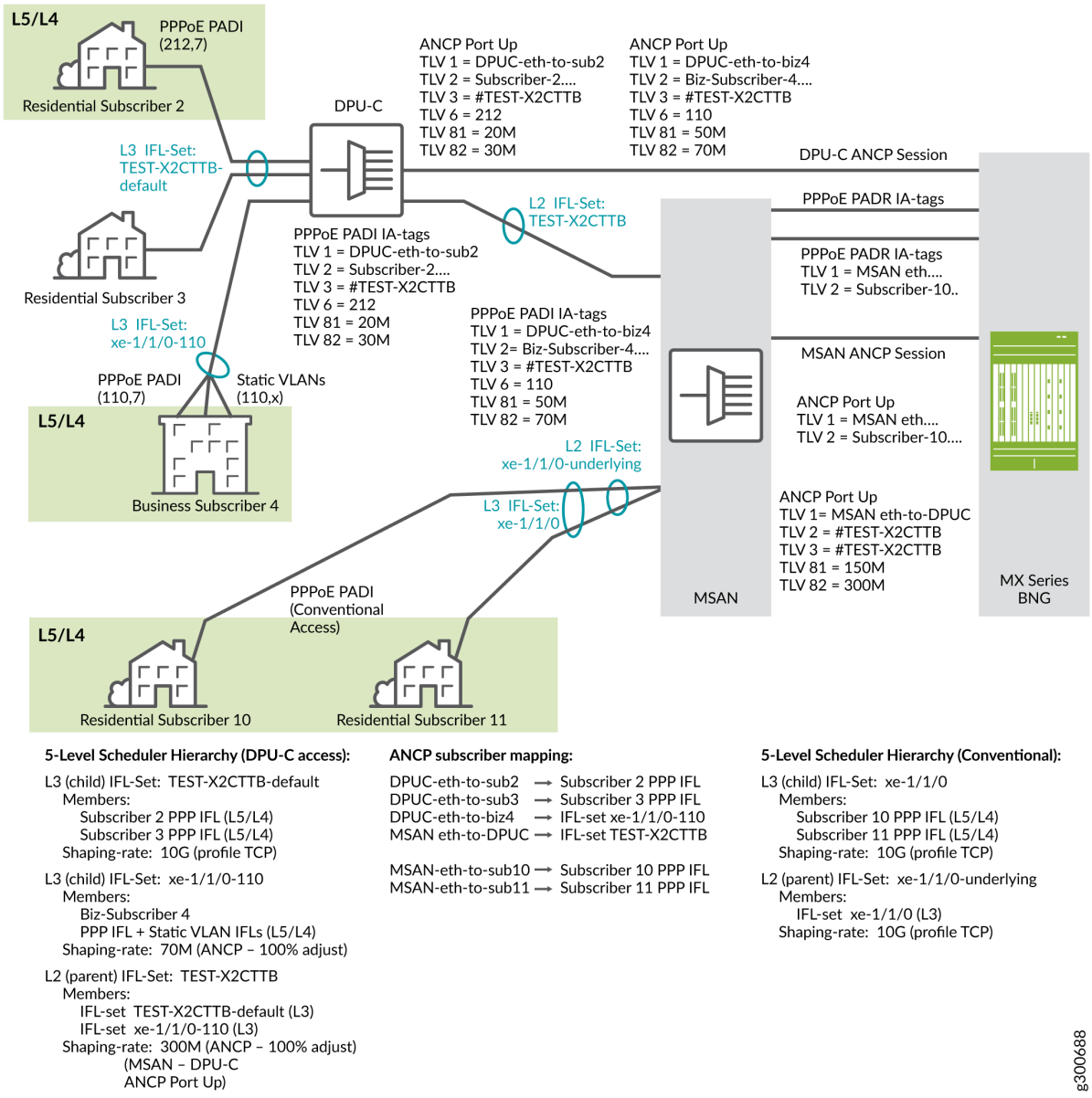
- Level 1 node—Corresponds to the access-facing physical interface.
- Level 2 node—Corresponds to a dynamic aggregation interface set that conserves Level 2 nodes. This interface set is based on the backhaul identifier from the Access-Aggregation-Circuit-Id-ASCII TLV (0x03), which represents the PON tree connection. The name is derived from the predefined-variable, $junos-aggregation-interface-set-name. Traffic shaping is determined by the Actual-Data-Rate-Downstream TLV (0x82) for bonded copper connections and by the PON-Tree-Maximum-Data-Rate-Downstream TLV (0x98) for PON tree connections.
- Level 3 node—Corresponds to the subscriber's PPPoE session logical interface. Traffic shaping is determined by the Actual-Data-Rate-Downstream TLV (0x82) for bonded copper connections and by the ONT/ONU-Peak-Data-Rate-Downstream TLV (0x94) for PON tree connections.
- Level 4 node—Corresponds to the scheduling queue for the subscriber.

Business subscribers are not supported in a four-level, shared-media access network.

CuTTB Use Case Topology and CoS Hierarchy

Figure 11 on page 175 shows a heterogeneous CuTTB topology that includes both shared -media (bonded copper through a DPU-C) and conventional, (nonbonded copper) access for PPPoE subscribers.

Figure 11: CuTTB CoS Hierarchy Example



This topology has the following subscribers:

- Two residential subscribers, 2 and 3, and a business subscriber, 4, have a shared-media access to the network through a DPU-C to the MSAN and then to the BNG.
- Two residential subscribers, 10 and 11, have conventional access to the network through an MSAN to the BNG.
- Residential subscriber 3 is not currently logged in.
- When residential subscriber 2 and business subscriber 4 log in:

1. PPPoE sends a PADI message to the DPU-C that includes the outer VLAN tag for each.

2. The DPU-C sends an ANCP Port Up message to the BNG for each subscriber. ANCP TLVs in the message identify the access line, the subscriber, the ASCII identifier for the access line, the VLAN outer tag as the binary identifier for the access line, the upstream rate, and the downstream rate.

   The ASCII identifier (TLV 0x03) begins with the # character, signifying that the remainder of the value identifies the backhaul (bonded copper, shared media) line. TLV 0x03 is the same for both subscribers, because they connect through the same DPU-C.

3. The DPU-C sends a PADI message for each subscriber to the MSAN. The PADI conveys the PPPoE-IA tags that identify the same attributes as the ANCP TLVs.

4. The MSAN sends a PADR message with the PPPoE tags to the BNG. The MSAN also opens an ANCP session to the BNG by sending an ANCP Port Up message for the MSAN-to-DPU-C connection. The rates in TLVs 0x81 and 0x82 are the values for the MSAN-to-DPU-C line, represented by the L2 interface set. In other words, these are the rates for the bonded copper line itself rather than the subscriber access lines. TLV 0x03 value is also reported in TLV 0x02 to indicate the bonded copper line.

- When residential subscribers 10 and 11 log in:

1. PPPoE sends a PADI message for each subscriber to the MSAN. The PADI conveys the PPPoE-IA tags for the individual subscriber access lines.

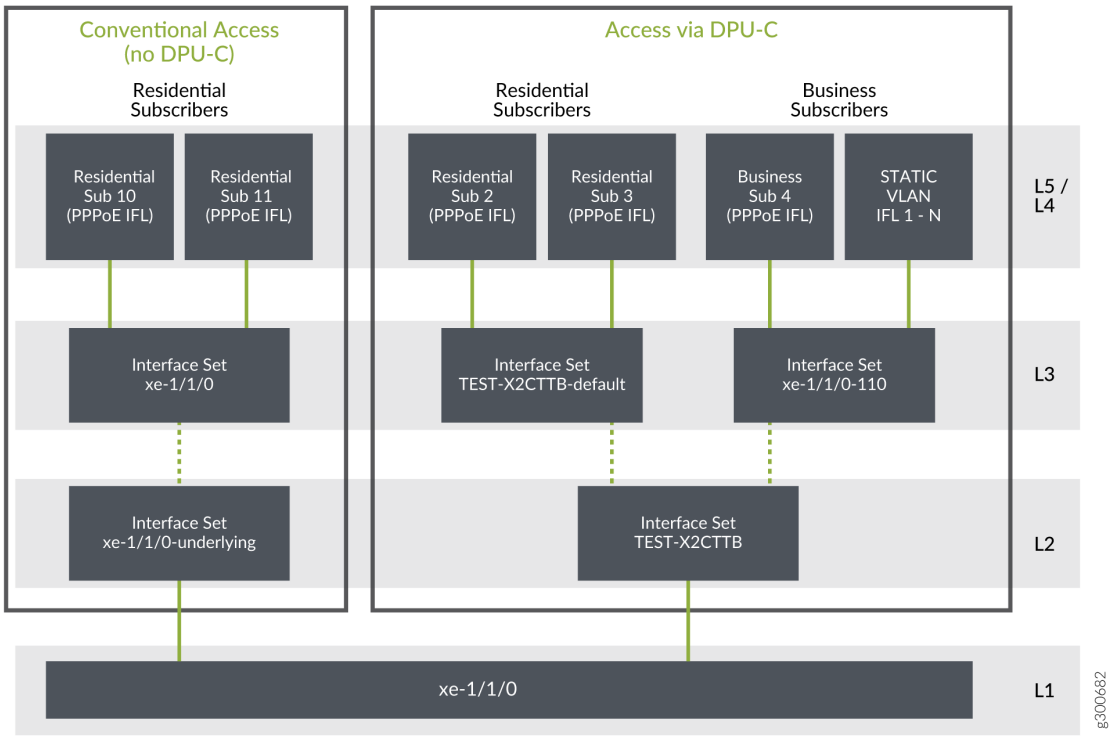
2. The MSAN sends a PADR message with the PPPoE tags for each subscriber line to the BNG.

3. The MSAN also sends an ANCP Port Up message to the BNG for each subscriber. ANCP TLVs in the message identify the access line, the subscriber, the ASCII identifier for the access line, the VLAN outer tag as the binary identifier for the access line, the upstream rate, and the downstream rate.

   Because these subscribers use conventional access rather than shared-media access through the DPU-C, the ASCII identifier (TLV 0x03) does not begin with the # character. In this case, the value is just the ASCII equivalent of the binary value conveyed in TLV 0x06.

Figure 12 on page 177 shows the five-level CoS hierarchy that corresponds to the CuTTB topology in Figure 11 on page 175.

Figure 12: CoS Hierarchy for CuTTB Topology



The following stanzas are part of the use case configuration that creates the Level 2 and Level 3 interface sets. The `stacked-interface-set` statement sets the Level 2 interface set to the $junos-aggregation-interface-set-name predefined variable. The stanza also specifies the Level 3 interface set as $junos-interface-set-name. It establishes the Level 2 set as the parent of the Level 3 set.

```
dynamic-profiles test-prof
    interfaces {
        stacked-interface-set {
            interface-set "$junos-aggregation-interface-set-name" {
                interface-set $junos-interface-set-name;
            }
        }
    }
}
```

The predefined-variable-defaults stanza uses variable expressions that set conditions to establish the names of the Level 2 and Level 3 interface sets. The default values are used only when RADIUS does not supply values for $junos-aggregation-interface-set-name and $junos-interface-set-name.

```
dynamic-profiles test-prof
    predefined-variable-defaults {
        aggregation-interface-set-name equals "$junos-phy-ifd-underlying-intf-set-name";
        interface-set-name equals "ifZero($junos-default-interface-set-name, $junos-phy-ifd-
interface-set-name)";
        default-interface-set-name equals "ifZero($junos-interface-set-name, ifNotZero($junos-
aggregation-interface-set-name, $junos-aggregation-interface-set-name##'-default'))";
    }
}
```

The following list describes the hierarchical CoS scheduler nodes for the CuTTB topology. It explains how the names of the interface sets are derived from predefined variables.

- Level 1 corresponds to the access-facing physical interface for all subscribers, xe-1/1/0.
- Level 2 corresponds to a parent interface set that has child interface sets as its members. The name of the interface set is supplied by the $junos-aggregation-interface-set-name predefined variable in the dynamic profile.
  - TEST-X2CTTB is the Level 2 interface set for all shared-media access subscribers. Its members are the Level 3 interface sets for residential subscribers 2 and 3 and for business subscriber 4.

    TLV 0x03 includes the # character, which identifies the line as shared. $junos-aggregation-interface-set-name takes the value of TLV 0x03.
  - xe-1/1/0-underlying is the Level 2 interface set for conventional access. Its member is the Level 3 interface set for residential subscribers 10 and 11.

    TLV 0x03 does not include the # character and so does not identify a shared line. $junos-aggregation-interface-set-name is dynamically taken from $junos-phy-ifd-underlying-intf-set-name. The value of $junos-phy-ifd-underlying-intf-set-name is simply the physical interface name with a suffix of “-underlying”.
- Level 3 corresponds to a child interface set that has subscriber logical interfaces as its members. The name of the interface set is supplied by the $junos-interface-set-name predefined variable in the dynamic profile.
  - TEST-X2CTTB-default is the Level 3 interface set for residential subscribers 2 and 3. These subscribers were identified as residential because the RADIUS server did not return VSA 26-4874-130, QoS-Set-Name. TLV 0x03 includes the # character, which identifies the line as

shared. $junos-interface-set-name is set to the value of $junos-aggregation-interface-set-name with a suffix of “default”.

- xe-1/1/0-110 is the Level 3 interface set for business subscriber 4. This subscriber was identified as business because the RADIUS server returned VSA 26-4874-130. TLV 0x03 includes the # character, which identifies the line as shared. $junos-interface-set-name is set to the value of VSA 26-4874-130. The VSA value is a concatenation of the physical interface name ($junos-phy-ifd-intf-set-name) and the outer VLAN tag.

- xe-1/1/0 is the Level 3 interface set for residential subscribers 10 and 11, which use conventional access. These subscribers were identified as residential because the RADIUS server did not return VSA 26-4874-130. $junos-interface-set-name is set to the value of $junos-phy-ifd-intf-set-name.

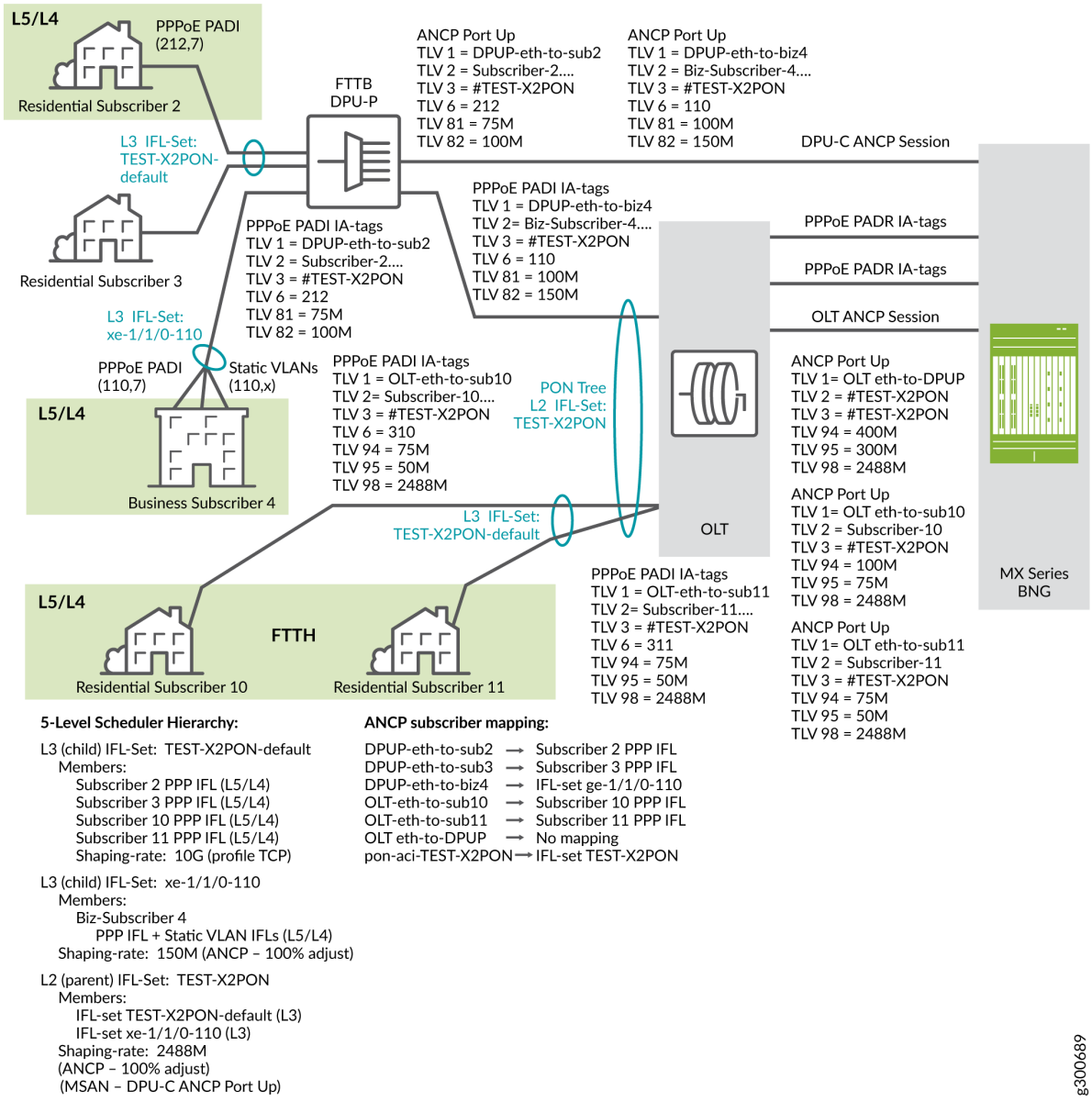
- Level 4 corresponds to the logical interface for individual subscribers. This includes PPPoE logical interfaces for residential and business subscribers, as well as static VLAN logical interfaces for business subscribers.

- Level 5 corresponds to the scheduling queue for each subscriber, regardless of subscriber type or access type. One or more queues are present per subscriber to provide subscriber services.

FTTB/FTTH Use Case Topology and CoS Hierarchy

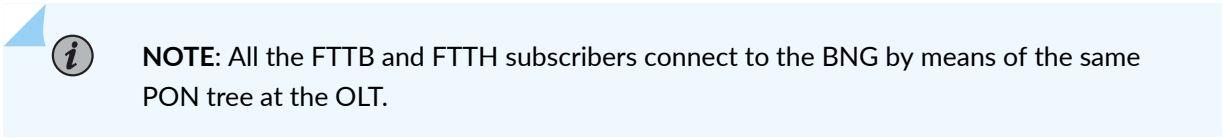
Figure 13 on page 180 shows a heterogeneous FTTB/FTTH topology that includes both shared -media (PON through a DPU-P) and conventional, (directly connected) access for PPPoE subscribers.

Figure 13: FTTB/FTTH CoS Hierarchy Example



This topology has the following subscribers:

- Two residential subscribers, 2 and 3, and a business subscriber, 4, have a shared-media access to the network through a DPU-P to the OLT and then to the BNG. These are FTTB subscribers.
- Two residential subscribers, 10 and 11, have conventional access to the network through the same OLT to the BNG. These are FTTH subscribers.

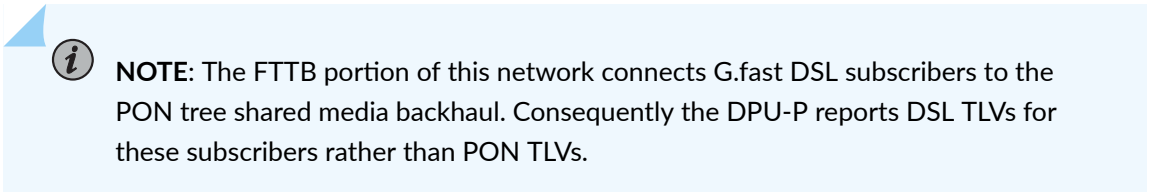


NOTE: All the FTTB and FTTH subscribers connect to the BNG by means of the same PON tree at the OLT.

- Residential subscriber 3 is not currently logged in.
- When residential subscriber 2 and business subscriber 4 log in:

  1. PPPoE sends a PADI message to the DPU-P that includes the outer VLAN tag for each.
  2. The DPU-P sends an ANCP Port Up message to the BNG for each subscriber. ANCP TLVs in the message identify the access line, the subscriber, the ASCII identifier for the access line, the VLAN outer tag as the binary identifier for the access line, the upstream rate, and the downstream rate.

     The ASCII identifier (TLV 0x03) begins with the # character, signifying that the remainder of the value identifies the backhaul (PON tree) line. TLV 0x03 is the same for both subscribers, because they connect through the same PON tree.
  3. The DPU-P sends a PADI message for each subscriber to the OLT. The PADI conveys the PPPoE-IA tags that identify the same attributes as the ANCP TLVs.
  4. The OLT sends a PADR message with the PPPoE tags to the BNG. The OLT also opens an ANCP session to the BNG by sending an ANCP Port Up message for the OLT-to-DPU-P connection. The rates in TLVs 0x81 and 0x82 are the values for the OLT-to-DPU-P line, represented by the L2 interface set. In other words, these are the rates for the PON tree itself rather than the subscriber access lines. Although this use case example shows that TLV 0x03 value is also reported in TLV 0x02 to indicate the PON tree line, this is not a requirement for PON networks.

     NOTE: The FTTB portion of this network connects G.fast DSL subscribers to the PON tree shared media backhaul. Consequently the DPU-P reports DSL TLVs for these subscribers rather than PON TLVs.

- When residential subscribers 10 and 11 log in:

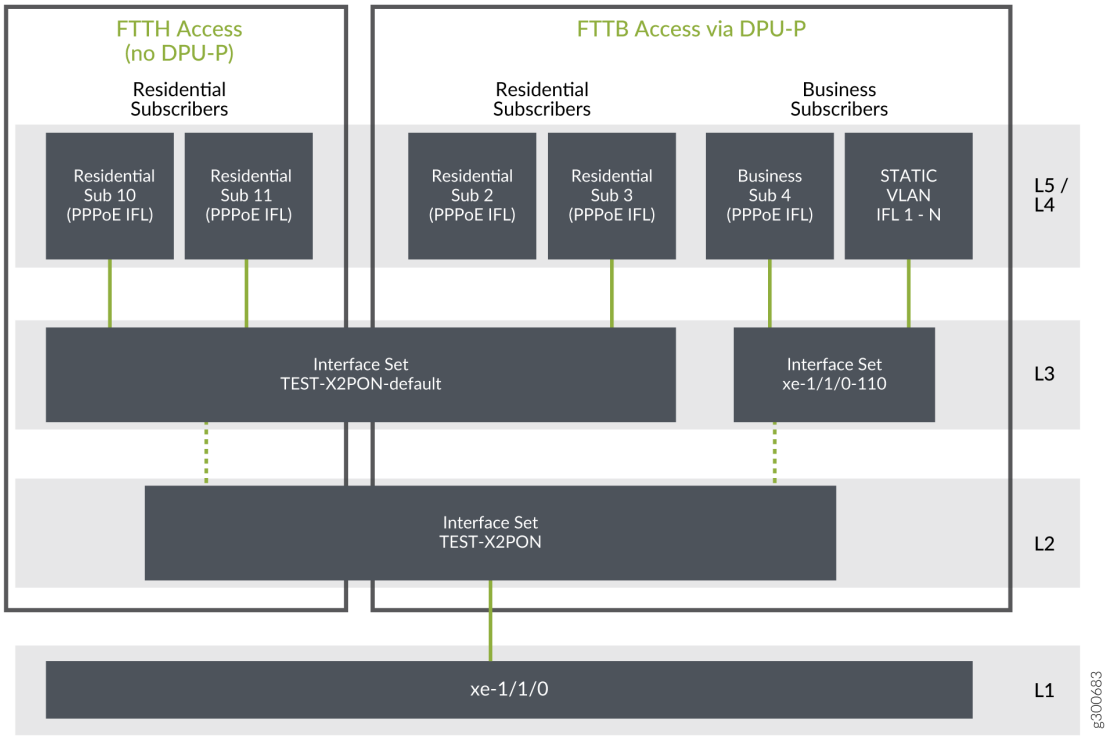
  1. PPPoE sends a PADI message for each subscriber to the OLT. The PADI conveys the PPPoE-IA tags for the individual subscriber access lines.
  2. The OLT sends a PADR message with the PPPoE tags for each subscriber line to the BNG.
  3. The OLT also sends an ANCP Port Up message to the BNG for each subscriber. ANCP TLVs in the message identify the access line, the subscriber, the ASCII identifier for the access line, the VLAN outer tag as the binary identifier for the access line, the upstream rate, and the downstream rate.

The ASCII identifier (TLV 0x03) begins with the # character, signifying that the remainder of the value identifies the backhaul (fiber PON tree, shared media) line. TLV 0x03 is the same for both subscribers, because they connect through the same DPU-P.

Because subscribers 10 and 11 connect to the same PON tree as the FTTB subscribers, the ASCII identifier (TLV 0x03) also begins with the # character, signifying that the remainder of the value identifies the backhaul (fiber PON tree, shared media) line. TLV 0x03 is the same for both subscribers.

Figure 14 on page 182 shows the five-level CoS hierarchy that corresponds to the FTTB/FTTH topology in Figure 13 on page 180.

Figure 14: CoS Hierarchy for FTTB/FTTH Topology



The following stanzas are part of the use case configuration that creates the Level 2 and Level 3 interface sets. The `stacked-interface-set` statement sets the Level 2 interface set to the $junos-aggregation-interface-set-name predefined variable. The stanza also specifies the Level 3 interface set as $junos-interface-set-name. It establishes the Level 2 set as the parent of the Level 3 set.

```
dynamic-profiles test-prof
    interfaces {
```

```
        stacked-interface-set {
            interface-set "$junos-aggregation-interface-set-name" {
                interface-set $junos-interface-set-name;
            }
        }
    }
}
```

The predefined-variable-defaults stanza uses variable expressions that set conditions to establish the names of the Level 2 and Level 3 interface sets. The default values are used only when RADIUS does not supply values for $junos-aggregation-interface-set-name and $junos-interface-set-name.

```
dynamic-profiles test-prof
    predefined-variable-defaults {
        aggregation-interface-set-name equals "$junos-phy-ifd-underlying-intf-set-name";
        interface-set-name equals "ifZero($junos-default-interface-set-name, $junos-phy-ifd-
interface-set-name)";
        default-interface-set-name equals "ifZero($junos-interface-set-name, ifNotZero($junos-
aggregation-interface-set-name, $junos-aggregation-interface-set-name##'-default'))";
    }
}
```

The following list describes the hierarchical CoS scheduler nodes for the FTTB/FTTH topology. It explains how the names of the interface sets are derived from predefined variables.

- Level 1 corresponds to the access-facing physical interface for all subscribers, xe-1/1/0.
- Level 2 corresponds to a parent interface set that has child interface sets as its members. The name of the interface set is supplied by the $junos-aggregation-interface-set-name predefined variable in the dynamic profile.

  TEST-X2PON is the Level 2 interface set for all PON subscribers, both conventional access and DPU-P access. Its members are the Level 3 interface set for the FTTB/FTTH residential subscribers and the Level 3 interface set for business subscriber 4. TLV 0x03 includes the # character, which identifies the PON tree line as the backhaul. $junos-aggregation-interface-set-name takes the value of TLV 0x03.
- Level 3 corresponds to an interface set that has subscriber logical interfaces as its members.
  - TEST-X2PON-default is the Level 3 interface set for FTTB residential subscribers 2 and 3, as well as FTTH residential subscribers 10 and 11. These subscribers all use the same PON tree and therefore are included in the same interface set.

These subscribers were identified as residential because the RADIUS server did not return VSA 26-4874-130, QoS-Set-Name. TLV 0x03 includes the # character, which identifies the PON tree line as the backhaul. $junos-interface-set-name is set to the value of $junos-aggregation-interface-set-name with a suffix of “default”.

- xe-1/1/0-110 is the Level 3 interface set for business subscriber 4, which uses shared-media access.

  This subscriber was identified as business because the RADIUS server returned VSA 26-4874-130. TLV 0x03 includes the # character, which identifies the PON tree line as the backhaul. $junos-interface-set-name is set to the value of VSA 26-4874-130. The VSA value is a concatenation of the physical interface name ($junos-phy-ifd-intf-set-name) and the outer VLAN tag.

- Level 4 corresponds to the logical interface for individual subscribers. This includes PPPoE logical interfaces for residential and business subscribers, as well as static VLAN logical interfaces for business subscribers.

- Level 5 corresponds to the scheduling queue for each subscriber, regardless of subscriber type or access type. One or more queues are present per subscriber to provide subscriber services.

Automatic Creation of Business Subscriber Interface Sets

For business subscribers in an access network, four-level scheduler hierarchies use static interface sets to represent the subscriber access line. The members of the interface set are static VLAN logical interfaces. This configuration is performed by Extensible Subscriber Services Manager (ESSM) operation scripts (op-scripts).

The op-scripts base the name on the outer VLAN tag of the subscriber interface, because the tag is unique per subscriber. The interface set name is in the format *physical_interface_name-outer_vlan_tag*. For example, an Ethernet interface ge-1/1/0, with a dual-tagged VLAN interface that has an outer tag of 111, results in an interface set name of ge-1/1/0-111. This format is the same as that used by the $junos-svlan-interface-set-name predefined variable.

In five-level scheduler hierarchies for business subscribers, each business session includes a dynamic PPPoE control session (and thus a dynamic PPPoE logical interface) and two or more static business VLAN logical interfaces. These interfaces need to be shaped as an aggregate in an interface set. The dynamic logical interfaces cannot be assigned to a static interface set. This means that this deployment design requires dynamic interface sets for logical intermediate (Level 3) CoS nodes to accommodate both the dynamic PPPoE logical interfaces and the static interfaces.

BEST PRACTICE: We recommend that you use dynamic interface sets to provide a uniform solution for both four-level and five-level hierarchies. This method ensures that all the logical interfaces, both dynamic and static, are members of the same interface set.

> This is not a requirement. You can continue to configure only static interface sets for business subscribers in four-level hierarchies.

The op-scripts need to reference the business subscriber dynamic interface set name during subscriber configuration. This means that the format of the dynamic interface set name must be the same format that the script uses for static interface sets. The interface set name is provided by the RADIUS server during subscriber authentication, because the server has to determine whether the subscriber logging in is a business subscriber or a residential subscriber. This means that you have to configure your RADIUS software to specify the interface set for each subscriber. This requirement adds initial and maintenance configuration overhead to your operations, especially as your networks scales to higher numbers of subscribers.

Starting in Junos OS Release 19.3R1, you can configure the BNG to dynamically create the interface set name and propose that name to the RADIUS server in the Access-Request message for the subscriber. This method reduces the complexity of the RADIUS configuration, because you avoid having to configure your RADIUS software to specify interface sets for each subscriber. To enable dynamic creation of the interface set name for business subscribers, use the `source-interface-set-at-login svlan` statement at the `[edit protocols ppp-service]` hierarchy level.

The interface set name that the BNG proposes is carried by the Juniper Networks VSA, Qos-Set-Name (26-130) in the RADIUS Access-Request message. The set name consists of the name of access-facing physical interface appended with the VLAN tag. This is the same format that is used by the op scripts:

- The outer vlan tag is used for a dual-tagged VLAN. For a business subscriber on xe-1/1/0 with VLAN tags (110,7), the name has this format:

  xe-1/1/0-110

- The lone vlan tag is used for a single-tagged VLAN. The single-tagged VLAN is used when the CPE device connects directly to the access node. For a business subscriber on xe-2/2/1 with VLAN tag (33), the name has this format:

  xe-2/2/1-33

When the subscriber logs in, the RADIUS server evaluates the Access-Request and determines whether the subscriber is business or residential:

- When the RADIUS server determines that the subscriber is a business subscriber, it returns the VSA with the name in the Access-Accept message to the BNG, where the name is used to create a dynamic interface set for the business subscriber.

- If the RADIUS server determines during authentication that the subscriber is residential, then the server does not return the VSA in the Access-Accept message. In this case, the dynamic PPPoE IFL is added to a default dynamic interface set to conserve L3 CoS nodes for a five-level hierarchy or L2 CoS nodes for a four-level hierarchy. The dynamic interface set for residential subscribers always

resolves to the default interface set. The default dynamic interface set is determined by how you configure the `predefined-variable-defaults` statement with expressions in the dynamic profile. See Dynamic Level 2 and Level 3 Interface Set Naming with Predefined Variables for information about configured the defaults.

How to Configure the Automatic Creation of Business Subscriber Interface Sets

In heterogeneous access networks, you can reduce some of the complexity of your RADIUS configuration by having PPP on the BNG dynamically create the interface set name for business subscribers and propose that name to the RADIUS server in the Access-Request message for the subscriber. This method reduces complexity because you do not have to configure all the possible interface set names on the RADIUS server. The proposed name is carried by the Qos-Set-Name VSA (26-4874–130).

If the server determines that the subscriber is a business subscriber, it returns the name in the Access-Accept message to the BNG. PPP on the BNG then uses the name to create a dynamic interface set for the business subscriber. This interface set is for an intermediate CoS node; for example, Level 3 in a five-level hierarchy. This interface set includes the business subscriber PPPoE IFL and the static VLAN IFLs created by ESSMD op-scripts. It is the child interface set of the Level 2 parent interface set.

For information about how the interface set names are formed, see Automatic Creation of Business Subscriber Interface Sets.

If the RADIUS server determines that the subscriber is residential, then the server does not return the VSA in the Access-Accept message. In this case, the dynamic PPPoE IFL is added to a default dynamic interface set.

To configure dynamic creation of business subscriber interface sets with the same format as $junos-svlan-interface-set-name:

- Enable PPP to dynamic creation.

```
[edit protocols ppp-service]
user@host# set source-interface-set-at-loginsvlan
```

Dynamic Level 2 and Level 3 Interface Set Naming with Predefined Variables

IN THIS SECTION

- Predefined Variable Default for the Level 2 Node Interface Set | **188**
- Predefined Variable Default for the Level 3 Node Interface Set | **189**

In heterogeneous access networks, Juniper Networks predefined variables supply the names of the interface sets for the Level 2 and Level 3 CoS nodes:

- Level 2—$junos-aggregation-interface-set-name
- Level 3—$junos-interface-set-name

You specify these variables in the dynamic client profile at the `[edit dynamic-profiles profile-name interfaces]` hierarchy level as follows:

```
stacked-interface-set {
    interface-set "$junos-aggregation-interface-set-name" {
        interface-set “$junos-interface-set-name”;
    }
}
```

These interfaces are said to be stacked. Level 2 is the parent interface set and Level 3 is the child interface set.

You can optionally configure default values for the predefined variables. The default value must be appropriate to the variable, such as an integer or an alphanumeric string. The Junos OS uses the default value when the variable is not resolved, meaning that it does not have a value. The predefined variable might not be resolved for several reasons, depending on the access type (conventional or shared-media) and the subscriber type (residential or business), such as the following:

- The Access-Aggregation-Circuit-Id-ASCII TLV (0x03) is not present or does not include the # character that indicates it carries the backhaul identifier).
- The external RADIUS server does not return the QoS-Set-Name VSA (26-4874-130).

Starting in Junos OS Release 19.3R1, you can configure the default value of a predefined variable to be another predefined variable by using a variable expression. In earlier releases, the default value must be fixed; it cannot be a variable.

NOTE: Expressions are typically configured for user-defined variables and dynamic service profiles. See *Using Variable Expressions in User-Defined Variables* for more information.

When you use a variable expression, you are setting up a condition that determines the default value of the predefined variable. The value of the default is different when the condition is matched than when it is not matched. This capability enables you to configure a single dynamic client profile for a heterogeneous network. The profile can instantiate the proper interface sets for business subscribers and residential subscribers on both conventional access lines and shared-media access lines.

In dynamic client profiles, you can configure variable expressions that use any of the following:

- `equals`—Assigns a predefined variable or expression as the default value.
- `ifNotZero(`*`parameter-1`*`, `*`parameter-2`*`)`—Sets a condition to be matched. Assigns the value from *parameter-2* as the default value only when *parameter-1* is nonzero, meaning that the parameter resolved to some value.
- `ifZero(`*`parameter-1`*`, `*`parameter-2`*`)`—Sets a condition to be matched. Assigns the value from *parameter-2* as the default value only when *parameter-1* is zero, meaning that the parameter did not resolve to any value. If *parameter-1* did resolve to a value (therefore it is not zero), then the value from *parameter-1* is assigned as the default.

You can also nest expressions, which provides additional conditions for setting the variable value. For a heterogeneous network, you use the following expressions to determine the name for the Level 2 and Level 3 CoS nodes:

```
dynamic-profiles name {
    predefined-variable-defaults {
        interface-set-name equals "ifZero($junos-default-interface-set-name, $junos-phy-ifd-
interface-set-name)";
        default-interface-set-name equals "ifZero($junos-interface-set-name, ifNotZero($junos-
aggregation-interface-set-name, $junos-aggregation-interface-set-name##'-default'))";
    }
}
```

The following sections explain how to evaluate each of these expressions.

Predefined Variable Default for the Level 2 Node Interface Set

The following definition simply assigns a predefined variable as the default value for $junos-aggregation-interface-set-name:

```
aggregation-interface-set-name equals “$junos-phy-ifd-underlying-intf-set-name”
```

The expression has no conditions to evaluate. The $junos-phy-ifd-underlying-intf-set-name predefined variable has the format *physical-interface-name*-underlying. For example, if the physical interface is xe-1/1/0, then $junos-phy-ifd-underlying-intf-set-name resolves to xe-1/1/0-underlying. That becomes the default value for $junos-aggregation-interface-set-name:

$junos-aggregation-interface-set-name = $junos-phy-ifd-underlying-intf-set-name = xe-1/1/0-underlying

The default value is not used when $junos-aggregation-interface-set-name is already resolved. If the Access-Aggregation-Circuit-ID-ASCII attribute (TLV 0x03) begins with a # character (the backhaul identifier), then the variable takes the value of the remainder of the string after the # character. It is therefore resolved and the default is not used.

The following table shows the value of $junos-aggregation-interface-set-name when TLV 0x03 identifies the backhaul node and when it is not present. The physical interface is xe-1/1/0.

TLV 0x03 (Access Type)	$junos-aggregation-interface-set-name
#TEST-X2PON (DPU-C/DPU-P)	TEST-X2PON
Not present in PPPoE-IA tags (Conventional)	xe-1/1/0-underlying

Predefined Variable Default for the Level 3 Node Interface Set

You have to use multiple expressions to provide a default value for $junos-interface-set-name:

```
interface-set-name equals "ifZero($junos-default-interface-set-name, $junos-phy-ifd-interface-
set-name)";
default-interface-set-name equals "ifZero($junos-interface-set-name, ifNotZero($junos-
aggregation-interface-set-name, $junos-aggregation-interface-set-name##'-default'))";
```

1. The first expression means that it has to check whether $junos-default-interface-set-name is resolved.

   ```
   interface-set-name equals "ifZero($junos-default-interface-set-name, $junos-phy-ifd-interface-
   set-name)";
   ```

   - If it is not resolved, then the default value for $junos-interface-set-name is set to the value of $junos-phy-ifd-interface-set-name:

     $junos-interface-set-name = $junos-phy-ifd-interface-set-name

- If it is resolved, then the default value for $junos-interface-set-name is set to the resolved value of $junos-default-interface-set-name:

  $junos-interface-set-name = $junos-default-interface-set-name

2. The value of $junos-default-interface-set-name is determined by a nested expression.

```
default-interface-set-name equals "ifZero($junos-interface-set-name, ifNotZero($junos-
aggregation-interface-set-name, $junos-aggregation-interface-set-name##'-default'))";
```

   a. If $junos-interface-set-name is not resolved, then $junos-interface-set-name is set to the result of the nested expression (ifNotZero). However, the predefined variable defaults are used only if $junos-interface-set-name is not resolved. Consequently, the expression must reduce to this:

```
default-interface-set-name equals “ifNotZero($junos-aggregation-interface-set-name, $junos-
aggregation-interface-set-name##'-default')"
```

   b. The ifNotZero expression is solved by evaluating whether $junos-aggregation-interface-set-name is resolved. $junos-aggregation-interface-set-name is resolved only when TLV 0x03 includes the backhaul identifier (#).

      - If $junos-aggregation-interface-set-name is resolved, then `-default` is appended to that name and that becomes the default value for $junos-default-interface-set-name:

        $junos-default-interface-set-name = $junos-aggregation-interface-set-name+ “-default”

      - If $junos-aggregation-interface-set-name is not resolved, then $junos-default-interface-set-name is also not resolved.

3. Now the value for $junos-interface-set-name can be determined:

```
interface-set-name equals "ifZero($junos-default-interface-set-name, $junos-phy-ifd-interface-
set-name)";
```

   - If $junos-default-interface-set-name is resolved, then that is also the value of $junos-interface-set:

     $junos-interface-set-name = $junos-default-interface-set-name = $junos-aggregation-interface-set-name+ “-default”

   - If $junos-default-interface-set-name is not resolved, then:

     $junos-interface-set-name = $junos-phy-ifd-interface-set-name

The following table shows the possible values of the predefined variables based on the expressions described above. It can be helpful to refer to the figures and text in CoS Node Shaping in Four-Level and Five-Level Heterogeneous Networks, CuTTB Use Case Topology and CoS Hierarchy, and FTTB/FTTH Use Case Topology and CoS Hierarchy.

TLV 0x03 (Access Type)	VSA 26–4874–130 (Subscriber Type)	$junos-phy-ifd-interface-set-name	$junos-default-interface-set-name	$junos-interface-set-name
#TEST-X2PON (DPU-C/DPU-P)	Not returned (Residential)	xe-1/1/0	Not resolved	TEST-X2PON-default
#TEST-X2PON (DPU-C/DPU-P)	Returned as xe-1/1/0 (Business)	xe-1/1/0	xe-1/1/0	xe-1/1/0-110
Not present in PPPoE-IA tags (Conventional)	Not returned (Residential)	xe-1/1/0	Not resolved	xe-1/1/0
Not present in PPPoE-IA tags (Conventional)	Returned as xe-1/1/0 (Business)	xe-1/1/0	xe-1/1/0	xe-1/1/0-110

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
19.3R1	Starting in Junos OS Release 19.3R1, you can configure the BNG to dynamically create the interface set name and propose that name to the RADIUS server in the Access-Request message for the subscriber.
19.3R1	Starting in Junos OS Release 19.3R1, you can configure the default value of a predefined variable to be another predefined variable by using a variable expression.

RELATED DOCUMENTATION

ANCP Agent and AAA

ANCP Agent Traffic Shaping and CoS

DSL Forum Vendor-Specific Attributes

OLT Migration to Using PON TLVs Instead of DSL TLVs | **192**

CoS for Subscriber Access Overview

Hierarchical Class of Service for Subscriber Management Overview

Predefined Variables in Dynamic Profiles

OLT Migration to Using PON TLVs Instead of DSL TLVs

IN THIS SECTION

- Support for OLT Migration to PON TLVs | **192**
- How to Configure Preference for DSL or PON TLVs When an OLT Sends Both | **193**

Support for OLT Migration to PON TLVs

Before the introduction of PON-specific TLVs (see the Internet draft, *Access Extensions for the Access Node Control Protocol*), OLTs passed information about PON access line rates in the ANCP DSL TLVs. The DSL TLVs are *overloaded* with the PON data. In this situation, the access line type is classified as OTHER in the DSL-Type TLV (0x91). The raw PON line rates are conveyed in the Actual-Net-Data-Rate-Upstream TLV (0x81) and the Actual-Net-Data-Rate-Downstream TLV (0x82). For example, this is the behavior used for FTTH networks.

With the availability of the PON TLVs, OLTs provide PON access line information in one of the following ways:

- Only in DSL TLVs—OLTs that do not support the PON TLVs continue to send PON rates in DSL TLVs. This is the same situation as before the introduction of PON TLVs.
- Only in PON TLVs—OLTs that support the PON TLVs might use them exclusively to convey attributes for the subscriber access line and PON tree.
- In both DSL and PON TLVs—OLTs that support the PON TLVs might send them and also, redundantly, overload the DSL TLVs with the PON rates. This behavior enables the OLT to successfully provide rate information both to BNGs that support PON TLVs and BNGs that do not. The OLT is expected to provide both types of TLVs in both the ANCP port status messages and the PPPoE-IA tags.

The following expectations apply to OLTs that provide both DSL TLVs and PON TLVs:

- The OLT uses both types of TLVs for both ANCP port status messages and PPPoE-IA tags.
- The ANCP line attribute TLVs carry only the TLVs that match that line:
  - The DSL-Line-Attributes TLV (0x04) carries only DSL TLVs, including G.fast TLVs.
  - The PON-Access-Line-Attributes TLV (0x12) carries only PON TLVs.
  - The Access-Loop Encapsulation TLV (0x90) is independent of the transport method. The ANCP agent accepts and saves 0x90 when it is present in either the PON-Access-Line-Attributes TLV (0x12) or in PPPoE-IA tags.
- The access-line identification attributes are common to both DSL and PON access lines and convey the same information. This set of attributes consists of the following:
  - Access-Loop-Circuit-ID (0x01)
  - Access-Loop-Remote-ID (0x02)
  - Access-Aggregation-Circuit-ID-ASCII(0x03)
  - Access-Aggregation-Circuit-ID-Binary (0x04)

When the OLT sends both types of TLVs, the router accepts, saves, and process only one type or the other, according to a preference setting. The router saves or discards the corresponding line attribute that carries the TLVs for that line type. By default, the router prefers the PON TLVs over the DSL TLVs. This means that the router accepts the PON-Line-Attributes TLV (0x12) and discards the DSL-Line-Attributes-TLV (0x04).

You can change the preference with the `preference (dsl | pon)` option at the `[edit system access-line attributes]` hierarchy level. For example, when the PON TLVs are unreliable, perhaps because of an OLT issue, you might configure the router prefer the DSL TLVs for improved reliability.

How to Configure Preference for DSL or PON TLVs When an OLT Sends Both

You can configure which set of TLVs is saved and processed when the OLT sends both DSL TLVs and PON TLVs in ANCP port status messages or in PPPoE-IA tags. The TLVs that you do not select are discarded. OLTs provide PON access line information in one of the following ways:

- Only in DSL TLVs—OLTs that do not support the PON TLVs continue to use the method available before PON TLVs were available. These OLTs send PON rates in DSL TLVs, overloading the DSL TLVs with the PON information. In this case, the DSL-Type TLV (0x91) is set to OTHER and PON rates for the subscriber access line are presented in the Actual-Net-Data-Rate-Upstream TLV (0x81) and the Actual-Net-Data-Rate-Downstream TLV (0x82).
- Only in PON TLVs—OLTs that support the PON TLVs might use them exclusively to convey attributes for the subscriber access line and PON tree.

- In both DSL and PON TLVs—OLTs that support the PON TLVs might send them and also, redundantly, overload the DSL TLVs with the PON rates. This behavior enables the OLT to successfully provide rate information both to BNGs that support PON TLVs and BNGs that do not. The OLT is expected to provide both types of TLVs in both the ANCP port status messages and the PPPoE-IA tags.

> **NOTE**: The default preference on the router is to accept and process PON TLVs when both are received. This means that you typically use the `preference` option to prioritize DSL TLVs over PON TLVs. For example, if the PON TLVs are unreliable, perhaps because of an OLT issue, you can prioritize the DSL TLVs for reliability.

To select the type of access line TLVs to accept:

- Configure the preference.

```
[edit system access-line]
user@host# set preference (dsl | pon)
```

RELATED DOCUMENTATION

DSL Forum Vendor-Specific Attributes

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

Five-Level and Four-Level Heterogeneous Networks | 169

PART 5

Configuration Statements and Operational Commands

- dynamic-profile (DHCP Local Server) | **196**
- Junos CLI Reference Overview | **198**

dynamic-profile (DHCP Local Server)

IN THIS SECTION

- Syntax | 196
- Hierarchy Level | 196
- Description | 197
- Options | 197
- Required Privilege Level | 197
- Release Information | 197

Syntax

```
dynamic-profile profile-name {
    aggregate-clients (merge | replace);
    use-primary primary-profile-name;
}
```

Hierarchy Level

```
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name],
[edit system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server dhcpv6 group group-name],
[edit system services dhcp-local-server dhcpv6 group group-name interface interface-name],
[edit system services dhcp-local-server group group-name],
[edit system services dhcp-local-server group group-name interface interface-name],
[edit logical-systems logical-system-name system services dhcp-local-server ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server ...],
[edit routing-instances routing-instance-name system services dhcp-local-server ...]
```

Description

Specify the dynamic profile that is attached to all interfaces, a named group of interfaces, or a specific interface.

Options

profile-name—Name of the dynamic profile.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.2.

Options `aggregate-clients` and `use-primary` introduced in Junos OS Release 9.3.

Support at the `[edit ... interface]` hierarchy levels introduced in Junos OS Release 11.2.

RELATED DOCUMENTATION

> *Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*
>
> *Configuring a Default Subscriber Service*

Junos CLI Reference Overview

We've consolidated all Junos CLI commands and configuration statements in one place. Read this guide to learn about the syntax and options that make up the statements and commands. Also understand the contexts in which you'll use these CLI elements in your network configurations and operations.

- Junos CLI Reference

Click the links to access Junos OS and Junos OS Evolved configuration statement and command summary topics.

- Configuration Statements
- Operational Commands