JUNIPER NETWORKS

Junos® OS

Layer 2 Wholesale for Subscriber Services Feature Guide

Release
13.2

Published: 2013-07-31

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

Junos® OS Layer 2 Wholesale for Subscriber Services Feature Guide
13.2

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

List of Figures

List of Tables

About the Documentation

Documentation and Release Notes

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

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

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

Supported Platforms

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

- MX Series

Using the Examples in This Manual

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

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

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

Merging a Full Example

To merge a full example, follow these steps:

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

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

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

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

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

Merging a Snippet

To merge a snippet, follow these steps:

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

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

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

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

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

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

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

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

Documentation Conventions

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

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the**configure** command: user@host> **configure**
`Fixed-width text like this`	Represents output that appears on the terminal screen.	`user@host>` **show chassis alarms** `No alarms currently active`

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

Convention	Description	Examples
Italic text like this	• Introduces or emphasizes important new terms. • Identifies book names. • Identifies RFC and Internet draft titles.	• A policy *term* is a named structure that defines match conditions and actions. • *Junos OS System Basics Configuration Guide* • RFC 1997, *BGP Communities Attribute*
Italic text like this	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: **[edit]** **root@# set system domain-name** *domain-name*
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	• To configure a stub area, include the **stub** statement at the **[edit protocols ospf area area-id]** hierarchy level. • The console port is labeled **CONSOLE**.
< > (angle brackets)	Enclose optional keywords or variables.	**stub <default-metric** *metric***>;**
| (pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	**broadcast | multicast** **(***string1* **|** *string2* **|** *string3***)**
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	**rsvp { # Required for dynamic MPLS only**
[ ] (square brackets)	Enclose a variable for which you can substitute one or more values.	**community name members [** *community-ids* **]**
Indention and braces ({ })	Identify a level in the configuration hierarchy.	**[edit]** **routing-options {** ** static {** ** route default {** ** nexthop** *address*; ** retain;** ** }** ** }** **}**
; (semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	• In the Logical Interfaces box, select **All Interfaces**. • To cancel the configuration, click **Cancel**.
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select **Protocols>Ospf**.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/ . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/

- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

CHAPTER 1

Broadband Subscriber Management Basics Overview

Broadband Subscriber Management Overview

Broadband Subscriber Management is a method of dynamically provisioning and managing subscriber access in a multiplay or triple play network environment. This method uses AAA configuration in conjunction with dynamic profiles to provide dynamic, per-subscriber authentication, addressing, access, and configuration for a host of broadband services including Internet access, gaming, IPTV, Video on Demand (VoD), and subscriber wholesaling.

NOTE: **The Junos OS broadband subscriber management solution currently supports Dynamic Host Configuration Protocols (DHCP)-based and Point-to-Point Protocol /Point-to-Point Protocol over Ethernet (PPP/PPPoE)-based configuration and RADIUS authentication and authorization.**

This guide focuses on the general components necessary for configuring a Juniper Networks MX Series 3D Universal Edge Router to dynamically provision and manage subscribers. However, you can also use a Juniper Networks EX Series Ethernet Switch in a subscriber network.

Managing subscribers in a DHCP-based or PPP/PPPoE-based residential broadband network using an MX Series router requires the following:

- Planning and configuring a virtual LAN (VLAN) architecture for the access network.
- Configuring an authentication, authorization, and accounting (AAA) framework for subscriber authentication and authorization through external servers (for example, RADIUS) as well as accounting and dynamic-request change of authorization (CoA)

and disconnect operations through external servers, and address assignment through a combination of local address-assignment pools and RADIUS.

- Configuring DHCP local server or DHCP relay for subscriber address assignment for DHCP-based networks.
- Configuring address assignment pools for PPPoE-based networks.
- Configuring dynamic profiles to include dynamic IGMP, firewall filter, and class of service (CoS) configuration for subscriber access.
- Configuring multicast access to the core network.

To better understand the subscriber access network, this guide also provides general information about some hardware not from Juniper Networks and suggests methods for choosing different network configuration options. You can configure a subscriber network in many different ways. This guide does not cover all configuration scenarios. It is intended as a starting point for understanding subscriber management and how you can use Juniper Networks hardware and software to plan and build your own subscriber management solution.

Related Documentation

- Broadband Subscriber Management Platform Support on page 4
- *Broadband Subscriber Management Network Topology Overview*
- Broadband Subscriber Management Solutions Terms and Acronyms on page 5
- Supporting Documentation for Broadband Subscriber Management on page 6
- *Triple Play and Multiplay Overview*
- *Broadband History*

Broadband Subscriber Management Platform Support

Juniper Networks currently supports DHCP and PPP/PPPoE broadband subscriber management solutions on MX Series routers and PPP/PPPoE broadband subscriber management solutions on M120 and M320 routers.

NOTE: **This guide describes configuration on MX Series routers.**

Related Documentation

- Broadband Subscriber Management Overview on page 3
- Broadband Subscriber Management Edge Router Overview on page 9

Broadband Subscriber Management Solutions Terms and Acronyms

- **AAA (authentication, authorization, and accounting)**—An IP-based networking system that controls user access to computer resources and manages the activity of users over a network.
- **ASM (Any Source Multicast)**—A method of allowing a multicast receiver to listen to all traffic sent to a multicast group, regardless of its source.
- **BSR (broadband services router)**—A router used for subscriber management and edge routing.
- **CoA (change of authorization)**—RADIUS messages that contain information for dynamically changing session authorizations.
- **CoS (class of service)**—A method of managing network traffic by grouping similar types of traffic together and treating each traffic type as a "class" with a defined service priority.
- **DHCP (Dynamic Host Configuration Protocol)**—A mechanism through which hosts using TCP/IP can obtain protocol configuration parameters automatically from a DHCP server on the network; allocates IP addresses dynamically so that they can be reused when no longer needed.
- **IGMP (Internet Group Membership Protocol)**—A host-to-router signaling protocol for IPv4 used to support IP multicasting.
- **IS-IS (Intermediate System-to-Intermediate System)**—A link-state interior gateway routing protocol (IGRP) for IP networks that uses the shortest-path-first (SPF) algorithm to determine routes.
- **LSP (label-switched path)**—The path traversed by a packet that is routed by MPLS. Some LSPs act as tunnels. LSPs are unidirectional, carrying traffic only in the downstream direction from an ingress node to an egress node.
- **MPLS (Multiprotocol Label Switching)**—A mechanism for engineering network traffic patterns that functions by assigning to network packets short labels that describe how to forward the packets through the network.
- **MSAN (multiservice access node)**—A group of commonly used aggregation devices including digital subscriber line access multiplexers (DSLAMs) used in xDSL networks, optical line termination (OLT) for PON/FTTx networks, and Ethernet switches for Active Ethernet connections.
- **Multiplay**—A networking paradigm that enables the ability to add new and robust networking services that individual subscribers can access.
- **OIF (outgoing interface)**—An interface used by multicast functions within a router to determine which egress ports to use for fowarding multicast groups.
- **OSPF (Open Shortest Path First)**—A link-state interior gateway protocol (IGP) that makes routing decisions based on the shortest-path-first (SPF) algorithm (also referred to as the Dijkstra algorithm).

- **PIM (Protocol Independent Multicast)**—A multicast routing protocol used for delivering multicast messages in a routed environment.
- **PPP (Point-to-Point Protocol)**—A link-layer protocol that provides multiprotocol encapsulation. PPP is used for link-layer and network-layer configuration. Provides a standard method for transporting multiprotocol datagrams over point-to-point links.
- **PPPoE (Point-to-Point Protocol over Ethernet)**—A network protocol that encapsulates PPP frames in Ethernet frames and connects multiple hosts over a simple bridging access device to a remote access concentrator.
- **RADIUS (Remote Authentication Dial-In User Service)**—A networking protocol that provides centralized access, authorization, and accounting management for subscribers to connect and use a network service.
- **Residential gateway**—A firewall, Network Address Translation (NAT) router, or other routing device used as a customer premises equipment (CPE) terminator in the home, office, or local point of presence (POP).
- **SSM (single-source multicast)**—A routing method that allows a multicast receiver to detect only a specifically identified sender within a multicast group.
- **set-top box**—The end host or device used to receive IPTV video streams.
- **Triple play**—A networking paradigm that dedicates bandwidth to data, voice, and video service.
- **VOD (video on demand)**—A unicast streaming video offering by service providers that enables the reception of an isolated video session per user with rewind, pause, and similar VCR-like capabilities.
- **VSR (video services router)**—A router used in a video services network to route video streams between an access network and a metro or core network. The video services router is any M Series Multiservice Edge Router or MX Series router that supports the video routing package provided with Junos OS Release 8.3 or later.

Related Documentation

- Broadband Subscriber Management Overview on page 3

Supporting Documentation for Broadband Subscriber Management

The *Junos OS Subscriber Management and Services Library* relies heavily on existing configuration documentation. In particular, this guide references configuration material presented in the *Junos OS Subscriber Management and Services Library*. We recommend you become familiar with the configuration options presented for subscriber access before reading this guide.

Several guides in the Junos OS documentation set provide detailed configuration information that is not fully covered in this guide. This guide might reference other Junos OS configuration and solutions documents that can provide more detail about a specific feature or configuration option.

For more detailed configuration information, see the following Junos OS documents:

- *Junos OS Subscriber Management and Services Library*
- *Junos OS Layer 2 Switching and Bridging Library for Routing Devices*
- *Multicast Protocols Feature Guide for Routing Devices*
- *Junos OS Network Interfaces Library for Routing Devices*
- *Routing Policy Feature Guide for Routing Devices*

In addition to related Junos OS documentation, you can obtain useful information from the JunosE Software documentation. Many features described in the *JunosE Broadband Access Configuration Guide* are similar to those described in both this guide and the *Junos OS Subscriber Management and Services Library*.

Related Documentation

- Broadband Subscriber Management Overview on page 3

CHAPTER 2

Broadband Subscriber Management Solution Hardware Overview

Broadband Subscriber Management Edge Router Overview

The edge router is the demarcation point between the residential broadband access network and the core network. The Juniper Networks MX Series router (along with the Juniper Networks EX Series Ethernet Switch) can play multiple roles as an edge router. The most common include the following:

- **Broadband services router (BSR)**—This router supports high speed Internet access along with several other subscriber-based services including VoIP, IPTV, and gaming.
- **Video services router (VSR)**—The video services router capabilities are a subset of those provided by a broadband services router. In general, using the MX Series router as a video services router provides bi-directional traffic destined for the set-top box (STB). This traffic includes IPTV and video on demand (VoD) streams as well as associated control traffic such as IGMP and electronic program guide (EPG) updates.

You can also use the MX Series router in certain Layer 2 solutions. For information about configuring the MX Series router in Layer 2 scenarios, see the *Junos OS Layer 2 Switching and Bridging Library for Routing Devices* or the *Ethernet Networking Feature Guide for MX Series Routers*.

Broadband Services Router Overview

A broadband services router is an edge router that traditionally supports primarily Internet-bound traffic. This router replaces and provides a superset of the functionality provided by a Broadband Remote Access Server (B-RAS). The broadband services router functions can be broken into two key areas—high speed Internet access and IPTV support.

High-Speed Internet Access Support

The broadband services router communicates with the RADIUS server to enforce which services each subscriber can access. For example, one subscriber might have signed up

for a smaller Internet access service of 1 Mbps where another subscriber might have signed up for a higher, 10 Mbps service. The broadband services router manages the traffic to each subscriber, ensuring that each subscriber obtains the level of access service they have purchased, while also ensuring that any VoIP traffic receives priority. The broadband services router also makes traffic forwarding decisions based on aggregate bandwidth detected on any adjacent multiservice access node (MSAN).

IPTV Support

The broadband services router supports IPTV traffic including support for IGMP multicast group start and stop requests from downstream MSANs. The broadband services router manages the bandwidth allocations associated with high-bandwidth IPTV as well as video on demand (VoD) traffic to ensure high quality service delivery.

Video Services Router

When configuring a multiedge network, you can use the MX Series router as a video services router (VSR) to support only video traffic without supporting the high-speed Internet access (HSIA) capabilities.

NOTE: We recommend a single-edge network model but the MX Series router allows for flexibility when defining a multiplay network topology.

Some advantages of using a separate video services router for video traffic include the following:

- Provides the ability to add IPTV service without the need to modify an existing edge router that is performing other functions.
- Reduces network bandwidth by moving the video edge further out to the network edge while still allowing for centralized broadband services router operation.
- Typically requires less capital investment because the video services router does not need to provide per-subscriber management.

Services Router Placement

Depending on the type of network you are creating—single edge or multiedge—you can place a broadband services router or video services router in various locations.

Single-Edge Placement

In a single-edge network, you use only broadband services routers because the single device must perform all of the necessary edge functions—providing subscriber management for high-speed Internet access and IPTV services. You can use the two following topology models when placing the broadband services router:

- **Centralized single edge**—The edge router is centrally located and placed at one location to cover a particular region. A secondary router is sometimes placed in this location to act as a backup. Downstream MSANs are connected to the broadband services router using a ring or mesh topology.

- **Distributed single edge**—The edge router is placed further out into the network, typically in the central office (CO) closest to the subscribers that it services. Downstream MSANs are typically connected directly to the broadband services router (in a true, single edge topology) or through an Ethernet aggregation switch.

In general, the addition of IPTV service favors a more distributed model because it pushes the need for subscriber management farther out into the network.

Multiedge Placement

In a multiedge network, you use both broadband services routers and video services routers. The broadband services router controls any high-speed Internet traffic and the video services router controls video traffic. You can use the two following topology models when placing service routers in a multiedge network topology:

- **Co-located multiedge**—The broadband services router and video services router are housed in the same location and an Ethernet switch directs traffic in the CO to the appropriate edge router.

NOTE: A single MX Series router can serve as both Ethernet switch and video services router. For information about configuring the MX Series router in Layer 2 scenarios, see the *Junos OS Layer 2 Switching and Bridging Library for Routing Devices* or the *Ethernet Networking Feature Guide for MX Series Routers*.

- **Split multiedge**—The video services router and broadband services router reside in different locations. In this model, the broadband services router is typically located more centrally and video services routers are distributed.

Related Documentation

- Multiservice Access Node Overview on page 11
- Ethernet MSAN Aggregation Options on page 13
- Broadband Subscriber Management Platform Support on page 4

Multiservice Access Node Overview

A *multiservice access node* is a broader term that refers to a group of commonly used aggregation devices. These devices include digital subscriber line access multiplexers (DSLAMs) used in xDSL networks, optical line termination (OLT) for PON/FTTx networks, and Ethernet switches for Active Ethernet connections. Modern MSANs often support all of these connections, as well as providing connections for additional circuits such as plain old telephone service (referred to as POTS) or Digital Signal 1 (DS1 or T1).

The defining function of a multiservice access node is to aggregate traffic from multiple subscribers. At the physical level, the MSAN also converts traffic from the *last mile technology* (for example, ADSL) to Ethernet for delivery to subscribers.

You can broadly categorize MSANs into three types based on how they forward traffic in the network:

- **Layer–2 MSAN**—This type of MSAN is essentially a Layer 2 switch (though typically not a fully functioning switch) with some relevant enhancements. These MSANs use Ethernet (or ATM) switching to forward traffic. The MSAN forwards all subscriber traffic upstream to an edge router that acts as the centralized control point and prevents direct subscriber-to-subscriber communication. Ethernet Link Aggregation (LAG) provides the resiliency in this type of network.

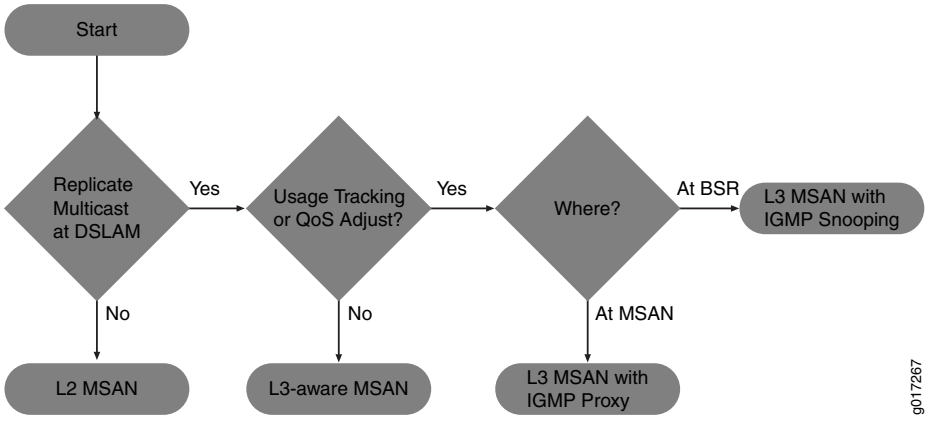
  Layer 2 DSLAMs cannot interpret IGMP, so they cannot selectively replicate IPTV channels.

- **Layer–3 aware MSAN**—This IP-aware MSAN can interpret and respond to IGMP requests by locally replicating a multicast stream and forwarding the stream to any subscriber requesting it. Layer 3 awareness is important when supporting IPTV traffic to perform channel changes (sometimes referred to as *channel zaps*). Static IP-aware MSANs always receive all multicast television channels. They do not have the ability to request that specific channels be forwarded to the DSLAM. Dynamic IP-aware DSLAMs, however, can inform the network to begin (or discontinue) sending individual channels to the DSLAM. Configuring IGMP proxy or IGMP snooping on the DSLAM accomplishes this function.

- **Layer–3 MSAN**—These MSANs use IP routing functionality rather than Layer 2 technologies to forward traffic. The advantage of this forwarding method is the ability to support multiple upstream links going to different upstream routers and improving network resiliency. However, to accomplish this level of resiliency, you must assign a separate IP subnetwork to each MSAN, adding a level of complexity that can be more difficult to maintain or manage.

In choosing a MSAN type, refer to Figure 1 on page 12:

Figure 1: Choosing an MSAN Type



Related Documentation

- Ethernet MSAN Aggregation Options on page 13

Ethernet MSAN Aggregation Options

Each MSAN can connect directly to an edge router (broadband services router or video services router), or an intermediate device (for example, an Ethernet switch) can aggregate MSAN traffic before being sent to the services router. Table 3 on page 13 lists the possible MSAN aggregation methods and under what conditions they are used.

Table 3: Ethernet MSAN Aggregation Methods

Method	When Used
Direct connection	Each MSAN connects directly to the broadband services router and optional video services router.
Ethernet aggregation switch connection	Each MSAN connects directly to an intermediate Ethernet switch. The switch, in turn, connects to the broadband services router or optional video services router.
Ethernet ring aggregation connection	Each MSAN connects to a ring topology of MSANs. The head-end MSAN (the device closest to the upstream edge router) connects to the broadband services router.

You can use different aggregation methods in different portions of the network. You can also create multiple layers of traffic aggregation within the network. For example, an MSAN can connect to a central office terminal (COT), which, in turn, connects to an Ethernet aggregation switch, or you can create multiple levels of Ethernet aggregation switches prior to connecting to the edge router.

Direct Connection

In the direct connection method, each MSAN has a point-to-point connection to the broadband services router. If an intermediate central office exists, traffic from multiple MSANs can be combined onto a single connection using wave-division multiplexing (WDM). You can also connect the MSAN to a video services router. However, this connection method requires that you use a Layer 3 MSAN that has the ability to determine which link to use when forwarding traffic.

When using the direct connection method, keep the following in mind:

- We recommend this approach when possible to simplify network management.
- Because multiple MSANs are used to connect to the services router, and Layer 3 MSANs generally require a higher equipment cost, this method is rarely used in a multiedge subscriber management model.
- Direct connection is typically used when most MSAN links are utilized less than 33 percent and there is little value in combining traffic from multiple MSANs.

Ethernet Aggregation Switch Connection

An Ethernet aggregation switch aggregates traffic from multiple downstream MSANs into a single connection to the services router (broadband services router or optional video services router).

When using the Ethernet aggregation switch connection method, keep the following in mind:

- Ethernet aggregation is typically used when most MSAN links are utilized over 33 percent or to aggregate traffic from lower speed MSANs (for example, 1 Gbps) to a higher speed connection to the services router (for example, 10 Gbps).
- You can use an MX Series router as an Ethernet aggregation switch. For information about configuring the MX Series router in Layer 2 scenarios, see the *Junos OS Layer 2 Switching and Bridging Library for Routing Devices* or the *Ethernet Networking Feature Guide for MX Series Routers*.

Ring Aggregation Connection

In a ring topology, the remote MSAN that connects to subscribers is called the remote terminal (RT). This device can be located in the outside plant (OSP) or in a remote central office (CO). Traffic traverses the ring until it reaches the central office terminal (COT) at the head-end of the ring. The COT then connects directly to the services router (broadband services router or video services router).

NOTE: **The RT and COT must support the same ring resiliency protocol.**

You can use an MX Series router in an Ethernet ring aggregation topology. For information about configuring the MX Series router in Layer 2 scenarios, see the *Junos OS Layer 2 Switching and Bridging Library for Routing Devices* or the *Ethernet Networking Feature Guide for MX Series Routers*.

Related Documentation

- Multiservice Access Node Overview on page 11

CHAPTER 3

Broadband Subscriber Management Solution Software Overview

Broadband Subscriber Management VLAN Architecture Overview

The subscriber management logical network architecture is as important as the physical network architecture. You configure the logical portion of the subscriber management network using virtual local area networks (VLANs).

Three VLAN models deliver multiple services to subscribers. These models include the following:

- **Service VLAN**—The service VLAN (S-VLAN) provides many-to-one (N:1) subscriber-to-service connectivity: The service VLAN carries a service (for example, data, video, or voice) to all subscribers instead of having different services share a VLAN. Adding a new service requires adding a new VLAN and allocating bandwidth to the new service. The service VLAN model enables different groups that are using the broadband network (for example, external application providers) to manage a given service. One limitation of service VLANs is the absence of any logical isolation between user sessions at the VLAN level. This lack of isolation requires that the multiservice access node (MSAN) and broadband services router provide the necessary security filtering.
- **Customer VLAN**—The customer VLAN (C-VLAN) provides one-to-one (1:1) subscriber-to-service connectivity: One VLAN carries all traffic to each subscriber on the network. Having a single VLAN per subscriber simplifies operations by providing a 1:1 mapping of technology (VLANs) to subscribers. You can also understand what applications any subscriber is using at any given time. Because you use only one VLAN to carry traffic to each subscriber, this approach is not affected when adding new services. However, using a pure C-VLAN model consumes more bandwidth because a single television channel being viewed by multiple subscribers is carried across the network several times—once on each C-VLAN. This approach requires a more scalable, robust edge router that can support several thousand VLANs.
- **Hybrid C-VLAN**—The hybrid VLAN combines the best of both previous VLANs by using one VLAN per subscriber to carry unicast traffic and one shared multicast VLAN

(M-VLAN) for carrying broadcast (multicast) television traffic. You can use both the *pure* and *hybrid* C-VLAN models in different portions of the network, depending upon available bandwidth and MSAN capabilities.

NOTE: The term *C-VLAN*, when used casually, often refers to a *hybrid* C-VLAN implementation.

We recommend using one of the C-VLAN models to simplify configuration and management when expanding services. However, some MSANs are limited to the number of VLANs they can support, limiting the ability to use either C-VLAN model.

NOTE: Most MSANs can support the service VLAN model.

Broadband Subscriber Management VLANs Across an MSAN

You configure VLANs to operate between the MSAN and the edge router (broadband services router or video services router). However, the MSAN might modify VLAN identifiers before forwarding information to the subscriber in the following ways:

NOTE: Not all MSANs support these options.

- The VLAN identifiers can be carried within the ATM VCs or they can be removed. The value of keeping the VLAN header is that it carries the IEEE 802.1p Ethernet priority bits. These priority bits can be added to upstream traffic by the residential gateway, allowing the DSLAM to easily identify and prioritize more important traffic (for example, control and VoIP traffic). Typically, a VLAN identifier of zero (0) is used for this purpose.
- In a C-VLAN model, the MSAN might modify the VLAN identifier so that the same VLAN is sent to each subscriber. This enables the use of the same digital subscriber line (DSL) modem and residential gateway configuration for all subscribers without the need to define a different VLAN for each device.

Customer VLANs and Ethernet Aggregation

The 12-bit VLAN identifier (VLAN ID) can support up to 4095 subscribers. When using an aggregation switch with a C-VLAN topology, and fewer than 4095 subscribers are connected to a single edge router port, the aggregation switch can transparently pass all VLANs. However, if the VLAN can exceed 4095 subscribers per broadband services router port, you must use VLAN stacking (IEEE 802.1ad, also known as Q-in-Q). VLAN stacking includes two VLAN tags—an outer tag to identify the destination MSAN and an inner tag to identify the subscriber. For downstream traffic (that is, from the broadband services router or Ethernet switch to the MSAN), the outer tag determines which port to forward traffic. The forwarding device then uses the VLAN pop function on this tag before forwarding the traffic with a single tag. The reverse process occurs for upstream traffic.

VLAN stacking is not necessary for S-VLANs or M-VLANs. However, for the hybrid (C-VLAN and M-VLAN) model, the Ethernet switch or services router must be able to pop or push tags onto C-VLAN traffic while not modifying M-VLAN packets.

VLANs and Residential Gateways

One function provided by a residential gateway is to enable each subscriber to have a private (in-home) network, unseen by other broadband subscribers, while enabling the subscriber to have multiple devices connected to the broadband network. This private network is made possible by using Network Address Translation (NAT).

Most conditional access systems (for example, video on demand) require detecting the real IP address of the set-top box (STB). This security measure means that traffic to and from the STB must be bridged, not routed, across all network elements including aggregation switches, MSANs, and residential gateways. NAT cannot be used at the residential gateway for traffic to and from the STB. In addition, some residential gateways associate VLANs (or ATM virtual circuits) with ports. Traffic on a given VLAN is always forwarded to specific downstream port. Use caution when mapping VLANs on an MSAN.

Related Documentation

- *Static Subscriber Interfaces and VLAN Overview* in the *Junos OS Subscriber Management and Services Library*.

AAA Service Framework and Broadband Subscriber Management Overview

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

NOTE: **The broadband subscriber management solution currently supports the use of only RADIUS servers.**

The broadband services router interacts with external servers to determine how individual subscribers access the broadband network. The router also obtains information from external servers for the following:

- Methods used for authentication and accounting.
- How accounting statistics are collected and used.
- How dynamic requests are handled.

Related Documentation

- *AAA Service Framework Overview* in the *Junos OS Subscriber Management and Services Library*.
- *RADIUS-Initiated Change of Authorization (CoA) Overview* in the *Junos OS Subscriber Management and Services Library*.

- *RADIUS-Initiated Disconnect Overview* in the *Junos OS Subscriber Management and Services Library*.

CHAPTER 4

Broadband Subscriber Management Layer 2 Wholesale Overview

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*
- *Broadband Subscriber Management PPPoE Layer 3 Wholesale Topology and Configuration Elements*
- Broadband Subscriber Management Layer 2 Wholesale Topology and Configuration Elements on page 25

Wholesale Network Configuration Options and Considerations

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

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

RADIUS VSAs and Broadband Subscriber Management Wholesale Configuration Overview

You can use RADIUS to assign various values through the use of dynamic variables within dynamic profiles. However, the configuration of at least one of the two VSAs described in Table 4 on page 21 is required for a wholesale network to function.

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

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

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

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

Related Documentation

- *Juniper Networks VSAs Supported by the AAA Service Framework* in the *Junos OS Subscriber Management and Services Library*.

PART 2

Configuration

CHAPTER 5

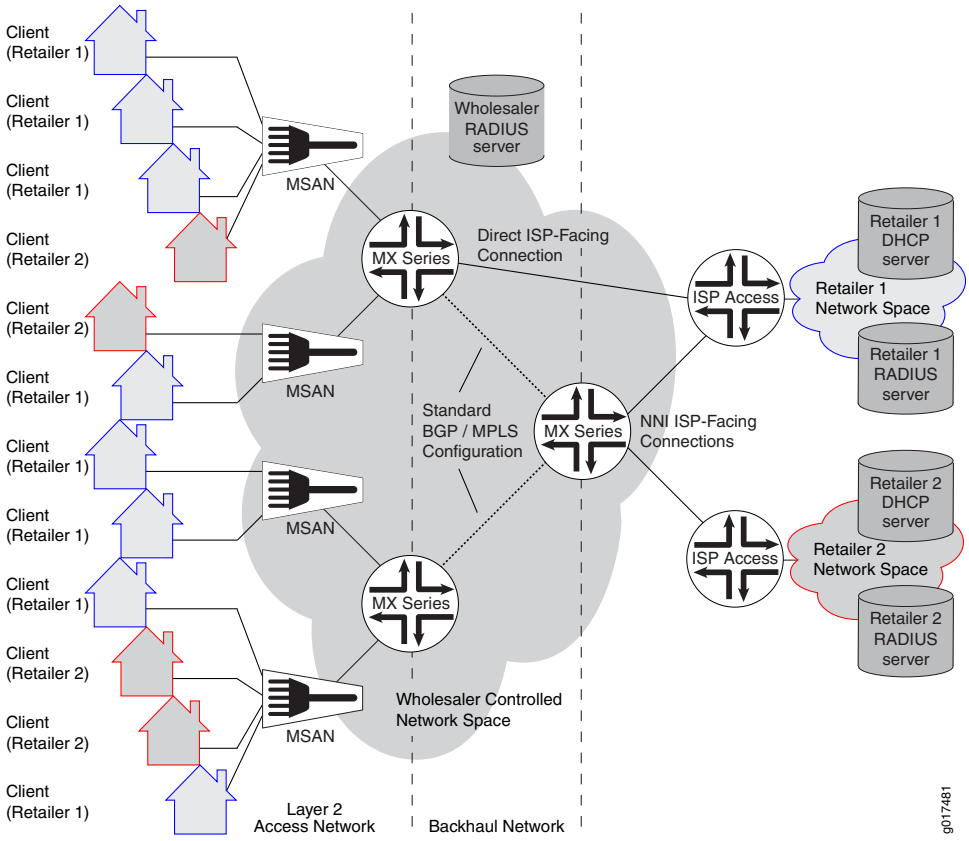
Broadband Subscriber Management Layer 2 Wholesale Network Configuration

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.

To explain the concept but limit complexity, this solution provides a configuration with one wholesaler and only two retailers. Figure 2 on page 26 illustrates a basic Layer 2 wholesale topology model from which you can expand.

Figure 2: Basic Subscriber Management Layer 2 Wholesale Solution Topology



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

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

Related Documentation

- Layer 2 and Layer 3 Wholesale Overview on page 19
- Layer 2 Wholesale Network Topology Overview on page 26

Layer 2 Wholesale Network Topology Overview

This configuration explains how to configure a simple Layer 2 wholesale subscriber access network. This solution illustrates two Internet Service Provider (ISP) retailers sharing

access to a wholesaler network. The wholesaler network contains a Layer 2 Network access router and two Virtual Private LAN Service (VPLS) network-to-network interface (NNI) routers.

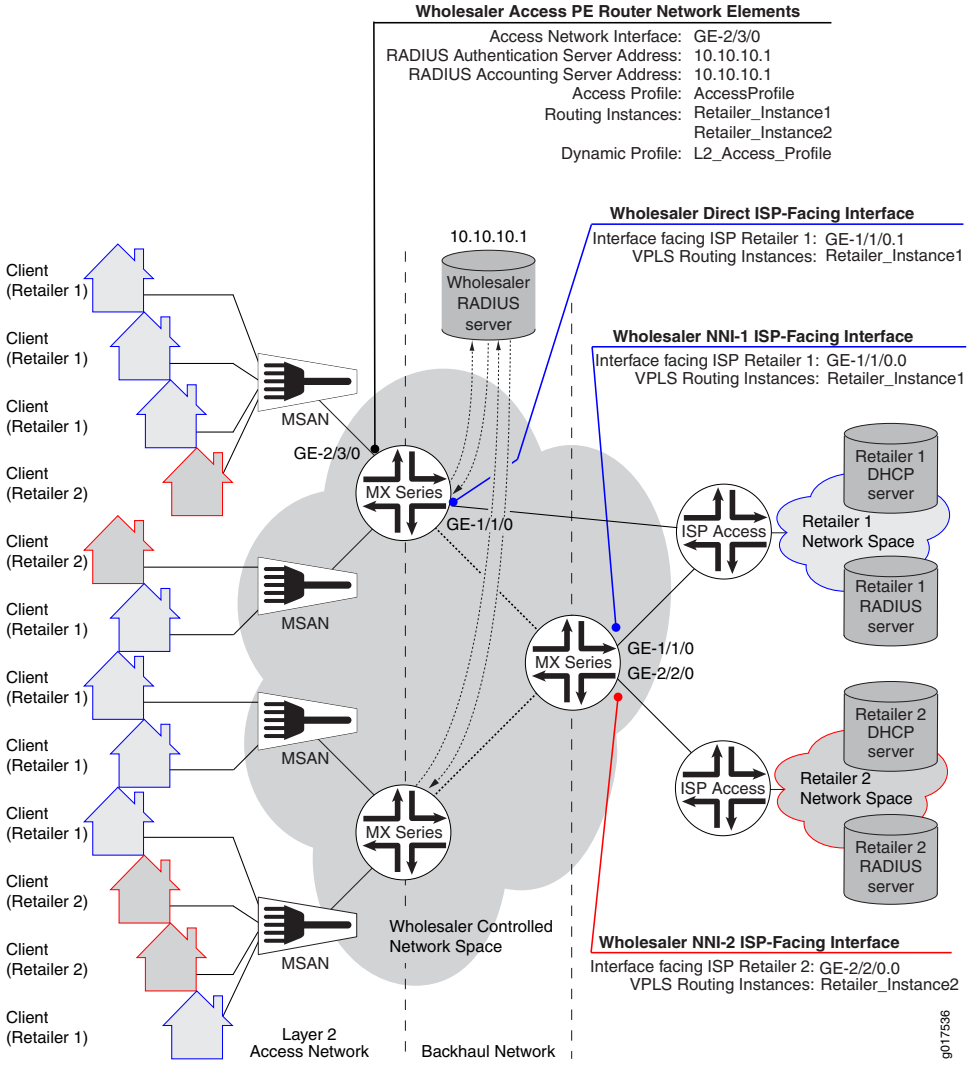
NOTE: You can have more than one ISP router connecting to a single VPLS NNI router with VPLS interfaces configured with routing instances specific to each different ISP-facing interfaces.

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

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

Figure 3 on page 28 provides the reference topology for this configuration example.

Figure 3: Layer 2 Wholesale Network Reference Topology



Related Documentation

- Layer 2 and Layer 3 Wholesale Overview on page 19
- Broadband Subscriber Management Layer 2 Wholesale Topology and Configuration Elements on page 25

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

To configure a dynamic profile for use with retailer access:

1. Create a retail dynamic profile.

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

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

   ```
   [edit dynamic-profiles Subscriber_Profile_Retail1]
   ```

```
user@host# edit routing-instances $junos-routing-instance
```

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

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

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

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

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

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

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

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

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

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

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

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

8. Define the input and output VLAN maps. See "Stacking and Rewriting VLAN Tags for the Layer 2 Wholesale Solution" on page 29 for details.

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

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

Stacking and Rewriting VLAN Tags for the Layer 2 Wholesale Solution

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

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

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

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

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

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

The type of VLAN rewrite operation permitted depends upon whether the frame is single-tagged or dual-tagged. Table 5 on page 30 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 5: 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 6 on page 30 shows what rewrite operation combinations you can configure. "None" means that no rewrite operation is specified for the VLAN map.

Table 6: 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

Table 6: Applying Rewrite Operations to VLAN Maps *(continued)*

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

To configure the input VLAN map:

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

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

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

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

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

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

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

To configure the output VLAN map:

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

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

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

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

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

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

Configuring VLAN Interfaces for the Layer 2 Wholesale Solution

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

To configure a VLAN interface for dynamic access of clients:

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

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

2. Specify the desired VLAN tagging.

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

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

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

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

4. Specify that you want to configure single VLANs.

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

5. Define the VLAN ranges for the configuration.

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

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

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

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

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

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

9. Specify the encapsulation type for the VLAN interfaces.

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

Related Documentation

- *Configuring Single-Level VLAN Ranges for Use with VLAN Dynamic Profiles*
- Configuring Encapsulation for Layer 2 Wholesale VLAN Interfaces on page 33

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 7 on page 33 provides the valid encapsulation combinations for both dynamic profiles and physical interfaces in the Layer 2 wholesale network.

Table 7: Encapsulation Combinations for Layer 2 Wholesale Interfaces

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

To configure encapsulation for Layer 2 wholesale VLAN interfaces:

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

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

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

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

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

Related Documentation

- Configuring a Retail Dynamic Profile for Use in the Layer 2 Wholesale Solution on page 28
- Configuring VLAN Interfaces for the Layer 2 Wholesale Solution on page 32

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

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

To configure an NNI ISP-facing interface:

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

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

2. Specify the encapsulation type for the VLAN interfaces.

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

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

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

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

Related Documentation

- *Configuring Single-Level VLAN Ranges for Use with VLAN Dynamic Profiles*
- Configuring Direct ISP-Facing Interfaces for the Layer 2 Wholesale Solution on page 34
- Configuring Separate Access Routing Instances for Layer 2 Wholesale Service Retailers on page 35

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 Single-Level VLAN Ranges for Use with VLAN Dynamic Profiles*
- Configuring NNI ISP-Facing Interfaces for the Layer 2 Wholesale Solution on page 34
- Configuring Separate Access Routing Instances for Layer 2 Wholesale Service Retailers on page 35

Configuring Separate Access Routing Instances for Layer 2 Wholesale Service Retailers

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

When creating separate routing instances, it is important to understand the role that the router plays in the Layer 2 Wholesale network and specify that role (either access or NNI) in the routing instance configuration. If the router connects directly to an ISP network (or ISP-controlled device), you must configure the routing instances as an NNI routing instance. See "Configuring Separate NNI Routing Instances for Layer 2 Wholesale Service Retailers" on page 38.

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.

Related Documentation

- *Configuring VPLS Routing Instances*
- Configuring NNI ISP-Facing Interfaces for the Layer 2 Wholesale Solution on page 34
- Configuring Separate NNI Routing Instances for Layer 2 Wholesale Service Retailers on page 38

Configuring Separate NNI Routing Instances for Layer 2 Wholesale Service Retailers

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

When creating separate routing instances, it is important to understand the role that the router plays in the Layer 2 Wholesale network and specify that role (either access or NNI) in the routing instance configuration. If the router connects to the access portion of the network (for example, to an MSAN device) , you must configure the routing instances as an access routing instance. See "Configuring Separate Access Routing Instances for Layer 2 Wholesale Service Retailers" on page 35.

To define a retailer routing instance:

1. Create the retailer routing instance.

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

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

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

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

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

4. Specify the routing instance type for the retailer.

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

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

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

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

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

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

   ```
   [edit routing-instances RetailerInstance1]
   user@host# set route-distinguisher 10.10.1.1:1
   ```

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 1000
      ```

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

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

   e. Specify a site name.

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

   f. Specify a site identifier.

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

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

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

10. Repeat this procedure for other retailers.

Related Documentation

- *Configuring VPLS Routing Instances*
- Configuring VLAN Interfaces for the Layer 2 Wholesale Solution on page 32
- Configuring Separate Access Routing Instances for Layer 2 Wholesale Service Retailers on page 35

Configuring Access Components for the Layer 2 Wholesale Network Solution

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

- Configuring RADIUS Server Access on page 40
- Configuring a Layer 2 Wholesaler Access Profile on page 40

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 $9$CzBxBBf1eWx-wM8xgaU.m345B02EcyKXL
   user@host# set 10.10.10.1 secret $7$OsCsBAf1fXx-wY3xgaU.m123A02ZtyNMT
   ```

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
```

CHAPTER 6

Broadband Subscriber Management Layer 2 Wholesale Network Configuration Statements

accept

Syntax accept (any | dhcp-v4 |dhcp-v6| inet | inet6 | pppoe);

Hierarchy Level [edit interfaces *interface-name* auto-configure stacked-vlan-ranges dynamic-profile *profile-name*],
[edit interfaces *interface-name* auto-configure vlan-ranges dynamic-profile *profile-name*]

Release Information Statement introduced in Junos OS Release 9.5.
dhcp-v4 option added in Junos OS Release 10.0.
dhcp-v6, **inet6** and **pppoe** options added in Junos OS Release 10.2.
any option added in Junos OS Release 10.4.

Description Specify the type of VLAN Ethernet packet accepted by an interface that is associated with a VLAN dynamic profile or stacked VLAN dynamic profile.

Options

any—Any packet type. Specifies that any incoming packets trigger the dynamic creation of a VLAN with properties determined by the auto-configure interface configuration stanza and associated profile attributes. This option is used when configuring wholesaling in a Layer 2 network.

dhcp-v4—IPv4 DHCP packet type. Specifies that incoming IPv4 DHCP discover packets trigger the dynamic creation of a VLAN with properties determined by the auto-configure interface configuration stanza and associated profile attributes

NOTE: The DHCP-specific **mac-address** and **option-82** options are rejected if the **accept** statement is not set to **dhcp-v4**.

dhcp-v6—IPv6 DHCP packet type. Specifies that incoming IPv6 DHCP discover packets trigger the dynamic creation of a VLAN with properties determined by the auto-configure interface configuration stanza and associated profile attributes.

inet—IPv4 Ethernet and ARP packet type.

inet6—IPv6 Ethernet packet type.

pppoe—Point-to-Point Protocol over Ethernet packet type.

NOTE: The **pppoe** VLAN Ethernet packet type option is supported only for Trio MPC/MIC interfaces on MX Series Routers.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Configuring the VLAN Ethernet Packet Type for Single-Tag VLAN Dynamic Profiles*
- *Configuring the VLAN Ethernet Packet Type for Stacked VLAN Dynamic Profiles*
- Configuring VLAN Interfaces for the Layer 2 Wholesale Solution on page 32

accounting-server

Syntax accounting-server [*ip-address*];

Hierarchy Level [edit access profile *profile-name* radius]

Release Information Statement introduced in Junos OS Release 9.1.

Description Specify a list of the RADIUS accounting servers used for accounting for DHCP, L2TP, and PPP clients.

Options ***ip-address***—IP version 4 (IPv4) address.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- *Configuring Authentication and Accounting Parameters for Subscriber Access*

authentication-order

Syntax authentication-order [*authentication-methods*];

Hierarchy Level [edit access profile *profile-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
none option introduced in Junos OS Release 11.2.

Description Set the order in which the Junos OS tries different authentication methods when verifying that a client can access the router or switch. For each login attempt, the software tries the authentication methods in order, from first to last.

Default password

Options *authentication-methods*

- **none**—Grants authentication without examining the client credentials. Can be used, for example, when the Diameter function Gx-Plus is employed for notification during subscriber provisioning.
- **password**—Verify the client using the information configured at the **[edit access profile *profile-name* client *client-name*]** hierarchy level.
- **radius**—Verify the client using RADIUS authentication services.

NOTE: For subscriber access management, you must always specify the radius method. Subscriber access management does not support the password option (the default), and authentication fails when no method is specified.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring CHAP Authentication with RADIUS*
- *Specifying the Authentication and Accounting Methods for Subscriber Access*
- *Configuring Access Profiles for L2TP or PPP Parameters*

authentication-server

Syntax authentication-server [*ip-address*];

Hierarchy Level [edit access profile *profile-name* radius]

Release Information Statement introduced in Junos OS Release 9.1.

Description Specify a list of the RADIUS authentication servers used to authenticate DHCP, L2TP, and PPP clients. The servers in the list are also used as RADIUS dynamic-request servers, from which the router accepts and processes RADIUS disconnect requests, CoA requests, and dynamic service activations and deactivations.

Options ***ip-address***—IPv4 address.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- *Configuring RADIUS Server Parameters for Subscriber Access*

auto-configure

Syntax

```
auto-configure {
  vlan-ranges {
    access-profile profile-name;
    authentication {
      password password-string;
      username-include{
        circuit-type;
        delimiter delimiter-character;
        domain-name domain-name-string;
        interface-name;
        mac-address;
        option-18;
        option-37;
        option-82 <circuit-id> <remote-id>;
        radius-realm radius-realm-string;
        user-prefix user-prefix-string;
      }
    }
    dynamic-profile profile-name {
      accept (any | dhcp-v4 |dhcp-v6| inet | inet6 | pppoe);
      ranges (any | low-tag)–(any | high-tag);
    }
    override;
  }
  stacked-vlan-ranges {
    access-profile profile-name;
    authentication {
      password password-string;
      username-include {
        circuit-type;
        delimiter delimiter-character;
        domain-name domain-name-string;
        interface-name;
        mac-address;
        option-18;
        option-37;
        option-82 <circuit-id> <remote-id>;
        radius-realm radius-realm-string;
        user-prefix user-prefix-string;
      }
    }
    dynamic-profile profile-name {
      accept (any | dhcp-v4 |dhcp-v6| inet | inet6 | pppoe);
      ranges (any | low-tag–high-tag),(any | low-tag–high-tag);
    }
    override;
  }
  remove-when-no-subscribers;
}
```

Hierarchy Level [edit interfaces *interface-name*]

Release Information Statement introduced in Junos OS Release 9.5.

Description Enable the configuration of dynamic, auto-sensed VLANs.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Configuring VLAN Interfaces to Use Dynamic Profiles*

connectivity-type

Syntax connectivity-type (ce | irb | permanent);

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vpls],
[edit routing-instances *routing-instance-name* protocols vpls]

Release Information Statement introduced in Junos OS Release 9.1.
irb option introduced in Junos OS Release 9.3.
permanent option introduced in Junos OS Release 10.4.

Description Specify when a VPLS connection is taken down depending on whether or not the interface for the VPLS routing instance is customer-facing or integrated routing and bridging (IRB).

Default ce

Options

ce—Require that for the VPLS connection to be up, the customer-facing interface for the VPLS routing instance must also be up. If the customer-facing interface fails, the VPLS connection is taken down.

irb—Allow a VPLS connection to remain up so long as an IRB interface is configured for the VPLS routing instance.

permanent—Allow a VPLS connection to remain up until specifically taken down. This option is reserved for use in configuring Layer 2 Wholesale subscriber networks. See the *Broadband Subscriber Management Solutions Guide* for details about configuring a Layer 2 Wholesale network.

NOTE: To specifically take down a VPLS routing instance that is using the permanent option, all associated static logical interfaces must also be down.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Configuring VPLS Routing Instances*
- Configuring Separate NNI Routing Instances for Layer 2 Wholesale Service Retailers on page 38

core-facing

Syntax core-facing;

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number* family *family*],
[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family *family*]

Release Information Statement introduced in Junos OS Release 11.2.

Description Specifies that the VLAN is physically connected to a core-facing ISP router and ensures that the network does not improperly treat the interface as a client interface. When specified, the interface is inserted into the core-facing default mesh group where traffic from pseudowires that belong to the default mesh group is not forwarded on the core-facing link.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- *Junos OS Subscriber Management and Services Library*

dynamic-profile (VLAN)

Syntax
```
dynamic-profile profile-name {
  accept (any | dhcp-v4 |dhcp-v6| inet | inet6 | pppoe);
  ranges (any | low-tag)–(any | high-tag);
}
```

Hierarchy Level [edit interfaces *interface-name* auto-configure vlan-ranges]

Release Information Statement introduced in Junos OS Release 9.5.

Description Configure a dynamic profile for use when configuring dynamic VLANs.

Options ***profile-name***—Name of the dynamic profile that you want to use when configuring dynamic VLANs.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation
- *Dynamic Profiles Overview*
- *Configuring a Basic Dynamic Profile*
- *Associating a Single-Tag VLAN Dynamic Profile with an Interface*

dynamic-profiles

Syntax

```
dynamic-profiles {
  profile-name {
    class-of-service {
      interfaces {
        interface-name ;
        }
        unit logical-unit-number {
          classifiers {
            type (classifier-name | default);
          }
          output-traffic-control-profile (profile-name | $junos-cos-traffic-control-profile);
          rewrite-rules {
            dscp (rewrite-name | default);
            dscp-ipv6 (rewrite-name | default);
            ieee-802.1 (rewrite-name | default) vlan-tag (outer | outer-and-inner);
            inet-precedence (rewrite-name | default);
            }
          }
        }
      }
      scheduler-maps {
        map-name {
          forwarding-class class-name scheduler scheduler-name;
        }
      }
      schedulers {
        (scheduler-name) {
          buffer-size (seconds | percent percentage | remainder | temporal microseconds);
          drop-profile-map loss-priority (any | low | medium-low | medium-high | high)
            protocol (any | non-tcp | tcp) drop-profile profile-name;
          excess-priority (low | high | $junos-cos-scheduler-excess-priority);
          excess-rate (percent percentage | percent $junos-cos-scheduler-excess-rate);
          overhead-accounting (shaping-mode) <bytes (byte-value>;
          priority priority-level;
          shaping-rate (rate | predefined-variable);
          transmit-rate (percent percentage | rate | remainder) <exact | rate-limit>;
        }
      }
      traffic-control-profiles profile-name {
        delay-buffer-rate (percent percentage | rate | $junos-cos-delay-buffer-rate);
        excess-rate (percent percentage | proportion value | percent $junos-cos-excess-rate);
        guaranteed-rate (percent percentage | rate | $junos-cos-guaranteed-rate);
        overhead-accounting (shaping-mode) <bytes (byte-value>;
        scheduler-map map-name;
        shaping-rate (rate | predefined-variable);
      }
    }
    firewall {
      family family {
        fast-update-filter filter-name {
          interface-specific;
          match-order [match-order];
```

```
    term term-name {
      from {
        match-conditions;
      }
      then {
        action;
        action-modifiers;
      }
      only-at-create;
    }
  }
  firewall {
    family family {
      fast-update-filter filter-name {
        interface-specific;
      match-order [match-order];
        term term-name {
          from {
            match-conditions;
          }
          then {
            action;
            action-modifiers;
          }
        only-at-create;
      filter filter-name {
      interface-specific;
        term term-name {
          from {
            match-conditions;
          }
          then {
            action;
            action-modifiers;
          }
        }
    policer policer-name {
      filter-specific;
      if-exceeding {
        (bandwidth-limit bps | bandwidth-percent percentage);
        burst-size-limit bytes;
      }
      logical-bandwidth-policer;
      logical-interface-policer;
      physical-interface-policer;
      then {
        policer-action;
      }
    }
    hierarchical-policer policer-name {
      aggregate {
        if-exceeding {
          bandwidth-limit-limit bps;
          burst-size-limit bytes;
        }
        then {
```

```
                policer-action;
              }
            }
            premium {
              if-exceeding {
                bandwidth-limit bps;
                burst-size-limit bytes;
              }
              then {
                policer-action;
              }
            }
          }
          three-color-policer policer-name {
            action {
              loss-priority high then discard;
            }
            logical-interface-policer;
            single-rate {
              (color-aware | color-blind);
              committed-burst-size bytes;
              committed-information-rate bps;
              excess-burst-size bytes;
            }
            two-rate {
              (color-aware | color-blind);
              committed-burst-size bytes;
              committed-information-rate bps;
              peak-burst-size bytes;
              peak-information-rate bps;
              }
            }
          }
        }
        policy-options {
          prefix-listname {
            ip-addresses;
          }
        }
      }
    }
    interfaces interface-name {
      interface-set interface-set-name {
        interface interface-name {
          unit logical unit number {
            advisory-options {
              downstream-rate rate;
              upstream-rate rate;
            }
          }
        }
      }
      unit logical-unit-number {
        auto-configure {
          agent-circuit-identifier {
            dynamic-profile profile-name;
```

```
    }
  }
  encapsulation (atm-ccc-cell-relay | atm-ccc-vc-mux | atm-cisco-nlpid |
    atm-tcc-vc-mux | atm-mlppp-llc | atm-nlpid | atm-ppp-llc | atm-ppp-vc-mux |
    atm-snap | atm-tcc-snap | atm-vc-mux | ether-over-atm-llc |
    ether-vpls-over-atm-llc | ether-vpls-over-fr | ether-vpls-over-ppp | ethernet |
    frame-relay-ccc | frame-relay-ppp | frame-relay-tcc | frame-relay-ether-type |
    frame-relay-ether-type-tcc | multilink-frame-relay-end-to-end | multilink-ppp |
    ppp-over-ether | ppp-over-ether-over-atm-llc | vlan-bridge | vlan-ccc | vlan-vci-ccc
    | vlan-tcc | vlan-vpls);
  family family {
    address address;
    filter {
      adf {
        counter;
        input-precedence precedence;
        not-mandatory;
        output-precedence precedence;
        rule rule-value;
      }
      input filter-name (
        precedence precedence;
      }
      output filter-name {
        precedence precedence;
      }
    }
    rpf-check {
      fail-filter filter-name;
      mode loose;
    }
    service {
      input {
        service-set service-set-name {
          service-filter filter-name;
        }
        post-service-filter filter-name;
      }
      input-vlan-map {
        inner-tag-protocol-id tpid;
        inner-vlan-id number;
        (push | swap);
        tag-protocol-id tpid;
        vlan-id number;
      }
      output {
        service-set service-set-name {
          service-filter filter-name;
        }
      }
      output-vlan-map {
        inner-tag-protocol-id tpid;
        inner-vlan-id number;
        (pop | swap);
        tag-protocol-id tpid;
        vlan-id number;
```

```
            }
          }
          unnumbered-address interface-name <preferred-source-address address>;
        }
        ppp-options {
          chap;
          pap;
        }
        vlan-id number;
        vlan-tags outer [tpid].vlan-id [inner [tpid].vlan-id];
      }
    }
    interfaces {
      demux0 {...}
    }
    interfaces {
      pp0 {...}
    }
    protocols {
      igmp {
        interface interface-name {
          accounting;
          disable;
          group-policy;
          immediate-leave
          no-accounting;
          promiscuous-mode;
          ssm-map ssm-map-name;
          static {
            group group {
              source source;
            }
          }
          version version;
        }
        mld {
          interfaceinterface-name {
            disable;
            (accounting | no-accounting);
            group-policy;
            immediate-leave;
            oif-map;
            passive;
            ssm-map ssm-map-name;
            static {
              group multicast-group-address {
                exclude;
                group-count number;
                group-increment increment;
                source ip-address {
                  source-count number;
                  source-increment increment;
                }
              }
            }
            version version;
```

```
        }
      }
      router-advertisement {
        interface interface-name {
          current-hop-limit number;
          default-lifetime seconds;
          (managed-configuration | no-managed-configuration);
          max-advertisement-interval seconds;
          min-advertisement-interval seconds;
          (other-stateful-configuration | no-other-stateful-configuration);
          prefix prefix;
          reachable-time milliseconds;
          retransmit-timer milliseconds;
        }
      }
    }
  }
  routing-instances routing-instance-name {
    interface interface-name;
    routing-options {
      access {
        route prefix {
          next-hop next-hop;
          metric route-cost;
          preference route-distance;
          tag route-tag;
        }
      }
      access-internal {
        route subscriber-ip-address {
          qualified-next-hop underlying-interface {
            mac-address address;
          }
        }
      }
      multicast {
        interface interface-name {
          no-qos-adjust;
        }
      }
    }
    rib routing-table-name {
      access {
        route prefix {
          next-hop next-hop;
          metric route-cost;
          preference route-distance;
          tag route-tag;
        }
      }
      access-internal {
        route subscriber-ip-address {
          qualified-next-hop underlying-interface {
            mac-address address;
          }
        }
```

```
        }
      }
    }
    routing-options {
      access {
        route prefix {
          next-hop next-hop;
          metric route-cost;
          preference route-distance;
          tag route-tag;
        }
      }
      access-internal {
        route subscriber-ip-address {
          qualified-next-hop underlying-interface {
            mac-address address;
          }
        }
      }
      multicast {
        interface interface-name {
          no-qos-adjust;
        }
      }
    }
    variables {
      variable-name {
        default-value default-value;
        equals expression;
        mandatory;
        radius {
          vendor-id id {
            attribute attribute-number;
            tag tag-number;
          }
        }
        uid;
        uid-reference;
      }
    }
  }
}
```

Hierarchy Level [edit]

Release Information Statement introduced in Junos OS Release 9.2.
Support at the **filter, policer, hierarchical-policer, three-color-policer, and policy options** hierarchy levels introduced in Junos OS Release 11.4.

Description Create dynamic profiles for use with DHCP or PPP client access.

Options ***profile-name***—Name of the dynamic profile; string of up to 80 alphanumeric characters.

The remaining statements are explained separately.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Configuring a Basic Dynamic Profile*
- *Configuring Dynamic VLANs Based on Agent Circuit Identifier Information*
- *Dynamic Profiles Overview*

encapsulation (Dynamic Interfaces)

Syntax encapsulation (atm-ccc-cell-relay | atm-ccc-vc-mux | atm-cisco-nlpid | atm-tcc-vc-mux | atm-mlppp-llc | atm-nlpid | atm-ppp-llc | atm-ppp-vc-mux | atm-snap | atm-tcc-snap | atm-vc-mux | ether-over-atm-llc | ether-vpls-over-atm-llc | ether-vpls-over-fr | ether-vpls-over-ppp | ethernet | frame-relay-ccc | frame-relay-ppp | frame-relay-tcc | frame-relay-ether-type | frame-relay-ether-type-tcc | multilink-frame-relay-end-to-end | multilink-ppp | ppp-over-ether | ppp-over-ether-over-atm-llc | vlan-bridge | vlan-ccc | vlan-vci-ccc | vlan-tcc | vlan-vpls);

Hierarchy Level [edit dynamic-profiles *profile-name* interfaces *interface-name* unit *logical-unit-number*]

Release Information Statement introduced in Junos OS Release 10.4.

Description Dynamic interface configuration of the logical link-layer encapsulation type.

Options

atm-ccc-cell-relay—Use ATM cell-relay encapsulation.

atm-ccc-vc-mux—Use ATM virtual circuit (VC) multiplex encapsulation on circuit cross-connect (CCC) circuits. When you use this encapsulation type, you can configure the **ccc** family only.

atm-cisco-nlpid—Use Cisco ATM network layer protocol ID (NLPID) encapsulation. When you use this encapsulation type, you can configure the **inet** family only.

atm-mlppp-llc—For ATM2 IQ interfaces only, use Multilink Point-to-Point Protocol (MLPPP) over AAL5 LLC. For this encapsulation type, your router must be equipped with a link services or voice services PIC. MLPPP over ATM encapsulation is not supported on ATM2 IQ OC48 interfaces.

atm-nlpid—Use ATM NLPID encapsulation. When you use this encapsulation type, you can configure the **inet** family only.

atm-ppp-llc—For ATM2 IQ interfaces only, use PPP over AAL5 LLC encapsulation.

atm-ppp-vc-mux—For ATM2 IQ interfaces only, use PPP over ATM AAL5 multiplex encapsulation.

atm-snap—Use ATM subnetwork attachment point (SNAP) encapsulation.

atm-tcc-snap—Use ATM SNAP encapsulation on translational cross-connect (TCC) circuits.

atm-tcc-vc-mux—Use ATM VC multiplex encapsulation on TCC circuits. When you use this encapsulation type, you can configure the **tcc** family only.

atm-vc-mux—Use ATM VC multiplex encapsulation. When you use this encapsulation type, you can configure the **inet** family only.

ether-over-atm-llc—For interfaces that carry IPv4 traffic, use Ethernet over ATM LLC encapsulation. When you use this encapsulation type, you cannot configure multipoint interfaces.

ether-vpls-over-atm-llc—For ATM2 IQ interfaces only, use the Ethernet virtual private LAN service (VPLS) over ATM LLC encapsulation to bridge Ethernet interfaces and ATM interfaces over a VPLS routing instance (as described in RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*). Packets from the ATM interfaces are converted to standard ENET2/802.3 encapsulated Ethernet frames with the frame check sequence (FCS) field removed.

ether-vpls-over-fr—For E1, T1, E3, T3, and SONET interfaces only, use the Ethernet virtual private LAN service (VPLS) over Frame Relay encapsulation to support Bridged Ethernet over Frame Relay encapsulated TDM interfaces for VPLS applications, as per *Multiprotocol Interconnect over Frame Relay* (RFC 2427 [1490]).

ether-vpls-over-ppp—For E1, T1, E3, T3 and SONET interfaces only, use the Ethernet virtual private LAN service (VPLS) over PPP encapsulation to support Bridged Ethernet over PPP encapsulated TDM interfaces for VPLS applications.

ethernet—Use Ethernet II encapsulation (as described in RFC 894, *A Standard for the Transmission of IP Datagrams over Ethernet Networks*).

ethernet-vpls—Use Ethernet VPLS encapsulation on Ethernet interfaces that have VPLS enabled and that must accept packets carrying standard Tag Protocol ID (TPID) values.

extended-vlan-vpls—Use extended virtual LAN (VLAN) VPLS encapsulation on Ethernet interfaces that have VLAN 802.1Q tagging and VPLS enabled and that must accept packets carrying TPIDs 0x8100, 0x9100, and 0x9901.

NOTE: **The built-in Gigabit Ethernet PIC on an M7i router does not support extended VLAN VPLS encapsulation.**

frame-relay-ccc—Use Frame Relay encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only.

frame-relay-ppp—Use PPP over Frame Relay circuits. When you use this encapsulation type, you can configure the **ppp** family only. J Series routers do not support **frame-relay-ppp** encapsulation.

frame-relay-tcc—Use Frame Relay encapsulation on TCC circuits for connecting unlike media. When you use this encapsulation type, you can configure the **tcc** family only.

frame-relay-ether-type—Use Frame Relay ether type encapsulation for compatibility with Cisco Frame Relay. The physical interface must be configured with **flexible-frame-relay** encapsulation.

frame-relay-ether-type-tcc—Use Frame Relay ether type TCC for Cisco-compatible Frame Relay on TCC circuits to connect unlike media. The physical interface must be configured with **flexible-frame-relay** encapsulation.

multilink-frame-relay-end-to-end—Use MLFR FRF.15 encapsulation. This encapsulation is used only on multilink, link services,and voice services interfaces and their constituent T1 or E1 interfaces, and is supported on LSQ and redundant LSQ interfaces.

multilink-ppp—Use MLPPP encapsulation. This encapsulation is used only on multilink, link services, and voice services interfaces and their constituent T1 or E1 interfaces.

ppp-over-ether—For underlying Ethernet interfaces on J Series Services routers, use PPP over Ethernet encapsulation. When you use this encapsulation type, you cannot configure the interface address. Instead, configure the interface address on the PPP interface. You also use PPP over Ethernet encapsulation to configure an underlying Ethernet interface for a dynamic PPPoE logical interface on M120 and M320 Series routers with Intelligent Queuing 2 (IQ2) PICs, and on MX Series routers with MPCs.

ppp-over-ether-over-atm-llc—For underlying ATM interfaces on J Series Services routers only, use PPP over Ethernet over ATM LLC encapsulation. When you use this encapsulation type, you cannot configure the interface address. Instead, configure the interface address on the PPP interface.

vlan-bridge—Use Ethernet VLAN bridge encapsulation on Ethernet interfaces that have IEEE 802.1Q tagging, flexible ethernet services, and bridging enabled, and that must accept packets carrying TPID 0x8100 or a user-defined TPID.

vlan-ccc—Use Ethernet virtual LAN (VLAN) encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only.

vlan-vci-ccc—Use ATM-to-Ethernet interworking encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only.

vlan-tcc—Use Ethernet VLAN encapsulation on TCC circuits. When you use this encapsulation type, you can configure the **tcc** family only.

vlan-vpls—Use Ethernet VLAN encapsulation on VPLS circuits.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Configuring a Retail Dynamic Profile for Use in the Layer 2 Wholesale Solution on page 28
- *Junos OS Services Interfaces Library for Routing Devices*

encapsulation (Physical Interface)

Syntax encapsulation (atm-ccc-cell-relay | atm-pvc | cisco-hdlc | cisco-hdlc-ccc | cisco-hdlc-tcc | ethernet-bridge | ethernet-ccc | ethernet-over-atm | ethernet-tcc | ethernet-vpls | ethernet-vpls-fr | ether-vpls-over-atm-llc | ethernet-vpls-ppp |extended-frame-relay-ccc | extended-frame-relay-ether-type-tcc | extended-frame-relay-tcc | extended-vlan-bridge | extended-vlan-ccc | extended-vlan-tcc | extended-vlan-vpls | flexible-ethernet-services | flexible-frame-relay | frame-relay | frame-relay-ccc | frame-relay-ether-type | frame-relay-ether-type-tcc | frame-relay-port-ccc | frame-relay-tcc | generic-services | multilink-frame-relay-uni-nni | ppp | ppp-ccc | ppp-tcc | vlan-ccc | vlan-vci-ccc | vlan-vpls);

Hierarchy Level [edit interfaces *interface-name*],
[edit interfaces rlsq *number:number*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 11.1 for EX Series switches.
Statement introduced in Junos OS Release 12.1X48 for PTX Series Packet Transport Routers (**flexible-ethernet-services**, **ethernet-ccc**, and **ethernet-tcc** options only).

Description Specify the physical link-layer encapsulation type. Not all encapsulation types are supported on the switches. See the switch CLI.

Default **ppp**—Use serial PPP encapsulation.

Options **atm-ccc-cell-relay**—Use ATM cell-relay encapsulation.

atm-pvc—Use ATM PVC encapsulation.

cisco-hdlc—Use Cisco-compatible High-Level Data Link Control (HDLC) framing.

cisco-hdlc-ccc—Use Cisco-compatible HDLC framing on CCC circuits.

cisco-hdlc-tcc—Use Cisco-compatible HDLC framing on TCC circuits for connecting different media.

ethernet-bridge—Use Ethernet bridge encapsulation on Ethernet interfaces that have bridging enabled and that must accept all packets.

ethernet-ccc—Use Ethernet CCC encapsulation on Ethernet interfaces that must accept packets carrying standard Tag Protocol ID (TPID) values. For 8-port, 12-port, and 48-port Fast Ethernet PICs, CCC is not supported.

ethernet-over-atm—For interfaces that carry IPv4 traffic, use Ethernet over ATM encapsulation. When you use this encapsulation type, you cannot configure multipoint interfaces. As defined in RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*, this encapsulation type allows ATM interfaces to connect to devices that support only bridge protocol data units (BPDUs). Junos OS does not completely support bridging, but accepts BPDU packets as a default gateway. If you use the router as an edge device, then the router acts as a default gateway. It accepts Ethernet LLC/SNAP frames with IP or ARP in the payload, and drops the rest. For packets destined to the Ethernet LAN, a route lookup is done using the destination

IP address. If the route lookup yields a full address match, the packet is encapsulated with an LLC/SNAP and MAC header, and the packet is forwarded to the ATM interface.

ethernet-tcc—For interfaces that carry IPv4 traffic, use Ethernet TCC encapsulation on interfaces that must accept packets carrying standard TPID values. For 8-port, 12-port, and 48-port Fast Ethernet PICs, TCC is not supported.

ethernet-vpls—Use Ethernet VPLS encapsulation on Ethernet interfaces that have VPLS enabled and that must accept packets carrying standard TPID values. On M Series routers, except the M320 router, the 4-port Fast Ethernet TX PIC and the 1-port, 2-port, and 4-port, 4-slot Gigabit Ethernet PICs can use the Ethernet VPLS encapsulation type.

ethernet-vpls-fr—Use in a VPLS setup when a CE device is connected to a PE device over a time division multiplexing (TDM) link. This encapsulation type enables the PE device to terminate the outer layer 2 Frame Relay connection, use the 802.1p bits inside the inner Ethernet header to classify the packets, look at the MAC address from the Ethernet header, and use the MAC address to forward the packet into a given VPLS instance.

ethernet-vpls-ppp—Use in a VPLS setup when a CE device is connected to a PE device over a time division multiplexing (TDM) link. This encapsulation type enables the PE device to terminate the outer layer 2 PPP connection, use the 802.1p bits inside the inner Ethernet header to classify the packets, look at the MAC address from the Ethernet header, and use it to forward the packet into a given VPLS instance.

ether-vpls-over-atm-llc—For ATM intelligent queuing (IQ) interfaces only, use the Ethernet virtual private LAN service (VPLS) over ATM LLC encapsulation to bridge Ethernet interfaces and ATM interfaces over a VPLS routing instance (as described in RFC 2684, *Multiprotocol Encapsulation over ATM Adaptation Layer 5*). Packets from the ATM interfaces are converted to standard ENET2/802.3 encapsulated Ethernet frames with the frame check sequence (FCS) field removed.

extended-frame-relay-ccc—Use Frame Relay encapsulation on CCC circuits. This encapsulation type allows you to dedicate DLCIs 1 through 1022 to CCC.

extended-frame-relay-ether-type-tcc—Use extended Frame Relay ether type TCC for Cisco-compatible Frame Relay for DLCIs 1 through 1022. This encapsulation type is used for circuits with different media on either side of the connection.

extended-frame-relay-tcc—Use Frame Relay encapsulation on TCC circuits to connect different media. This encapsulation type allows you to dedicate DLCIs 1 through 1022 to TCC.

extended-vlan-bridge—Use extended VLAN bridge encapsulation on Ethernet interfaces that have IEEE 802.1Q VLAN tagging and bridging enabled and that must accept packets carrying TPID 0x8100 or a user-defined TPID.

extended-vlan-ccc—Use extended VLAN encapsulation on CCC circuits with Gigabit Ethernet and 4-port Fast Ethernet interfaces that must accept packets carrying 802.1Q values. For 8-port, 12-port, and 48-port Fast Ethernet PICs, extended VLAN CCC is not supported. For 4-port Gigabit Ethernet PICs, extended VLAN CCC is not supported.

extended-vlan-tcc—For interfaces that carry IPv4 traffic, use extended VLAN encapsulation on TCC circuits with Gigabit Ethernet interfaces on which you want to use 802.1Q tagging. For 4-port Gigabit Ethernet PICs, extended VLAN TCC is not supported.

extended-vlan-vpls—Use extended VLAN VPLS encapsulation on Ethernet interfaces that have VLAN 802.1Q tagging and VPLS enabled and that must accept packets carrying TPIDs 0x8100, 0x9100, and 0x9901. On M Series routers, except the M320 router, the 4-port Fast Ethernet TX PIC and the 1-port, 2-port, and 4-port, 4-slot Gigabit Ethernet PICs can use the Ethernet VPLS encapsulation type.

NOTE: **The built-in Gigabit Ethernet PIC on an M7i router does not support extended VLAN VPLS encapsulation.**

flexible-ethernet-services—For Gigabit Ethernet IQ interfaces and Gigabit Ethernet PICs with small form-factor pluggable transceivers (SFPs) (except the 10-port Gigabit Ethernet PIC and the built-in Gigabit Ethernet port on the M7i router), use flexible Ethernet services encapsulation when you want to configure multiple per-unit Ethernet encapsulations. Aggregated Ethernet bundles can use this encapsulation type. This encapsulation type allows you to configure any combination of route, TCC, CCC, Layer 2 virtual private networks (VPNs), and VPLS encapsulations on a single physical port. If you configure flexible Ethernet services encapsulation on the physical interface, VLAN IDs from 1 through 511 are no longer reserved for normal VLANs.

flexible-frame-relay—For IQ interfaces only, use flexible Frame Relay encapsulation when you want to configure multiple per-unit Frame Relay encapsulations. This encapsulation type allows you to configure any combination of TCC, CCC, and standard Frame Relay encapsulations on a single physical port. Also, each logical interface can have any DLCI value from 1 through 1022.

frame-relay—Use Frame Relay encapsulation.

frame-relay-ccc—Use Frame Relay encapsulation on CCC circuits.

frame-relay-ether-type—Use Frame Relay ether type encapsulation for compatibility with the Cisco Frame Relay.

frame-relay-ether-type-tcc—Use Frame Relay ether type TCC for Cisco-compatible Frame Relay on TCC circuits to connect different media.

frame-relay-port-ccc—Use Frame Relay port CCC encapsulation to transparently carry all the DLCIs between two customer edge (CE) routers without explicitly configuring each DLCI on the two provider edge (PE) routers with Frame Relay transport. When you use this encapsulation type, you can configure the **ccc** family only.

frame-relay-tcc—Use Frame Relay encapsulation on TCC circuits to connect different media.

generic-services—Use generic services encapsulation for services with a hierarchical scheduler.

multilink-frame-relay-uni-nni—Use MLFR UNI NNI encapsulation. This encapsulation is used on link services, voice services interfaces functioning as FRF.16 bundles, and their constituent T1 or E1 interfaces, and is supported on LSQ and redundant LSQ interfaces.

ppp—Use serial PPP encapsulation.

ppp-ccc—Use serial PPP encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only.

ppp-tcc—Use serial PPP encapsulation on TCC circuits for connecting different media. When you use this encapsulation type, you can configure the **tcc** family only.

vlan-ccc—Use Ethernet VLAN encapsulation on CCC circuits.

vlan-vci-ccc—Use ATM-to-Ethernet interworking encapsulation on CCC circuits. When you use this encapsulation type, you can configure the **ccc** family only. All logical interfaces configured on the Ethernet interface must also have the encapsulation type set to **vlan-vci-ccc**.

vlan-vpls—Use VLAN VPLS encapsulation on Ethernet interfaces with VLAN tagging and VPLS enabled. Interfaces with VLAN VPLS encapsulation accept packets carrying standard TPID values only. On M Series routers, except the M320 router, the 4-port Fast Ethernet TX PIC and the 1-port, 2-port, and 4-port, 4-slot Gigabit Ethernet PICs can use the Ethernet VPLS encapsulation type.

NOTE: **Label-switched interfaces (LSIs) do not support VLAN VPLS encapsulation. Therefore, you can only use VLAN VPLS encapsulation on a PE-router-to-CE-router interface and not a core-facing interface.**

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Configuring Interface Encapsulation on Physical Interfaces*
- *Configuring CCC Encapsulation for Layer 2 VPNs*
- *Configuring Layer 2 Switching Cross-Connects Using CCC*
- *Configuring TCC Encapsulation for Layer 2 VPNs and Layer 2 Circuits*
- *Configuring ATM Interface Encapsulation*
- *Configuring ATM-to-Ethernet Interworking*
- *Configuring VLAN Encapsulation*
- *Configuring Extended VLAN Encapsulation*
- Configuring Encapsulation for Layer 2 Wholesale VLAN Interfaces on page 33
- *Configuring Interfaces for Layer 2 Circuits*
- *Configuring Interface Encapsulation on PTX Series Packet Transport Routers*
- *Configuring an MPLS-Based Layer 2 VPN (CLI Procedure)*
- *Configuring MPLS LSP Tunnel Cross-Connects Using CCC*
- *Configuring TCC*
- *Configuring VPLS Interface Encapsulation*
- *Configuring Interfaces for VPLS Routing*
- *Defining the Encapsulation for Switching Cross-Connects*
- *Understanding Encapsulation on an Interface*

family (Dynamic Standard Interface)

Syntax

```
family family {
  access-concentrator name;
  address address;
  duplicate-protection;
  dynamic-profile profile-name;
  filter {
    adf {
      counter;
      input-precedence precedence;
      not-mandatory;
      output-precedence precedence;
      rule rule-value;
    }
    input filter-name {
      precedence precedence;
    }
    output filter-name {
      precedence precedence;
    }
  }
  mac-validate (loose | strict);
  max-sessions number;
  max-sessions-vsa-ignore;
  rpf-check {
    fail-filter filter-name;
    mode loose;
  }
  service {
    input {
      service-set service-set-name {
        service-filter filter-name;
      }
      post-service-filter filter-name;
    }
    output {
      service-set service-set-name {
        service-filter filter-name;
      }
    }
  }
  service-name-table table-name
  short-cycle-protection <lockout-time-min minimum-seconds lockout-time-max
    maximum-seconds>;
  unnumbered-address interface-name <preferred-source-address address>;
}
```

Hierarchy Level [edit dynamic-profiles *profile-name* interfaces *interface-name* unit *logical-unit-number*]

Release Information Statement introduced in Junos OS Release 9.2.
Option **pppoe** introduced in Junos OS Release 11.2.

Description Configure protocol family information for the logical interface.

NOTE: Not all subordinate stanzas are available to every protocol family.

Options

family—Protocol family:

- **inet**—IP version 4 suite
- **inet6**—IP version 6 suite
- **pppoe**—(MX Series routers with MPCs only) Point-to-Point Protocol over Ethernet
- **vpls**—Virtual private LAN service

The remaining statements are explained separately.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- For general information about configuring static interfaces, see the *Junos OS Network Interfaces Library for Routing Devices*.
- "Configuring the Protocol Family," in the *Junos OS Network Interfaces Library for Routing Devices*.

family

Syntax

```
family family {
    accounting {
        destination-class-usage;
        source-class-usage {
            (input | output | input output);
        }
    }
    access-concentrator name;
    address address {
        ... the address subhierarchy appears after the main [edit interfaces interface-name unit
            logical-unit-number family family-name] hierarchy ...
    }
    bridge-domain-type (bvlan | svlan);
    bundle interface-name;
    core-facing;
    demux-destination {
        destination-prefix;
    }
    demux-source {
        source-prefix;
    }
    duplicate-protection;
    dynamic-profile profile-name;
    filter {
        group filter-group-number;
        input filter-name;
        input-list [ filter-names ];
        output filter-name;
        output-list [ filter-names ];
    }
    interface-mode (access | trunk);
    ipsec-sa sa-name;
    isid-list all-service-groups;
    keep-address-and-control;
    mac-validate (loose | strict);
    max-sessions number;
    max-sessions-vsa-ignore;
    mtu bytes;
    multicast-only;
    negotiate-address;
    no-redirects;
    policer {
        arp policer-template-name;
        input policer-template-name;
        output policer-template-name;
    }
    primary;
    protocols [inet iso mpls];
    proxy inet-address address;
    receive-options-packets;
    receive-ttl-exceeded;
    remote (inet-address address | mac-address address);
```

```
rpf-check {
  fail-filter filter-name
  mode loose;
}
sampling {
  input;
  output;
}
service {
  input {
    post-service-filter filter-name;
    service-set service-set-name <service-filter filter-name>;
  }
  output {
    service-set service-set-name <service-filter filter-name>;
  }
}
service-name-table table-name
short-cycle-protection <lockout-time-min minimum-seconds lockout-time-max
  maximum-seconds>;
(translate-discard-eligible | no-translate-discard-eligible);
(translate-fecn-and-becn | no-translate-fecn-and-becn);
translate-plp-control-word-de;
unnumbered-address interface-name destination address destination-profile profile-name;
vlan-id number;
vlan-id-list [number number-number];
address address {
  arp ip-address (mac | multicast-mac) mac-address <publish>;
  broadcast address;
  destination address;
  destination-profile name;
  eui-64;
  master-only;
  multipoint-destination address dlci dlci-identifier;
  multipoint-destination address {
    epd-threshold cells;
    inverse-arp;
    oam-liveness {
      up-count cells;
      down-count cells;
    }
    oam-period (disable | seconds);
    shaping {
      (cbr rate | rtvbr burst length peak rate sustained rate | vbr burst length peak rate
        sustained rate);
      queue-length number;
    }
    vci vpi-identifier.vci-identifier;
  }
  preferred;
  primary;
  vrrp-groupgroup-id {
    (accept-data | no-accept-data);
    advertise-interval seconds;
    authentication-key key;
    authentication-type authentication;
```

```
        fast-interval milliseconds;
        (preempt | no-preempt) {
          hold-time seconds;
        }
        priority number;
        track {
          interface interface-name {
            bandwidth-threshold bits-per-second priority-cost priority;
            priority-cost priority;
          }
          priority-hold-time seconds;
          route prefix routing-instance instance-name priority-cost priority;
          }
        }
        virtual-address [ addresses ];
        }
      virtual-link-local-addressipv6-address;
    }
}
```

Hierarchy Level [edit interfaces *interface-name* unit *logical-unit-number*],
[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number*]

Release Information Statement introduced before Junos OS Release 7.4.
Option **max-sessions-vsa-ignore** introduced in Junos OS Release 11.4.

Description Configure protocol family information for the logical interface.

NOTE: Not all subordinate stanzas are available to every protocol family.

Options *family*—Protocol family:

- **any**—Protocol-independent family used for Layer 2 packet filtering

NOTE: This option is not supported on T4000 Type 5 FPCs.

- **ethernet-switching**—(M Series and T Series routers only) Configure only when the physical interface is configured with **ethernet-bridge** type encapsulation or when the logical interface is configured with **vlan-bridge** type encapsulation
- **ccc**—Circuit cross-connect protocol suite
- **inet**—Internet Protocol version 4 suite
- **inet6**—Internet Protocol version 6 suite
- **iso**—International Organization for Standardization Open Systems Interconnection (ISO OSI) protocol suite
- **mlfr-end-to-end**—Multilink Frame Relay FRF.15
- **mlfr-uni-nni**—Multilink Frame Relay FRF.16
- **multilink-ppp**—Multilink Point-to-Point Protocol
- **mpls**—Multiprotocol Label Switching (MPLS)
- **pppoe**—Point-to-Point Protocol over Ethernet
- **tcc**—Translational cross-connect protocol suite
- **tnp**—Trivial Network Protocol
- **vpls**—(M Series and T Series routers only) Virtual private LAN service

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Configuring the Protocol Family*
- *Example: Configuring E-LINE and E-LAN Services for a PBB Network on MX Series Routers*
- *Junos OS Services Interfaces Library for Routing Devices*

flexible-vlan-tagging

Syntax flexible-vlan-tagging;

Hierarchy Level [edit interfaces ge-*fpc/pic/port*],
[edit interfaces et-*fpc/pic/port*],
[edit interfaces ps0]

Release Information Statement introduced in Junos OS Release 8.1.
Support for aggregated Ethernet added in Junos OS Release 9.0.
Statement introduced in Junos OS Release 12.1x48 for PTX Series Packet Transport Routers.

Description Support simultaneous transmission of 802.1Q VLAN single-tag and dual-tag frames on logical interfaces on the same Ethernet port, and on pseudowire logical interfaces.

This statement is supported on M Series and T Series routers, for Fast Ethernet and Gigabit Ethernet interfaces only on Gigabit Ethernet IQ2 and IQ2-E, IQ, and IQE PICs, and for aggregated Ethernet interfaces with member links in IQ2, IQ2-E, and IQ PICs or in MX Series DPCs, or on Ethernet interfaces for PTX Series Packet Transport Routers or 100-Gigabit Ethernet Type 5 PIC with CFP.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Configuring Mixed Tagging*
- *Configuring Flexible VLAN Tagging on PTX Series Packet Transport Routers*

input-vlan-map (Dynamic Interfaces)

Syntax

```
input-vlan-map {
  inner-tag-protocol-id tpid;
  inner-vlan-id number;
  (push | swap);
  tag-protocol-id tpid;
  vlan-id number;
}
```

Hierarchy Level [edit dynamic-profiles *profile-name* interfaces *interface-name* unit *logical-unit-number*]

Release Information Statement introduced in Junos OS Release 10.4.

Description For dynamic interfaces, define the rewrite profile to be applied to incoming frames on this logical interface.

The statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Stacking and Rewriting VLAN Tags for the Layer 2 Wholesale Solution on page 29

instance-role

Syntax instance-role (access | nni);

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*], [edit routing-instances *routing-instance-name*]

Release Information Statement introduced in Junos OS Release 11.2.

Description Define the role of the routing instance in a Layer 2 Wholesale network.

Options

access—Defines the connectivity role of the routing instance in a Layer 2 Wholesale network as an access routing instance. When defined for this role, the same process occurs as in a Layer 3 Wholesale network—when the first packet is received from a given client, authentication for the client initiates with an external entity (for example, RADIUS). If authentication is successful, a logical interface is created with the appropriate outer and inner VLAN tags for that client.

nni—Defines the connectivity role of the routing instance in a Layer 2 Wholesale network as a network to network interface (NNI) routing instance. When defined for this role, only outer VLAN tags are learned. In addition, when the NNI routing instance receives a response from the ISP, the packets are forwarded to the appropriate client, provided the packet has the same two tags that were verified during authentication.

NOTE: If you connect an access node or MSAN device to a router participating in the Layer 2 Wholesale network in an NNI role, you must create a new routing instance of type **l2backhaul-vpn** with an instance role of type **access** for that connection.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Separate Access Routing Instances for Layer 2 Wholesale Service Retailers on page 35
- Configuring Separate NNI Routing Instances for Layer 2 Wholesale Service Retailers on page 38
- *Junos OS Subscriber Management and Services Library*

instance-type

Syntax instance-type *type*;

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*], [edit routing-instances *routing-instance-name*]

Release Information Statement introduced before Junos OS Release 7.4.
virtual-switch and **layer2-control** options introduced in Junos OS Release 8.4.
Statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.
evpn option introduced in Junos OS Release 13.2 for MX 3D Series routers.

Description Define the type of routing instance.

Options

NOTE: On ACX Series routers, you can configure only the forwarding, virtual router, and VRF routing instances.

type—Can be one of the following:

- **evpn**—(MX 3D Series routers only) Enable an Ethernet VPN (EVPN) on the routing instance. You cannot configure the **evpn** option under the **[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* instance-type]** hierarchy level.
- **forwarding**—Provide support for filter-based forwarding, where interfaces are not associated with instances. All interfaces belong to the default instance. Other instances are used for populating RPD learned routes. For this instance type, there is no one-to-one mapping between an interface and a routing instance. All interfaces belong to the default instance inet.0.
- **l2backhaul-vpn**—Provide support for Layer 2 wholesale VLAN packets with no existing corresponding logical interface. When using this instance, the router learns both the outer tag and inner tag of the incoming packets, when the **instance-role** statement is defined as **access**, or the outer VLAN tag only, when the **instance-role** statement is defined as **nni**.
- **l2vpn**—Enable a Layer 2 VPN on the routing instance. You must configure the **interface**, **route-distinguisher**, **vrf-import**, and **vrf-export** statements for this type of routing instance.
- **layer2-control**—(MX Series routers only) Provide support for RSTP or MSTP in customer edge interfaces of a VPLS routing instance. This instance type cannot be used if the customer edge interface is multihomed to two provider edge interfaces. If the customer edge interface is multihomed to two provider edge interfaces, use the default BPDU tunneling.

- **no-forwarding**—This is the default routing instance. Do not create a corresponding forwarding instance. Use this routing instance type when a separation of routing table information is required. There is no corresponding forwarding table. All routes are installed into the default forwarding table. IS-IS instances are strictly nonforwarding instance types.
- **virtual-router**—Enable a virtual router routing instance. This instance type is similar to a VPN routing and forwarding instance type, but used for non-VPN-related applications. You must configure the **interface** statement for this type of routing instance. You do not need to configure the **route-distinguisher**, **vrf-import**, and **vrf-export** statements.
- **virtual-switch**—(MX Series routers only) Provide support for Layer 2 bridging. Use this routing instance type to isolate a LAN segment with its Spanning Tree Protocol (STP) instance and to separate its VLAN identifier space.
- **vpls**—Enable VPLS on the routing instance. Use this routing instance type for point-to-multipoint LAN implementations between a set of sites in a VPN. You must configure the **interface**, **route-distinguisher**, **vrf-import**, and **vrf-export** statements for this type of routing instance.
- **vrf**—VPN routing and forwarding (VRF) instance. Provides support for Layer 3 VPNs, where interface routes for each instance go into the corresponding forwarding table only. Required to create a Layer 3 VPN. Create a VRF table (***instance-name*.inet.0**) that contains the routes originating from and destined for a particular Layer 3 VPN. For this instance type, there is a one-to-one mapping between an interface and a routing instance. Each VRF instance corresponds with a forwarding table. Routes on an interface go into the corresponding forwarding table. You must configure the **interface**, **route-distinguisher**, **vrf-import**, and **vrf-export** statements for this type of routing instance.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Example: Using Virtual Routing Instances to Route Among VLANs on EX Series Switches*
- *Configuring Routing Instances on PE Routers in VPNs*
- *Configuring EVPN Routing Instances*
- *Configuring Virtual Routing Instances (CLI Procedure)*
- *Configuring Virtual Router Routing Instances*
- *Example: Configuring Filter-Based Forwarding on the Source Address*
- *Example: Configuring Filter-Based Forwarding on Logical Systems*
- *Layer 2 Routing Instance Types*

interface (Dynamic Routing Instances)

Syntax interface *interface-name*;

Hierarchy Level [edit dynamic-profiles *profile-name*routing-instances *routing-instance-name*]

Release Information Statement introduced in Junos OS Release 9.6.

Description Assign the specified interface to the dynamically created routing instance.

Options ***interface-name***—The interface name variable (*$junos-interface-name*). The interface name variable is dynamically replaced with the interface the accessing client uses when connecting to the router.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- *[edit routing-instances] Hierarchy Level*
- *Configuring a Dynamic Profile for use by a Retailer in the DHCPv4 Solution*

interface (Routing Instances)

Syntax
```
interface interface-name {
  description text;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*], [edit routing-instances *routing-instance-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.2 for EX Series switches.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.
Statement introduced in Junos OS Release 13.2 for MX 3D Series routers.

Description Interface over which the VPN traffic travels between the PE device and CE device. You configure the interface on the PE device. If the value **vrf** is specified for the **instance-type** statement included in the routing instance configuration, this statement is required.

Options ***interface-name***—Name of the interface.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- *Configuring Routing Instances on PE Routers in VPNs*
- *Configuring EVPN Routing Instances*
- *Example: Configuring MPLS-Based Layer 3 VPNs on EX Series Switches*
- *interface (VPLS Routing Instances)*

interface-mac-limit

Syntax

```
interface-mac-limit limit {
    packet-action drop;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vpls site *site-name* interfaces *interface-name*],
[edit routing-instances *routing-instance-name* protocols evpn],
[edit routing-instances *routing-instance-name* protocols evpn interface *interface-name*],
[edit routing-instances *routing-instance-name* protocols vpls site *site-name* interfaces *interface-name*]

Release Information

Statement introduced before Junos OS Release 7.4.
Support for EVPNs introduced in Junos OS Release 13.2 on MX 3D Series routers.

Description

Specify the maximum number of media access control (MAC) addresses that can be learned by the EVPN or VPLS routing instance. You can configure the same limit for all interfaces configured for a routing instance. You can also configure a limit for a specific interface.

Options

limit—Specify the number of MAC addresses that can be learned from each interface.

Range: 16 through 65,536 MAC addresses

Default: 512 addresses

The remaining statement is explained separately.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Configuring EVPN Routing Instances*
- *Configuring VPLS Routing Instances*
- *interface*
- mac-table-size on page 86

interfaces (Static and Dynamic Subscribers)

Syntax

```
interfaces {
    interface-name {
        unit logical-unit-number {
            auto-configure {
                agent-circuit-identifier {
                    dynamic-profile profile-name;
                }
            }
            family family {
                access-concentrator name;
                address address;
                duplicate-protection;
                dynamic-profile profile-name;
                filter {
                    adf {
                        counter;
                        input-precedence precedence;
                        not-mandatory;
                        output-precedence precedence;
                        rule rule-value;
                    }
                    input filter-name (
                        precedence precedence;
                        shared-name filter-shared-name;
                    }
                    output filter-name {
                        precedence precedence;shared-name filter-shared-name;
                    }
                }
                max-sessions number;
                max-sessions-vsa-ignore;
                rpf-check {
                    mode loose;
                }
                service {
                    input {
                        service-set service-set-name {
                            service-filter filter-name;
                        }
                        post-service-filter filter-name;
                    }
                    output {
                        service-set service-set-name {
                            service-filter filter-name;
                        }
                    }
                }
                service-name-table table-name
                short-cycle-protection <lockout-time-min minimum-seconds lockout-time-max
                    maximum-seconds>;
                unnumbered-address interface-name <preferred-source-address address>;
            }
```

```
      filter {
        input filter-name;
        shared-name filter-shared-name;
        output filter-name;
        shared-name filter-shared-name;
      }
      ppp-options {
        chap;
        pap;
      }
      proxy-arp;
      vlan-id;
      vlan-tags outer [tpid].vlan-id [inner [tpid].vlan-id];
    }
    vlan-tagging;
  }
  interface-set interface-set-name {
    interface interface-name {
      unit logical unit number {
        advisory-options {
          downstream-rate rate;
          upstream-rate rate;
        }
      }
    }
    pppoe-underlying-options {
      max-sessions number;
    }
  }
  demux0 {
    unit logical-unit-number {
      demux-options {
        underlying-interface interface-name
      }
      family family {
        access-concentrator name;
        address address;
        duplicate-protection;
        dynamic-profile profile-name;
        demux-source {
          source-prefix;
        }
        filter{
          input filter-name (
            precedence precedence;
            shared-name filter-shared-name;
          }
          output filter-name {
            precedence precedence;
            shared-name filter-shared-name;
          }
        }
        mac-validate (loose | strict):
        max-sessions number;
        max-sessions-vsa-ignore;
        rpf-check {
```

```
            fail-filter filter-name;
            mode loose;
          }
          service-name-table table-name
          short-cycle-protection <lockout-time-min minimum-seconds lockout-time-max
            maximum-seconds>;
          unnumbered-address interface-name <preferred-source-address address>;
        }
        filter {
          input filter-name;
          output filter-name;
        }
        vlan-id number;
        vlan-tags outer [tpid].vlan-id [inner [tpid].vlan-id];
      }
    }
    pp0 {
      unit logical-unit-number {
        keepalives interval seconds;
        no-keepalives;
        pppoe-options {
          underlying-interface interface-name;
          server;
        }
        ppp-options {
          authentication [ authentication-protocols ];
          chap {
            challenge-length minimum minimum-length maximum maximum-length;
          }
          pap;
        }
        family inet {
          unnumbered-address interface-name;
          address address;
          service {
            input {
              service-set service-set-name {
                service-filter filter-name;
              }
              post-service-filter filter-name;
            }
            output {
              service-set service-set-name {
                service-filter filter-name;
              }
            }
          }
          filter {
            input filter-name {
              precedence precedence;
              shared-name filter-shared-name;
            }
            output filter-name {
              precedence precedence;
              shared-name filter-shared-name;
            }
```

```
        }
      }
    }
  }
}
```

Hierarchy Level [edit dynamic-profiles *profile-name*]

Release Information Statement introduced in Junos OS Release 9.2.

Description Define interfaces for dynamic profiles.

Options ***interface-name***—The interface variable (**$junos-interface-ifd-name**). The interface variable is dynamically replaced with the interface the DHCP client accesses when connecting to the router.

NOTE: **Though we do not recommend it, you can also enter the specific name of the interface you want to assign to the dynamic profile.**

The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Configuring Static Subscriber Interfaces in Dynamic Profiles*
- *Configuring Dynamic Subscriber Interfaces Using IP Demux Interfaces in Dynamic Profiles*
- *Configuring Dynamic PPPoE Subscriber Interfaces Using Dynamic Profiles*
- *Configuring Dynamic VLANs Based on Agent Circuit Identifier Information*
- *Subscriber Interface Overview*
- *Relationship Between Subscribers and Interfaces in an Access Network*
- For general information about configuring static interfaces, see the *Junos OS Network Interfaces Library for Routing Devices*
- For information about static IP demux interfaces, see the *Junos OS Network Interfaces Library for Routing Devices*

interfaces

Syntax interfaces { ... }

Hierarchy Level [edit]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure interfaces on the router or switch.

Default The management and internal Ethernet interfaces are automatically configured. You must configure all other interfaces.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Physical Interface Configuration Statements Overview*
- *Configuring Aggregated Ethernet Link Protection*

mac-table-size

Syntax

```
mac-table-size size {
  packet-action drop;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vpls],
[edit routing-instances *routing-instance-name* protocols evpn],
[edit routing-instances *routing-instance-name* protocols vpls]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 13.2 for EVPNs on MX 3D Series routers.

Description

Specify the size of the MAC address table.

Options

size—Specify the size of the MAC address table.

Range:

- (M Series and T Series routers only) 16 through 65,536 MAC addresses
- (MX Series routers only) 16 through 1,048,575 MAC addresses
- (T4000 routers with Type 5 FPCs only) 16 through 262,143 MAC addresses

NOTE: Before modifying the size of the MAC address table (to 262,143 addresses), you must enable network services mode by including the **enhanced-mode** statement at the **[edit chassis network-services]** hierarchy level and then reboot the router.

Default: 512 MAC addresses

The remaining statement is explained separately.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Configuring EVPN Routing Instances*
- *Configuring VPLS Routing Instances*
- *Configuring Improved VPLS MAC Address Learning on T4000 Routers with Type 5 FPCs*
- *enhanced-mode*
- *evpn*

no-local-switching

Syntax no-local-switching

Hierarchy Level [edit vlans *vlan-name*]

Release Information Statement introduced in Junos OS Release 9.3 for EX Series switches.

Description Specify that access ports in this VLAN domain do not forward packets to each other. You use this statement with primary VLANs and isolated secondary VLANs.

Required Privilege Level system—To view this statement in the configuration.
system–control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring a Private VLAN on a Single EX Series Switch*
- *Creating a Private VLAN on a Single EX Series Switch (CLI Procedure)*

no-tunnel-services

Syntax no-tunnel-services;

Hierarchy Level [edit logical-systems *logical-system-name* protocols vpls static-vpls],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vpls],
[edit protocols vpls static-vpls],
[edit routing-instances *routing-instance-name* protocols vpls]

Release Information Statement introduced in Junos OS Release 7.6.
Support for static VPLS added in Junos OS Release 10.2.

Description Configure VPLS on a router without a Tunnel Services PIC. Configuring the **no-tunnel-services** statement creates a label-switched interface (LSI) to provide VPLS functionality. An LSI MPLS label is used as the inner label for VPLS. This label maps to a VPLS routing instance. On the PE router, the LSI label is stripped and then mapped to a logical LSI interface. The Layer 2 Ethernet frame is then forwarded using the LSI interface to the correct VPLS routing instance.

NOTE: In VPLS documentation, the word *Router* in terms such as *PR Router* is used to refer to any device that provides routing functions.

Label-switched interfaces configured with the **no-tunnel-services** statement are not supported with GRE tunnels.

NOTE: Although visible in the CLI, the **no-tunnel-services** statement is not supported at the **[edit logical-systems *logical-system-name* protocols vpls static-vpls]** and the **[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vpls]** hierarchy levels.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Configuring VPLS Without a Tunnel Services PIC*
- *Configuring Static Pseudowires for VPLS*
- *Configuring EXP-Based Traffic Classification for VPLS*

output-vlan-map (Dynamic Interfaces)

Syntax

```
output-vlan-map {
  inner-tag-protocol-id tpid;
  inner-vlan-id number;
  (pop | swap);
  tag-protocol-id tpid;
  vlan-id number;
}
```

Hierarchy Level [edit dynamic-profiles *profile-name* interfaces *interface-name* unit *logical-unit-number*]

Release Information Statement introduced in Junos OS Release 10.4.

Description For dynamic interfaces, define the rewrite profile to be applied to outgoing frames on this logical interface.

The statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Stacking and Rewriting VLAN Tags for the Layer 2 Wholesale Solution on page 29

pop (Dynamic VLANs)

Syntax pop;

Hierarchy Level [edit dynamic-profiles *profile-name* interfaces *interface-name* unit *logical-unit-number* output-vlan-map]

Release Information Statement introduced in Junos OS Release 10.4.

Description For dynamic VLAN interfaces, specify the VLAN rewrite operation to remove a VLAN tag from the top of the VLAN tag stack. The outer VLAN tag of the frame is removed.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Removing a VLAN Tag*
- Stacking and Rewriting VLAN Tags for the Layer 2 Wholesale Solution on page 29

profile (Access)

Syntax

```
profile profile-name {
  accounting {
    address-change-immediate-update
    accounting-stop-on-access-deny;
    accounting-stop-on-failure;
    coa-immediate-update;
    coa-no-override service-class-attribute;
    duplication;
    duplication-vrf {
      access-profile-name profile-name;
      vrf-name vrf-name;
    }
    immediate-update;
    order [ accounting-method ];
    send-acct-status-on-config-change;
    statistics (time | volume-time);
    update-interval minutes;
    wait-for-acct-on-ack;
    }
  authentication-order [ authentication-methods ];
  client client-name {
    chap-secret chap-secret;
    group-profile profile-name;
    ike {
      allowed-proxy-pair {
        remote remote-proxy-address local local-proxy-address;
      }
      pre-shared-key (ascii-text character-string | hexadecimal hexadecimal-digits);
      ike-policy policy-name;
      interface-id string-value;
    }
    l2tp {
      aaa-access-profile profile-name;
      interface-id interface-id;
      lcp-renegotiation;
      local-chap;
      maximum-sessions-per-tunnel number;
      multilink {
        drop-timeout milliseconds;
        fragment-threshold bytes;
      }
      ppp-authentication (chap | pap);
      ppp-profile profile-name;
      shared-secret shared-secret;
    }
    pap-password pap-password;
    ppp {
      cell-overhead;
      encapsulation-overhead bytes;
      framed-ip-address ip-address;
      framed-pool framed-pool;
      idle-timeout seconds;
```

```
        interface-id interface-id;
        keepalive seconds;
        primary-dns primary-dns;
        primary-wins primary-wins;
        secondary-dns secondary-dns;
        secondary-wins secondary-wins;
      }
      user-group-profile profile-name;
    }
    domain-name-server;
    domain-name-server-inet;
    domain-name-server-inet6;
    provisioning-order (gx-plus | jsrc);
    radius {
      accounting-server [ ip-address ];
      authentication-server [ ip-address ];
      options {
        accounting-session-id-format (decimal | description);
        calling-station-id-delimiter delimiter-character;
        calling-station-id-format {
          agent-circuit-id;
          agent-remote-id;
          interface-description;
          nas-identifier;
        }
        client-accounting-algorithm (direct | round-robin);
        client-authentication-algorithm (direct | round-robin);
        coa-dynamic-variable-validation;
        ethernet-port-type-virtual;
        interface-description-format {
          exclude-adapter;
          exclude-sub-interface;
        }
        juniper-dsl-attributes;
        nas-identifier identifier-value;
        nas-port-extended-format {
          adapter-width width;
          ae-width width;
          port-width width;
          slot-width width;
          stacked-vlan-width width;
          vlan-width width;
          atm {
            adapter-width width;
            port-width width:
            slot-width width;
            vci-width width:
            vpi-width width;
          }
        }
        nas-port-id-delimiter delimiter-character;
        nas-port-id-format {
          agent-circuit-id;
          agent-remote-id;
          interface-description;
          nas-identifier;
```

```
        }
        nas-port-type {
          ethernet {
            port-type;
          }
        }
        revert-interval interval;
        vlan-nas-port-stacked-format;
      }
      attributes {
        exclude {
          ...
        }
        ignore {
          framed-ip-netmask;
          input-filter;
          logical-system:routing-instance;
          output-filter;
        }
      }
    }
    radius-server server-address {
      accounting-port port-number;
      port port-number;
      retry attempts;
      routing-instance routing-instance-name;
      secret password;
      max-outstanding-requests value;
      source-address source-address;
      timeout seconds;
    }
    service {
      accounting-order (activation-protocol | radius);
    }
    session-options {
      client-group [ group-names ];
      client-idle-timeout minutes;
      client-session-timeoutminutes;
    }
}
```

Hierarchy Level [edit access]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure PPP CHAP, or a profile and its subscriber access, L2TP, or PPP properties.

Options ***profile-name***—Name of the profile.

For CHAP, the name serves as the mapping between peer identifiers and CHAP secret keys. This entity is queried for the secret key whenever a CHAP challenge or response is received.

The remaining statements are explained separately.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- *Configuring the PPP Authentication Protocol*
- *Configuring Access Profiles for L2TP or PPP Parameters*
- *Configuring L2TP Properties for a Client-Specific Profile*
- *Configuring an L2TP LNS with Inline Service Interfaces*
- *Configuring PPP Properties for a Client-Specific Profile*
- *Configuring Service Accounting with JSRC*
- *AAA Service Framework Overview*
- show network-access aaa statistics on page 134
- *clear network-access aaa statistics*

protocols

Syntax

```
protocols {
    bgp {
        ... bgp-configuration ...
    }
    isis {
        ... isis-configuration ...
    }
    ldp {
        ... ldp-configuration ...
    }
    msdp {
        ... msdp-configuration ...
    }
    mstp {
        ... mstp-configuration ...
    }
    ospf {
        domain-id domain-id;
        domain-vpn-tag number;
        route-type-community (iana | vendor);
        ... ospf-configuration ...
    }
    ospf3 {
        domain-id domain-id;
        domain-vpn-tag number;
        route-type-community (iana | vendor);
        ... ospf3-configuration ...
    }
    pim {
        ... pim-configuration ...
    }
    rip {
        ... rip-configuration ...
    }
    ripng {
        ... ripng-configuration ...
    }
    rstp {
        rstp-configuration;
    }
    vstp {
        vstp configuration;
    }
    vpls {
        vpls configuration;
    }
}
```

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*], [edit routing-instances *routing-instance-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Support for RIPng introduced in Junos OS Release 9.0.
Statement introduced in Junos OS Release 11.1 for EX Series switches.
Statement introduced in Junos OS Release 11.3 for the QFX Series.

Description Specify the protocol for a routing instance. You can configure multiple instances of many protocol types. Not all protocols are supported on the switches. See the switch CLI.

Options

bgp—Specify BGP as the protocol for a routing instance.

isis—Specify IS-IS as the protocol for a routing instance.

ldp—Specify LDP as the protocol for a routing instance.

l2vpn—Specify Layer 2 VPN as the protocol for a routing instance.

msdp—Specify the Multicast Source Discovery Protocol (MSDP) for a routing instance.

mstp—Specify the Multiple Spanning Tree Protocol (MSTP) for a virtual switch routing instance.

ospf—Specify OSPF as the protocol for a routing instance.

ospf3—Specify OSPF version 3 (OSPFv3) as the protocol for a routing instance.

NOTE: **OSPFv3 supports the no-forwarding, virtual-router, and vrf routing instance types only.**

pim—Specify the Protocol Independent Multicast (PIM) protocol for a routing instance.

rip—Specify RIP as the protocol for a routing instance.

ripng—Specify RIP next generation (RIPng) as the protocol for a routing instance.

rstp—Specify the Rapid Spanning Tree Protocol (RSTP) for a virtual switch routing instance.

vstp—Specify the VLAN Spanning Tree Protocol (VSTP) for a virtual switch routing instance.

vpls—Specify VPLS as the protocol for a routing instance.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring Multiple Routing Instances of OSPF*

push (Dynamic VLANs)

Syntax push;

Hierarchy Level [edit dynamic-profiles *profile-name* interfaces *interface-name* unit *logical-unit-number* input-vlan-map]

Release Information Statement introduced in Junos OS Release 10.4.

Description For dynamic VLAN interfaces, specify the VLAN rewrite operation to add a new VLAN tag to the top of the VLAN stack. An outer VLAN tag is pushed in front of the existing VLAN tag. If you include the **push** statement in the configuration, you must also include the *pop* statement at the **[edit** dynamic-profiles ***profile-name*** interfaces ***interface-name*** unit ***logical-unit-number*** output-vlan-map**]** hierarchy level.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- Stacking and Rewriting VLAN Tags for the Layer 2 Wholesale Solution on page 29

radius (Access Profile)

Syntax

```
radius {
    accounting-server [ ip-address ];
    attributes {
        exclude
            ...
        }
        ignore {
            framed-ip-netmask;
            input-filter;
            logical-system-routing-instance;
            output-filter;
        }
    }
    authentication-server [ ip-address ];
    options {
        accounting-session-id-format (decimal | description);
        calling-station-id-delimiter delimiter-character;
        calling-station-id-format {
            agent-circuit-id;
            agent-remote-id;
            interface-description;
            nas-identifier;
        }
        client-accounting-algorithm (direct | round-robin);
        client-authentication-algorithm (direct | round-robin);
        coa-dynamic-variable-validation;
        ethernet-port-type-virtual;
        interface-description-format {
            exclude-adapter;
            exclude-sub-interface;
        }
        ip-address-change-notify message;
        juniper-dsl-attributes;
        nas-identifier identifier-value;
        nas-port-extended-format {
            adapter-width width;
            ae-width width;
            port-width width;
            slot-width width;
            stacked-vlan-width width;
            vlan-width width;
            atm {
                adapter-width width;
                port-width width:
                slot-width width;
                vci-width width:
                vpi-width width;
            }
        }
        nas-port-id-delimiter delimiter-character;
        nas-port-id-format {
            agent-circuit-id;
```

```
        agent-remote-id;
        interface-description;
        nas-identifier;
      }
      nas-port-type {
        ethernet {
          port-type;
        }
      }
      revert-interval interval;
      vlan-nas-port-stacked-format;
    }
}
```

Hierarchy Level [edit access profile *profile-name*]

Release Information Statement introduced in Junos OS Release 9.1.
Statement introduced in Junos OS Release 9.1 for EX Series switches.

Description Configure the RADIUS parameters that the router uses for AAA authentication and accounting for subscribers.

The remaining statements are explained separately.

Required Privilege Level admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Related Documentation

- *Configuring RADIUS Server Parameters for Subscriber Access*
- *RADIUS Server Options for Subscriber Access*

radius-server

Syntax

```
radius-server server-address {
    accounting-port port-number;
    port port-number;
    retry attempts;
    routing-instance routing-instance-name;
    secret password;
    max-outstanding-requests value;
    source-address source-address;
    timeout seconds;
}
```

Hierarchy Level

[edit access],
[edit access profile *profile-name*]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description

Configure RADIUS for subscriber access management, L2TP, or PPP.

To configure multiple RADIUS servers, include multiple **radius-server** statements. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.

Options

server-address—Address of the RADIUS authentication server.

The remaining statements are explained separately.

Required Privilege Level

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

Related Documentation

- *Configuring RADIUS Authentication for L2TP*
- *Configuring the PPP Authentication Protocol*
- *Configuring RADIUS Authentication*
- *Configuring Authentication and Accounting Parameters for Subscriber Access*
- *Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure)*
- show network-access aaa statistics on page 134
- *clear network-access aaa statistics*

ranges (Dynamic VLAN)

Syntax ranges (any | *low-tag*)-(any | *high-tag*);

Hierarchy Level [edit interfaces *interface-name* auto-configure vlan-ranges dynamic-profile *profile-name*]

Release Information Statement introduced in Junos OS Release 9.5.

Description Configure VLAN ranges for dynamic, auto-sensed VLANs.

Options **any**—The entire VLAN range.

low-tag—The lower limit of the VLAN range.

high-tag—The upper limit of the VLAN range.
Range: 1 through 4094

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Configuring Single-Level VLAN Ranges for Use with VLAN Dynamic Profiles*

route-distinguisher

Syntax route-distinguisher (*as-number:id* | *ip-address:id*);

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols l2vpn mesh-group *mesh-group-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vpls mesh-group *mesh-group-name*],
[edit routing-instances *routing-instance-name*],
[edit routing-instances *routing-instance-name* protocols l2vpn mesh-group *mesh-group-name*],
[edit routing-instances *routing-instance-name* protocols vpls mesh-group *mesh-group-name*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 11.1 for EX Series switches.
Support at **[edit routing-instances *routing-instance-name* protocols vpls mesh-group *mesh-group-name*]** hierarchy level introduced in Junos OS Release 11.2.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.
Support at **[edit routing-instances *routing-instance-name* protocols l2vpn mesh-group *mesh-group-name*]** hierarchy level introduced in Junos OS Release 13.2.

Description Specify an identifier attached to a route, enabling you to distinguish to which VPN or VPLS the route belongs. Each routing instance must have a unique route distinguisher associated with it. The route distinguisher is used to place bounds around a VPN so that the same IP address prefixes can be used in different VPNs without having them overlap. If the instance type is **vrf**, the **route-distinguisher** statement is required.

For Layer 2 VPNs and VPLS, if you configure the **l2vpn-use-bgp-rules** statement, you must configure a unique route distinguisher for each PE router participating in the routing instance.

For other types of VPNs, we recommend that you use a unique route distinguisher for each PE router participating in specific routing instance. Although you can use the same route distinguisher on all PE routers for the same VPN routing instance, if you use a unique route distinguisher, you can determine the CE router from which a route originated within the VPN.

For Layer 2 VPNs and VPLS, if you configure mesh groups, the route distinguisher in each mesh group must be unique.

CAUTION: We strongly recommend that if you change a route distinguisher that has already been configured, make the change during a maintenance window, as follows:

1. Deactivate the routing instance.
2. Change the route distinguisher.
3. Activate the routing instance.

This is not required if you are configuring the route distinguisher for the first time.

Options

as-number:number*—*as-number is an assigned AS number, and ***number*** is any 2-byte or 4-byte value. The AS number can be from 1 through 4,294,967,295. If the AS number is a 2-byte value, the administrative number is a 4-byte value. If the AS number is 4-byte value, the administrative number is a 2-byte value. A route distinguisher consisting of a 4-byte AS number and a 2-byte administrative number is defined as a type 2 route distinguisher in RFC 4364 *BGP/MPLS IP Virtual Private Networks (VPNs)*.

NOTE: In Junos OS Release 9.1 and later, the numeric range for AS numbers is extended to provide BGP support for 4-byte AS numbers, as defined in RFC 4893, *BGP Support for Four-octet AS Number Space*. All releases of Junos OS support 2-byte AS numbers. To configure a route distinguisher that includes a 4-byte AS number, append the letter "L" to the end of the AS number. For example, a route distinguisher with the 4-byte AS number 7,765,000 and an administrative number of 1,000 is represented as 77765000L:1000.

In Junos OS Release 9.2 and later, you can also configure a 4-byte AS number using the AS dot notation format of two integer values joined by a period: <*16-bit high-order value in decimal*>.<*16-bit low-order value in decimal*>. For example, the 4-byte AS number of 65,546 in the plain-number format is represented as 1.10 in AS dot notation format.

ip-address*:*id—IP address (***ip-address*** is a 4-byte value) within your assigned prefix range and a 2-byte value for the ***id***. The IP address can be any globally unique unicast address.

Range: 0 through 4,294,967,295 ($2^{32} - 1$). If the router you are configuring is a BGP peer of a router that does not support 4-byte AS numbers, you need to configure a local AS number. For more information, see *Using 4-Byte Autonomous System Numbers in BGP Networks Technology Overview*.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring BGP Route Target Filtering for VPNs*
- *Example: Configuring FEC 129 BGP Autodiscovery for VPWS*
- *Configuring EVPN Routing Instances*
- *Configuring Routing Instances on PE Routers in VPNs*
- *Configuring an MPLS-Based Layer 2 VPN (CLI Procedure)*
- *Configuring an MPLS-Based Layer 3 VPN (CLI Procedure)*
- *l2vpn-use-bgp-rules*

routing-instances

Syntax

```
routing-instances routing-instance-name {
  interface interface-name;
  routing-options {
    access {
      route prefix {
        metric route-cost;
        next-hop next-hop;
        preference route-distance;
        tag route-tag;
      }
    }
    access-internal {
      route subscriber-ip-address {
        qualified-next-hop underlying-interface {
          mac-address address;
        }
      }
    }
    multicast {
      interface interface-name {
        no-qos-adjust;
      }
    }
    rib routing-table-name {
      access {
        route prefix {
          metric route-cost;
          next-hop next-hop;
          preference route-distance;
          tag route-tag;
        }
      }
      access-internal {
        route subscriber-ip-address {
          qualified-next-hop underlying-interface {
            mac-address address;
          }
        }
      }
    }
  }
}
```

Hierarchy Level [edit dynamic-profiles]

Release Information Statement introduced in Junos OS Release 9.6.
The **routing-options** statement introduced in Junos OS Release 10.1.

Description Dynamically configure an additional routing entity for a router.

Options

routing-instance-name—The routing instance variable (*$junos-routing-instance*). The routing instance variable is dynamically replaced with the routing instance the accessing client uses when connecting to the router.

NOTE: Though we do not recommend it, you can also enter a specific name for the routing instance, a maximum of 31 characters.

The remaining statement is explained separately.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

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

routing-instances (Multiple Routing Entities)

Syntax routing-instances *routing-instance-name* { ... }

Hierarchy Level [edit],
[edit logical-systems *logical-system-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure an additional routing entity for a router. You can create multiple instances of BGP, IS-IS, OSPF, OSPFv3, and RIP for a router. You can also create multiple routing instances for separating routing tables, routing policies, and interfaces for individual wholesale subscribers (retailers) in a Layer 3 wholesale network.

Each routing instance consist of the following:

- A set of routing tables
- A set of interfaces that belong to these routing tables
- A set of routing option configurations

Each routing instance has a unique name and a corresponding IP unicast table. For example, if you configure a routing instance with the name **my-instance**, its corresponding IP unicast table is my-instance.inet.0. All routes for **my-instance** are installed into my-instance.inet.0.

Routes are installed into the default routing instance inet.0 by default, unless a routing instance is specified.

In Junos OS Release 9.0 and later, you can no longer specify a routing-instance name of *master*, *default*, or *bgp* or include special characters within the name of a routing instance.

In Junos OS Release 9.6 and later, you can include a slash (/) in a routing-instance name only if a logical system is not configured. That is, you cannot include the slash character in a routing-instance name if a logical system other than the default is explicitly configured. Routing-instance names, further, are restricted from having the form __.*__ (beginning and ending with underscores). The colon **:** character cannot be used when multitopology routing (MTR) is enabled.

Default Routing instances are disabled for the router.

Options ***routing-instance-name***—Name of the routing instance. This must be a non-reserved string of not more than 128 characters.

The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Example: Configuring Interprovider Layer 3 VPN Option A*
- *Example: Configuring Interprovider Layer 3 VPN Option B*
- *Example: Configuring Interprovider Layer 3 VPN Option C*
- *Example: Configuring E-LINE and E-LAN Services for a PBB Network on MX Series Routers*

secret

Syntax secret *password*;

Hierarchy Level [edit access profile *profile-name* radius-server *server-address*],
[edit access radius-disconnect *client-address*],
[edit access radius-server *server-address*]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the password to use with the RADIUS server. The secret password used by the local router or switch must match that used by the server.

Options ***password***—Password to use; it can include spaces if the character string is enclosed in quotation marks.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation

- *Configuring Authentication and Accounting Parameters for Subscriber Access*
- *Configuring Router or Switch Interaction with RADIUS Servers*
- *Example: Configuring CHAP Authentication with RADIUS*
- *Configuring RADIUS Authentication for L2TP*
- *Configuring the RADIUS Disconnect Server for L2TP*
- *Configuring an EX Series Switch to Use Junos Pulse Access Control Service for Network Access Control (CLI Procedure)*

site (VPLS Multihoming for FEC 128)

Syntax

```
site site-name {
    active-interface (any | primary interface-name);
    best-site;
    interface interface-name {
        interface-mac-limit limit;
    }
    mesh-group mesh-group-name;
    multi-homing;
    site-identifier identifier;
    site-preference preference-value;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vpls],
[edit routing-instances *routing-instance-name* protocols vpls]

Release Information

Statement introduced before Junos OS Release 7.4.

Description

Specify the site name and site identifier for a site. Allows you to configure a remote site ID for remote sites.

Options

site-name—Name of the site.

The remaining statements are explained separately.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Configuring VPLS Routing Instances*

site-identifier (VPLS)

Syntax site-identifier *identifier*;

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vpls site *site-name*],
[edit routing-instances *routing-instance-name* protocols vpls site *site-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify the numerical identifier for the local VPLS site.

Options ***identifier***—Specify the numerical identifier for the local VPLS site. The identifier must be an unsigned 16-bit number greater than zero.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- *Configuring VPLS Routing Instances*

site-range

Syntax site-range *number*;

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vpls],
[edit routing-instances *routing-instance-name* protocols vpls]

Release Information Statement introduced before Junos OS Release 7.4.

Description Specify an upper limit on the maximum site identifier that can be accepted to allow a pseudowire to be brought up. Pseudowires cannot be established to sites with site identifiers greater than the configured site range. If you issue the **show vpls connections** command, such sites are displayed as OR (out of range). You must specify a value from 1 through 65,534. We recommend using the default.

Default 65,534

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation
- *Configuring VPLS Routing Instances*

unit (Dynamic Profiles Standard Interface)

Syntax

```
unit logical-unit-number {
  auto-configure {
    agent-circuit-identifier {
      dynamic-profile profile-name;
    }
  }
  dial-options {
    ipsec-interface-id name;
    l2tp-interface-id name;
    (shared | dedicated);
  }
  encapsulation (atm-ccc-cell-relay | atm-ccc-vc-mux | atm-cisco-nlpid | atm-tcc-vc-mux
    | atm-mlppp-llc | atm-nlpid | atm-ppp-llc | atm-ppp-vc-mux | atm-snap | atm-tcc-snap
    | atm-vc-mux | ether-over-atm-llc | ether-vpls-over-atm-llc | ether-vpls-over-fr |
    ether-vpls-over-ppp | ethernet | frame-relay-ccc | frame-relay-ppp | frame-relay-tcc |
    frame-relay-ether-type | frame-relay-ether-type-tcc | multilink-frame-relay-end-to-end
    | multilink-ppp | ppp-over-ether | ppp-over-ether-over-atm-llc | vlan-bridge | vlan-ccc |
    vlan-vci-ccc | vlan-tcc | vlan-vpls);
  family family {
    access-concentrator name;
    address address;
    duplicate-protection;
    dynamic-profile profile-name;
    filter {
      adf {
        counter;
        input-precedence precedence;
        not-mandatory;
        output-precedence precedence;
        rule rule-value;
      }
      input filter-name (
        precedence precedence;
      }
      output filter-name {
        precedence precedence;
      }
    }
    max-sessions number;
    max-sessions-vsa-ignore;
    rpf-check {
      fail-filter filter-name;
      mode loose;
    }
    service {
      input {
        service-set service-set-name {
          service-filter filter-name;
        }
        post-service-filter filter-name;
      }
      input-vlan-map {
```

```
            inner-tag-protocol-id tpid;
            inner-vlan-id number;
            (push | swap);
            tag-protocol-id tpid;
            vlan-id number;
          }
          output {
            service-set service-set-name {
              service-filter filter-name;
            }
          }
          output-vlan-map {
            inner-tag-protocol-id tpid;
            inner-vlan-id number;
            (pop | swap);
            tag-protocol-id tpid;
            vlan-id number;
          }
        }
        service-name-table table-name
        short-cycle-protection <lockout-time-min minimum-seconds lockout-time-max
          maximum-seconds>;
        unnumbered-address interface-name <preferred-source-address address>;
        filter {
          input filter-name;
          output filter-name;
        }
        keepalives {
          interval seconds;
          }
        ppp-options {
          chap;
          pap;
        }
        vlan-id number;
        vlan-tags outer [tpid].vlan-id [inner [tpid].vlan-id];
      }
    }
```

Hierarchy Level [edit dynamic-profiles *profile-name* interfaces *interface-name*]

Release Information Statement introduced in Junos OS Release 9.2.

Description Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.

Options

logical-unit-number—The specific unit number of the interface you want to assign to the dynamic profile, or one of the following Junos OS predefined variables:

- **$junos-underlying-interface-unit**—For static VLANs, the unit number variable. The static unit number variable is dynamically replaced with the client unit number when the client session begins. The client unit number is specified by the DHCP when it accesses the subscriber network.
- **$junos-interface-unit**—The unit number variable on a dynamic underlying VLAN interface for which you want to enable the creation of dynamic VLAN subscriber interfaces based on agent circuit identifier information.

The remaining statements are explained separately.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Configuring Dynamic Underlying VLAN Interfaces to Use Agent Circuit Identifier Information*
- *Configuring Static Underlying VLAN Interfaces to Use Agent Circuit Identifier Information*
- *Agent Circuit Identifier-Based Dynamic VLANs Components Overview*

unit

Syntax

```
unit logical-unit-number {
  accept-source-mac {
    mac-address mac-address {
      policer {
        input cos-policer-name;
        output cos-policer-name;
      }
    }
  }
  accounting-profile name;
  advisory-options {
    downstream-rate rate;
    upstream-rate rate;
  }
  allow-any-vci;
  atm-scheduler-map (map-name | default);
  backup-options {
    interface interface-name;
  }
  bandwidth rate;
  cell-bundle-size cells;
  clear-dont-fragment-bit;
  compression {
    rtp {
      maximum-contexts number <force>;
      f-max-period number;
      queues [ queue-numbers ];
      port {
        minimum port-number;
        maximum port-number;
      }
    }
  }
  compression-device interface-name;
  copy-tos-to-outer-ip-header;
  demux-destination family;
  demux-source family;
  demux-options {
    underlying-interface interface-name;
  }
  description text;
  interface {
    l2tp-interface-id name;
    (dedicated | shared);
  }
  dialer-options {
    activation-delay seconds;
    callback;
    callback-wait-period time;
    deactivation-delay seconds;
    dial-string [ dial-string-numbers ];
    idle-timeout seconds;
```

```
    incoming-map {
      caller caller-id) | accept-all;
      initial-route-check seconds;
      load-interval seconds;
      load-threshold percent;
      pool pool-name;
      redial-delay time;
      watch-list {
        [ routes ];
      }
    }
  }
  disable;
  disable-mlppp-inner-ppp-pfc;
  dlci dlci-identifier;
  drop-timeout milliseconds;
  dynamic-call-admission-control {
    activation-priority priority;
    bearer-bandwidth-limit kilobits-per-second;
  }
  encapsulation type;
  epd-threshold cells plp1 cells;
  family family-name {
    ... the family subhierarchy appears after the main [edit interfaces interface-name unit
      logical-unit-number] hierarchy ...
  }
  fragment-threshold bytes;
  inner-vlan-id-range start start-id end end-id;
  input-vlan-map {
    (pop | pop-pop | pop-swap | push | push-push | swap |
    swap-push | swap-swap);
    inner-tag-protocol-id tpid;
    inner-vlan-id number;
    tag-protocol-id tpid;
    vlan-id number;
  }
  interleave-fragments;
  inverse-arp;
  layer2-policer {
    input-policer policer-name;
    input-three-color policer-name;
    output-policer policer-name;
    output-three-color policer-name;
  }
  link-layer-overhead percent;
  minimum-links number;
  mrru bytes;
  multicast-dlci dlci-identifier;
  multicast-vci vpi-identifier.vci-identifier;
  multilink-max-classes number;
  multipoint;
  oam-liveness {
    up-count cells;
    down-count cells;
  }
  oam-period (disable | seconds);
```

```
output-vlan-map {
  (pop | pop-pop | pop-swap | push | push-push | swap |
  swap-push | swap-swap);
  inner-tag-protocol-id tpid;
  inner-vlan-id number;
  tag-protocol-id tpid;
  vlan-id number;
}
passive-monitor-mode;
peer-unit unit-number;
plp-to-clp;
point-to-point;
ppp-options {
  chap {
    access-profile name;
    default-chap-secret name;
    local-name name;
    passive;
  }
  compression {
    acfc;
    pfc;
  }
  dynamic-profile profile-name;
  lcp-restart-timer milliseconds;
  loopback-clear-timer seconds;
  ncp-restart-timer milliseconds;
  pap {
    access-profile name;
    default-pap-password password;
    local-name name;
    local-password password;
    passive;
  }
}
pppoe-options {
  access-concentrator name;
  auto-reconnect seconds;
  (client | server);
  service-name name;
  underlying-interface interface-name;
}
pppoe-underlying-options {
  access-concentrator name;
  dynamic-profile profile-name;
  max-sessions number;
}
proxy-arp;
service-domain (inside | outside);
shaping {
  (cbr rate | rtvbr peak rate sustained rate burst length | vbr peak rate sustained rate burst
    length);
  queue-length number;
}
short-sequence;
targeted-distribution;
```

```
transmit-weight number;
(traps | no-traps);
trunk-bandwidth rate;
trunk-id number;
tunnel {
  backup-destination address;
  destination address;
  key number;
  routing-instance {
    destination routing-instance-name;
  }
  source source-address;
  ttl number;
}
vci vpi-identifier.vci-identifier;
vci-range start start-vci end end-vci;
vpi vpi-identifier;
vlan-id number;
vlan-id-range number-number;
vlan-tags inner tpid.vlan-id outer tpid.vlan-id;
family family {
  accounting {
    destination-class-usage;
    source-class-usage {
      (input | output | input output);
    }
  }
  access-concentrator name;
  address address {
    ... the address subhierarchy appears after the main [edit interfaces interface-name unit
      logical-unit-number family family-name] hierarchy ...
  }
  bridge-domain-type (bvlan | svlan);
  bundle interface-name;
  core-facing;
  demux-destination {
    destination-prefix;
  }
  demux-source {
    source-prefix;
  }
  duplicate-protection;
  dynamic-profile profile-name;
  filter {
    group filter-group-number;
    input filter-name;
    input-list [ filter-names ];
    output filter-name;
    output-list [ filter-names ];
  }
  interface-mode (access | trunk);
  ipsec-sa sa-name;
  isid-list all-service-groups;
  keep-address-and-control;
  mac-validate (loose | strict);
  max-sessions number;
```

```
mtu bytes;
multicast-only;
no-redirects;
policer {
  arp policer-template-name;
  input policer-template-name;
  output policer-template-name;
}
primary;
protocols [inet iso mpls];
proxy inet-address address;
receive-options-packets;
receive-ttl-exceeded;
remote (inet-address address | mac-address address);
rpf-check {
  fail-filter filter-name
  mode loose;
}
sampling {
  input;
  output;
}
service {
  input {
    post-service-filter filter-name;
    service-set service-set-name <service-filter filter-name>;
  }
  output {
    service-set service-set-name <service-filter filter-name>;
  }
}
service-name-table table-name
(translate-discard-eligible | no-translate-discard-eligible);
(translate-fecn-and-becn | no-translate-fecn-and-becn);
translate-plp-control-word-de;
unnumbered-address interface-name destination address destination-profile profile-name;
vlan-id number;
vlan-id-list [number number-number];
address address {
  arp ip-address (mac | multicast-mac) mac-address <publish>;
  broadcast address;
  destination address;
  destination-profile name;
  eui-64;
  master-only;
  multipoint-destination address {
    dlci dlci-identifier;
    epd-threshold cells <plp1 cells>;
    inverse-arp;
    oam-liveness {
      up-count cells;
      down-count cells;
    }
    oam-period (disable | seconds);
    shaping {
```

```
            (cbr rate | rtvbr burst length peak rate sustained rate | vbr burst length peak rate
              sustained rate);
            queue-length number;
          }
          vci vpi-identifier.vci-identifier;
        }
        preferred;
        primary;
        (vrrp-group | vrrp-inet6-group) group-number {
          (accept-data | no-accept-data);
          advertise–interval seconds;
          authentication-type authentication;
          authentication-key key;
          fast-interval milliseconds;
          (preempt | no-preempt) {
            hold-time seconds;
          }
          priority number;
          track {
            interface interface-name {
              bandwidth-threshold bits-per-second priority-cost number;
            }
            priority-hold-time seconds;
            route ip-address/prefix-length routing-instance instance-name priority-cost cost;
          }
          virtual-address [ addresses ];
          virtual-link-local-address ipv6–address;
          vrrp-inherit-from {
            active-interface interface-name;
            active-group group-number;
          }
        }
      }
    }
  }
}
```

Hierarchy Level [edit interfaces *interface-name*],
[edit logical-systems *logical-system-name* interfaces *interface-name*],
[edit interfaces interface-set *interface-set-name* interface *interface-name*]

Release Information Statement introduced before Junos OS Release 7.4.

Description Configure a logical interface on the physical device. You must configure a logical interface to be able to use the physical device.

Options ***logical-unit-number***—Number of the logical unit.

Range: 0 through 1,073,741,823 for demux and PPPoE static interfaces only. 0 through 16,385 for all other static interface types.

The remaining statements are explained separately.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Configuring Logical Interface Properties*
- *Example: Configuring E-LINE and E-LAN Services for a PBB Network on MX Series Routers*
- *Junos OS Services Interfaces Library for Routing Devices*

vlan-id (Dynamic VLANs)

Syntax vlan-id *number*;

Hierarchy Level [edit dynamic-profiles *profile-name* interfaces *interface-name* unit *logical-unit-number* input-vlan-map],
[edit dynamic-profiles *profile-name* interfaces *interface-name* unit *logical-unit-number* output-vlan-map]

Release Information Statement introduced in Junos OS Release 10.4.

Description For dynamic VLAN interfaces, specify the line VLAN identifiers to be rewritten at the input or output interface.

You cannot include the **vlan-id** statement with the **swap** statement, **swap-push** statement, **push-push** statement, or **push-swap** statement at the **[edit** dynamic-profiles ***profile-name*** interfaces ***interface-name*** unit ***logical-unit-number*** output-vlan-map**]** hierarchy level. If you include any of those statements in the output VLAN map, the VLAN ID in the outgoing frame is rewritten to the **vlan-id** statement that you include at the **[edit** dynamic-profiles ***profile-name*** interfaces ***interface-name*** unit ***logical-unit-number***] hierarchy level.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Rewriting the VLAN Tag on Tagged Frames*
- *Binding VLAN IDs to Logical Interfaces*

vlan-model

Syntax vlan-model one-to-one;

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*], [edit routing-instances *routing-instance-name*]

Release Information Statement introduced in Junos OS Release 11.2.

Description Define the network VLAN model.

Options **one-to-one**—Specify that any received, dual-tagged VLAN packet triggers the provisioning process in a Layer 2 Wholesale network. Using this option, the router learns VLAN tags for each individual client. The router learns both the outer tag and inner tag of the incoming packets, when the **instance-role** statement is defined as **access**, or the outer VLAN tag only, when the **instance-role** statement is defined as **nni**.

Required Privilege Level routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- Configuring Separate Access Routing Instances for Layer 2 Wholesale Service Retailers on page 35
- Configuring Separate NNI Routing Instances for Layer 2 Wholesale Service Retailers on page 38
- *Junos OS Subscriber Management and Services Library*

vlan-ranges

Syntax

```
vlan-ranges {
  access-profile profile-name;
  authentication {
    password password-string;
    username-include {
      circuit-type;
      delimiter delimiter-character;
      domain-name domain-name-string;
      interface-name;
      mac-address;
      option-82 <circuit-id> <remote-id>;
      radius-realm radius-realm-string;
      user-prefix user-prefix-string;
    }
  }
  dynamic-profile profile-name {
    accept (any | dhcp-v4 | inet);
    ranges (any | low-tag)–(any | high-tag);
  }
  override;
}
```

Hierarchy Level [edit interfaces *interface-name* auto-configure]

Release Information Statement introduced in Junos OS Release 9.5.

Description Configure multiple VLANs. Each VLAN is assigned a VLAN ID number from the range.

The remaining statements are explained separately.

Required Privilege Level routing—To view this statement in the configuration.
routing–control—To add this statement to the configuration.

Related Documentation

- *Configuring Single-Level VLAN Ranges for Use with VLAN Dynamic Profiles*
- *Configuring Dynamic Mixed VLAN Ranges*

vlan-tags

Syntax vlan-tags outer [*tpid*].*vlan-id* [inner [*tpid*].*vlan-id*];

Hierarchy Level [edit dynamic-profiles *profile-name* interfaces *interface-name* unit *logical-unit-number*]

Release Information Statement introduced in Junos OS Release 9.5.
VLAN demux interface support introduced in Junos OS Release 10.2.

Description For Gigabit Ethernet IQ and IQE interfaces only, binds TPIDs and 802.1Q VLAN tag IDs to a logical interface. You must include the **stacked-vlan-tagging** statement at the **[edit interfaces *interface-name*]** hierarchy level.

NOTE: The inner-range *vid1–vid2* option is supported on MX Series routers with IQE PICs only.

Options

inner [*tpid*].*vlan-id*—A TPID (optional) and a valid VLAN identifier in the format *tpid*.*vlan-id*. When used in the **dynamic-profiles** hierarchy, specify the **$junos-vlan-id** predefined variable to dynamically obtain the VLAN ID.

Range: For VLAN ID, 1 through 4094. VLAN ID 0 is reserved for tagging the priority of frames.

outer [*tpid*].*vlan-id*—A TPID (optional) and a valid VLAN identifier in the format *tpid*.*vlan-id*. When used in the **dynamic-profiles** hierarchy, specify the **$junos-stacked-vlan-id** predefined variable.

Range: For VLAN ID, 1 through 511 for normal interfaces, and 512 through 4094 for VLAN CCC interfaces. VLAN ID 0 is reserved for tagging the priority of frames.

Required Privilege Level interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Related Documentation

- *Configuring Dual VLAN Tags*
- *stacked-vlan-tagging*

vpls (Routing Instance)

Syntax

```
vpls {
  active-interface {
    any;
    primary interface-name;
  }
  community COMM;
  connectivity-type (ce | irb);
  encapsulation-type ethernet;
  ignore-encapsulation-mismatch;
  ignore-mtu-mismatch;
  interface interface-name;
  interface-mac-limit limit;
  label-block-size size;
  mac-flush [ explicit-mac-flush-message-options ];
  mac-table-aging-time time;
  mac-table-size size;
  mesh-group mesh-group-name {
    l2vpn-id (as-number:id | ip-address:id);
    local-switching;
    mac-flush [ explicit-mac-flush-message-options ];
    neighbor address {...}
    peer-as all;
    pseudowire-status-tlv;
    route-distinguisher (as-number:id | ip-address:id);
    vpls-id number;
    vrf-export [ policy-names ];
    vrf-import [ policy-names ];
    vrf-target {
      community;
      import community-name;
      export community-name;
    }
  }
  mtu mtu;
  no-tunnel-services;
  site site-name {
    active-interface interface-name {
      any;
      primary preference-value;
    }
    best-site;
    interface interface-name {
      interface-mac-limit limit;
    }
    mesh-group mesh-group-name;
    multi-homing;
    site-identifier identifier;
    site-preference preference-value {
      backup;
      primary;
    }
  }
```

```
    site-range number;
    traceoptions {
      file filename <files number> <size size> <world-readable | no-world-readable>;
      flag flag <flag-modifier> <disable>;
    }
    tunnel-services {
      devices device-names;
      primary primary-device-name;
    }
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols],
[edit routing-instances *routing-instance-name* protocols]

Release Information

Statement introduced before Junos OS Release 7.4. The **mac-flush** option was added in Junos OS Release 10.0.

Description

Configure a virtual private LAN service (VPLS) routing instance.

The remaining statements are explained separately.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Configuring VPLS Routing Instances*

vrf-target

Syntax

```
vrf-target {
    community;
    import community-name;
    export community-name;
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name*],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols l2vpn mesh-group *mesh-group-name*]
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* protocols vpls mesh-group *mesh-group-name*]
[edit routing-instances *routing-instance-name*],
[edit routing-instances *routing-instance-name* protocols l2vpn mesh-group *mesh-group-name*]
[edit routing-instances *routing-instance-name* protocols vpls mesh-group *mesh-group-name*]

Release Information

Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 11.1 for EX Series switches.
Statement introduced in Junos OS Release 12.3 for ACX Series routers.

Description

Specify a VRF target community. If you configure the ***community*** option only, default VRF import and export policies are generated that accept and tag routes with the specified target community. The purpose of the **vrf-target** statement is to simplify the configuration by allowing you to configure most statements at the **[edit routing-instances]** hierarchy level. In effect, this statement configures a single policy for import and a single policy for export to replace the per-VRF policies for every community.

You can still create more complex policies by explicitly configuring VRF import and export policies using the **import** and **export** options.

Options

community—Community name.

import *community-name*—Allowed communities accepted from neighbors.

export *community-name*—Allowed communities sent to neighbors.

Required Privilege Level

routing—To view this statement in the configuration.
routing-control—To add this statement to the configuration.

Related Documentation

- *Configuring Policies for the VRF Table on PE Routers in VPNs*
- *Example: Configuring FEC 129 BGP Autodiscovery for VPWS*

CHAPTER 7

Broadband Subscriber Management Layer 2 Wholesale Network Configuration Examples

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 on page 19
- Layer 2 Wholesale Network Topology Overview on page 26

- Configuring a Retail Dynamic Profile for Use in the Layer 2 Wholesale Solution on page 28

Example: Access Interface for a Layer 2 Wholesale Network

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

Related Documentation

- Layer 2 and Layer 3 Wholesale Overview on page 19
- Layer 2 Wholesale Network Topology Overview on page 26
- Configuring VLAN Interfaces for the Layer 2 Wholesale Solution on page 32

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

```
routing-instances {
  Retailer_Instance1 {
    vlan-model one-to-one;
    instance-role access;
    instance-type l2backhaul-vpn;
    interface ge-1/1/0.0
    no-local-switching;
    route-distinguisher 10.10.1.1:1;
    vrf-target target:100:1;
    protocols {
      vpls {
        site-range 10;
        mac-table-size {
          6000;
        }
        interface-mac-limit {
          2000;
        }
        no-tunnel-services;
        site A-PE {
          site-identifier 1;
        }
      }
```

```
    }
  }
  Retailer_Instance2 {
    vlan-model one-to-one;
    instance-role access;
    instance-type l2backhaul-vpn;
    interface ge-2/2/0.0
    no-local-switching;
    route-distinguisher 10.10.1.1:2;
    vrf-target target:300:1;
    protocols {
      vpls {
        site-range 1000;
        no-tunnel-services;
        site A-PE {
          site-identifier 1;
        }
      }
    }
  }
}
```

Related Documentation

- Layer 2 and Layer 3 Wholesale Overview on page 19
- Layer 2 Wholesale Network Topology Overview on page 26
- Configuring Separate Access Routing Instances for Layer 2 Wholesale Service Retailers on page 35

Example: Retailer NNI ISP-Facing Interfaces for a Layer 2 Wholesale Network

```
interfaces {
  ge-1/1/0 {
  description Retailer 1 NNI ISP-facing interface;
  encapsulation ethernet-vpls;
  unit 0{
}
interfaces {
  ge-2/2/0 {
  description Retailer 2 NNI ISP-facing interface;
  encapsulation ethernet-vpls;
  unit 0;
}
```

Related Documentation

- Layer 2 and Layer 3 Wholesale Overview on page 19
- Layer 2 Wholesale Network Topology Overview on page 26
- Configuring Separate NNI Routing Instances for Layer 2 Wholesale Service Retailers on page 38

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

```
interfaces {
```

```
    ge-1/1/0 {
    description Retailer 1 Direct ISP-facing interface;
    encapsulation ethernet-vpls;
    unit 1
      family vpls {
        core-facing;
      }
    }
}
```

Related Documentation

- Layer 2 and Layer 3 Wholesale Overview on page 19
- Layer 2 Wholesale Network Topology Overview on page 26
- Configuring Direct ISP-Facing Interfaces for the Layer 2 Wholesale Solution on page 34

PART 3

Administration

CHAPTER 8

Subscriber Management AAA CLI Commands

show network-access aaa statistics

Syntax

show network-access aaa statistics
<accounting>
<address-assignment (client | pool *pool-name*)>
<dynamic-requests>
<radius>

Release Information

Command introduced in Junos OS Release 9.1.
Option **address-assignment** introduced in Junos OS Release 10.0.
Option **radius** introduced in Junos OS Release 11.4.

Description

Display AAA accounting, address-assignment, dynamic request statistics, and RADIUS settings and statistics.

Options

accounting—(Optional) Display AAA accounting statistics.

address-assignment (client | pool *pool-name*)—(Optional) Display AAA address-assignment client and pool statistics.

dynamic-requests—(Optional) Display AAA dynamic requests.

radius— (Optional) Display RADIUS settings and statistics.

Required Privilege Level

view

Related Documentation

- *Verifying and Managing Subscriber AAA Information*

List of Sample Output

show network-access aaa statistics accounting on page 136
show network-access aaa statistics address-assignment client on page 136
show network-access aaa statistics address-assignment pool on page 136
show network-access aaa statistics dynamic-requests on page 136
show network-access aaa statistics radius on page 136

Output Fields

Table 8 on page 134 lists the output fields for the **show network-access aaa statistics** command. Output fields are listed in the approximate order in which they appear.

Table 8: show network-access aaa statistics Output Fields

Field Name	Field Description
Requests received	• Number of accounting requests generated by the AAA framework. • Number of dynamic requests received from the external server.
Accounting Response failures	Number of accounting requests not acknowledged (NAK) by the accounting server.
Accounting Response Success	Number of accounting requests acknowledged by the accounting server.

Table 8: show network-access aaa statistics Output Fields *(continued)*

Field Name	Field Description
Requests timedout	Number of accounting requests to the accounting server that timed out.
Client	Client type; for example, DHCP, Mobile IP, PPP.
Out of Memory	Number of times an address was not given to the client due to memory issues.
No Matches	Number of times there were no network matches for the pool.
Pool Name	Name of the address-assignment pool for this client.
Out of Addresses	Number of times there were no available addresses in the pool.
Address total	Number of addresses in the pool.
Addresses in use	Number of addresses in use.
Address Usage (percent)	Percentage of total addresses in use.
processed successfully	Number of dynamic requests processed successfully by the AAA framework.
errors during processing	Number of dynamic requests that resulted in processing errors by the AAA framework.
Link Name	Name of the secondary address-assignment pool to which the primary pool is linked.
Pool Usage	Percentage of allocated addresses in the specified address pool.
silently dropped	Number of dynamic requests dropped by the AAA framework due to multiple back-to-back or duplicate requests.
RADIUS Server	IP address of the RADIUS server to which the router is sending requests.
Profile	Name of the RADIUS profile associated with the RADIUS server. A RADIUS server can be associated with more than one RADIUS profile.
Configured	Configured maximum number of outstanding requests from the router to the RADIUS server for a specific profile. An outstanding request is a request to which the RADIUS server has not yet responded. The range of values is 0 through 2000 outstanding requests. The default value is 1000.
Current	Current number of outstanding requests from the router to the RADIUS server for a specific profile. An outstanding request is a request to which the RADIUS server has not yet responded.
Peak	Highest number of outstanding requests from the router to the RADIUS server for a specific profile at any point in time since the router was started or since the counter was last cleared. NOTE: If the value of this field is equal to the value of the **Configured** field, you may want to increase the value of the **Configured** field.

Table 8: show network-access aaa statistics Output Fields *(continued)*

Field Name	Field Description
Exceeded	Number of times that the router attempted to send requests to the RADIUS server in excess of the configured maximum value for a specific profile. NOTE: If the value of this field is nonzero, you may want to increase the value of the **Configured** field.

Sample Output

show network-access aaa statistics accounting

```
user@host> show network-access aaa statistics accounting
Accounting module statistics
  Requests received: 0
  Accounting Response failures: 0
  Accounting Response Success: 0
  Requests timedout: 0
```

show network-access aaa statistics address-assignment client

```
user@host> show network-access aaa statistics address-assignment client
Address-assignment statistics
 Client: jdhcpd
 Out of Memory: 0
 No Matches: 2
```

show network-access aaa statistics address-assignment pool

```
user@host> show network-access aaa statistics address-assignment pool isp_1
Address-assignment statistics
 Pool Name: isp_1
 Pool Name: (all pools in chain)
 Out of Memory: 0
 Out of Addresses: 9
 Address total: 47
 Addresses in use: 47
 Address Usage (percent): 100
```

show network-access aaa statistics dynamic-requests

```
user@host> show network-access aaa statistics dynamic-requests
requests received: 0
processed successfully: 0
errors during processing: 0
silently dropped: 0
```

show network-access aaa statistics radius

```
user@host> show network-access aaa statistics radius
Outstanding Requests
RADIUS Server     Profile      Configured   Current   Peak   Exceeded
172.28.32.239     prof1        1000         0         1000   14
                  prof2        500          17        432    0
171.27.82.211     myprof       200          0         200    27
12.1.11.254     pppoe-auth     111          0         1      0
```

show network-access aaa statistics authentication

Syntax **show network-access aaa statistics authentication <detail>**

Release Information Command introduced in Junos OS Release 9.1.
Option **detail** introduced in Junos OS Release 12.1.

Description Display AAA authentication statistics.

Options **detail**—(Optional) Displays detailed information about authentication.

Required Privilege Level view

Related Documentation
- *Verifying and Managing Subscriber AAA Information*

List of Sample Output
show network-access aaa statistics authentication on page 139
show network-access aaa statistics authentication detail on page 139

Output Fields Table 9 on page 137 lists the output fields for the **show network-access aaa statistics authentication** command. Output fields are listed in the approximate order in which they appear.

Table 9: show network-access aaa statistics authentication Output Fields

Field Name	Field Description	Level of Output
Requests received	Number of authentication requests received from clients.	All levels
Multistack requests	Number of authentication requests for dual-stack subscribers.	All levels
Accepts	Number of authentication requests accepted by the authentication server.	All levels
Rejects	Number of authentication requests rejected by the authentication server.	All levels
Challenges	Number of authentication requests challenged by the authentication server.	All levels
Requests timed out	Number of authentication requests that timed out.	All levels
RADIUS authentication failures	Number of RADIUS authentication requests that have failed.	Detail
Queue request deleted	Number of queue requests that have been deleted.	Detail

Table 9: show network-access aaa statistics authentication Output Fields *(continued)*

Field Name	Field Description	Level of Output
Malformed reply	Number of malformed replies received from the RADIUS authentication server.	Detail
No server configured	Number of authentication requests that failed because no authentication server is configured.	Detail
Access Profile configuration not found	Number of authentication requests that failed because no access profile is configured.	Detail
Unable to create client record	Number of times that the router is unable to create the client record for the authentication request.	Detail
Unable to create client request	Number of times that the router is unable to create the client request for the authentication request.	Detail
Unable to build authentication request	Number of times that the router is unable to build the authentication request.	Detail
No server found	Number of requests to the authentication server that have timed out; the server is then considered to be down.	Detail
Unable to create handle	Number of authentication requests that have failed because of an internal allocation failure.	Detail
Unable to queue request	Number of times the router was unable to queue the request to the authentication server.	Detail
Invalid credentials	Number of times the router did not have proper authorization to access the authentication server.	Detail
Malformed request	Number of times the router request to the authentication server is malformed.	Detail
License unavailable	Number of times the router did not have a license to access the authentication server.	Detail
Redirect requested	Number of authentication requests that have been redirected based on routing instance.	Detail
Internal failure	Number of internal failures.	Detail
Local authentication failures	Number of times local authentication failed.	Detail
LDAP lookup failures	Number of times the LDAP lookup operation failed.	Detail

Sample Output

show network-access aaa statistics authentication

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

show network-access aaa statistics authentication detail

```
user@host> show network-access aaa statistics authentication detail
Authentication module statistics
  Requests received: 2118
  Multistack requests: 0
  Accepts: 261
  Rejects: 975
    RADIUS authentication failures: 975
      Queue request deleted: 0
      Malformed reply: 0
      No server configured: 0
      Access Profile configuration not found: 0
      Unable to create client record: 0
      Unable to create client request: 0
      Unable to build authentication request: 0
      No server found: 975
      Unable to create handle: 0
      Unable to queue request: 0
      Invalid credentials: 0
      Malformed request: 0
      License unavailable: 0
      Redirect requested: 0
      Internal failure: 0
    Local authentication failures: 0
    LDAP lookup failures: 0
  Challenges: 0
  Requests timed out: 882
```

show network-access aaa subscribers

Syntax

show network-access aaa subscribers
<logical-system *logical-system-name*>
<routing-instance *routing-instance-name*>
<statistics>
<username>

Release Information

Command introduced in Junos OS Release 9.1.

Description

Display subscriber-specific AAA statistics.

Options

logical-system *logical-system-name*—(Optional) List subscribers in the specific logical system.

routing-instance *routing-instance-name*—(Optional) List subscribers for the specific routing instance. If you do not specify a routing instance name, the default routing instance is assumed.

statistics—(Optional) Display statistics for the subscriber events.

username—(Optional) Display information for the specified subscriber.

Required Privilege Level

view

Related Documentation

- *Verifying and Managing Subscriber AAA Information*

List of Sample Output

show network-access aaa subscribers logical-system on page 141
show network-access aaa subscribers logical-system routing-instance on page 141
show network-access aaa subscribers statistics username on page 142
show network-access aaa subscribers username on page 142

Output Fields

Table 10 on page 140 lists the output fields for the **show network-access aaa subscribers** command. Output fields are listed in the approximate order in which they appear.

Table 10: show network-access aaa subscribers Output Fields

Field Name	Field Description
Challenge requests	Number of authentication requests challenged by the authentication server for this subscriber.
Challenge responses	Number of challenge responses sent by the subscriber to the authentication server.
START sent successfully	Number of accounting start requests generated by the AAA framework for this subscriber.
START send failures	Number of accounting start requests that failed to make it to the accounting server for this subscriber.
START ack received	Number of accounting start requests acknowledged by the accounting server for this subscriber.

Table 10: show network-access aaa subscribers Output Fields *(continued)*

Field Name	Field Description
INTERIM sent successfully	Number of accounting interim requests generated by the AAA framework for this subscriber.
INTERIM send failures	Number of accounting interim requests that failed to make it to the accounting server for this subscriber.
INTERIM ack received	Number of accounting interim requests acknowledged by the accounting server for this subscriber.
Requests received	Number of reauthentication requests received by the authentication server.
Successful responses	Number of successful reauthentication requests granted by the authentication server.
Aborts handled	Number of reauthentication requests aborted by the authentication server.
Service name	Name of the subscriber service.
Creation requests	Number of requests to create the service.
Deletion requests	Number of requests to delete the service.
Request timeouts	Number of times the service request was timed out.
Client type	Type of client; for example, DHCP, Mobile IP, PPP.
Session-ID	ID of the subscriber session.
Session uptime	How long the session has been up, in *HH:MM:SS*.
Accounting	Status of accounting, and type of accounting if accounting is on.

Sample Output

show network-access aaa subscribers logical-system

```
user@host> show network-access aaa subscribers logical-system
Username            Client type    Logical system/Routing instance
cbenson@addr.net    ppp            default
00010e020304.1231   dhcp           isp-bos-metro-12:isp-cmbrg-12
conley@isp3.com     dhcp           default:isp-gtown-r3-00
0020df980102.2334   dhcp           isp-bos-metro-16:isp-cmbrg-12
```

show network-access aaa subscribers logical-system routing-instance

```
user@host> show network-access aaa subscribers logical-system isp-bos-metro-16
routing-instance isp-cmbrg-12-32
Username            Client type   Logical system/Routing instance
00010e020304.1231   dhcp          isp-bos-metro-12:isp-cmbrg-12
conley@isp3.com     dhcp          default:isp-gtown-r3-00
0020df980102.2334   dhcp          isp-bos-metro-16:isp-cmbrg-12
```

show network-access aaa subscribers statistics username

```
user@host> show network-access aaa subscribers statistics username 00010e020304.1231
Authentication statistics
   Challenge requests: 0
   Challenge responses: 0
 Accounting statistics
   START sent successfully: 1
   START send failures: 0
   START ack received: 1
   INTERIM sent successfully: 0
   INTERIM send failures: 0
   INTERIM ack received: 0
 Re-authentication statistics
   Requests received: 0
   Sucessfull responses: 0
   Aborts handled: 0
 Service statistics
   Service name: filter-serv
   Creation requests: 1
   Deletion requests: 0
   Request timeouts: 0
   Service name: filter-serv2
   Creation requests: 144
   Deletion requests: 0
   Request timeouts: 144
```

show network-access aaa subscribers username

```
user@host> show network-access aaa subscribers username fred@isp5.net
Logical system/Routing instance   Client type  Session-ID  Session uptime
Accounting
isp-bos-metro-16:isp-cmbrg-12     dhcp         7           01:12:56
on/volume
Service name       Service type      Quota          Accounting
I-Cast             volume            1200 Mbps      on/volume+time
Voip                                                on/volume
GamingBurst        time              6000 secs      on/volume
```

CHAPTER 9

Subscriber Management Interface CLI Commands

show interfaces filters

Syntax show interfaces filters
<interface-name>

Release Information Command introduced before Junos OS Release 7.4.
Command introduced on PTX Series Packet Transport Routers for Junos OS Release 12.1.

Description Display all firewall filters that are installed on each interface in a system.

Options **none**—Display filter information about all interfaces.

interface-name—(Optional) Display filter information about a particular interface.

Additional Information For information about how to configure firewall filters, see the *Routing Policy Feature Guide for Routing Devices*. For related operational mode commands, see the *Junos OS Operational Mode Commands*.

Required Privilege Level view

List of Sample Output
show interfaces filters on page 145
show interfaces filters interface-name on page 145
show interfaces filters (PTX Series Packet Transport Routers) on page 145

Output Fields Table 11 on page 144 lists the output fields for the **show interfaces filters** command. Output fields are listed in the approximate order in which they appear.

Table 11: show interfaces filters Output Fields

Field Name	Field Description
Interface	Name of the interface.
Admin	Interface state: **up** or **down**.
Link	Link state: **up** or **down**.
Proto	Protocol configured on the interface.
Input Filter	Names of any firewall filters to be evaluated when packets are received on the interface, including any filters attached through activation of dynamic service.
Output Filter	Names of any firewall filters to be evaluated when packets are transmitted on the interface, including any filters attached through activation of dynamic service.

Sample Output

show interfaces filters

```
user@host> show interfaces filters
Interface       Admin Link Proto Input Filter         Output Filter
ge-0/0/0        up    up
ge-0/0/0.0      up    up   inet
                           iso
ge-5/0/0        up    up
ge-5/0/0.0      up    up   any                        f-any
                           inet                       f-inet
                           multiservice
gr-0/3/0        up    up
ip-0/3/0        up    up
mt-0/3/0        up    up
pd-0/3/0        up    up
pe-0/3/0        up    up
vt-0/3/0        up    up
at-1/0/0        up    up
at-1/0/0.0      up    up   inet
                           iso
at-1/1/0        up    down
at-1/1/0.0      up    down inet
                           iso
....
```

show interfaces filters interface-name

```
user@host> show interfaces filters so-2/1/0
Interface       Admin Link Proto Input Filter         Output Filter
so-2/1/0        up    down
so-2/1/0.0      up    down inet  goop                 outfilter
                           iso
                           inet6 v6in                 v6out

user@host > show interfaces filters ge-3/0/1
Interface       Admin Link Proto Input Filter         Output Filter
ge-3/0/1        up    up
ge-3/0/1.0      up    up   inet  F1-ge-3/0/1.0-in     F2-ge-3/0/1.0-out
                           inet  F3-ge-3/0/1.0-in
```

show interfaces filters (PTX Series Packet Transport Routers)

```
user@host > show interfaces filters em0
Interface       Admin Link Proto Input Filter         Output Filter
      em0             up    up
      em0.0           up    up   inet
```

show interfaces routing

Syntax
show interfaces routing
<brief | detail>
<*interface-name*>
<logical-system (all | *logical-system-name*)>

Release Information
Command introduced before Junos OS Release 7.4.

Description
Display the state of the router's interfaces. Use this command for performing router diagnostics only, when you are determining whether the routing protocols and the Junos OS differ about the state of an interface.

Options
none—Display standard information about the state of all router interfaces on all logical systems.

brief | detail—(Optional) Display the specified level of output.

interface-name—(Optional) Name of a specific interface.

logical-system (all | *logical-system-name*)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Additional Information
For information about how to configure routing protocols, see the *Junos OS Routing Protocols Library for Routing Devices*. For information about related operational mode commands for routing instances and protocols, see the *Junos OS Operational Mode Commands*.

Required Privilege Level
view

List of Sample Output
show interfaces routing brief on page 147
show interfaces routing brief (TX Matrix Plus Router) on page 148
show interfaces routing detail on page 148
show interfaces routing detail (TX Matrix Plus Router) on page 149

Output Fields
Table 12 on page 146 lists the output fields for the **show interfaces routing** command. Output fields are listed in the approximate order in which they appear.

Table 12: show interfaces routing Output Fields

Field Name	Field Description	Level of Output
Interface	Name of the physical interface.	none **brief**
State	State of the physical interface: **Up** or **Down**.	none **brief**
Addresses	Protocols and addresses configured on the interface.	none **brief**
Index	Interface index number, which reflects its initialization sequence.	**detail**

Table 12: show interfaces routing Output Fields *(continued)*

Field Name	Field Description	Level of Output
Refcount	Number of references to the interface in the routing software.	**detail**
State	State (**Up** or **Down**) and type of interface.	**detail**
Change	Reflects one or more of the following recent changes to the interface: • **Add**—The interface was just added. • **Address**—The interface's link-layer address has changed. • **Delete**—The interface is being deleted. • **Encapsulation**—The type of encapsulation on the interface has changed. • **Metric**—The interface's metric value has changed. • **MTU**—The interface's maximim transmission unit size has changed. • **UpDown**—The interface has made an up or down transition.	**detail**
Up/down transitions	Number of times the interface has gone from **Down** to **Up**.	**detail**
Link layer	Describes the link layer of the interface.	**detail**
Encapsulation	Encapsulation on the interface.	**detail**
Bandwidth	Speed at which the interface is running.	**detail**

***Protocol* address**	Information about the configuration of protocols on the interface:
	• **Address**—Address configured on the interface for the protocol type.
	• **State**—State (**Up** or **down**) and type of interface.
	• **Change**—Reflects one or more of the following recent changes to the interface:
	  ◦ **Add**—The interface was just added.
	  ◦ **Address**—The interface's address has changed.
	  ◦ **Broadcast**—The interface's broadcast address has changed.
	  ◦ **Delete**—The interface is being deleted.
	  ◦ **Netmask**—The interface's netmask has changed.
	  ◦ **UpDown**—The interface has made an up or down transition.
	• **Preference**—Preference value for the route for this address.
	• **Metric**—Metric value on the interface for the protocol type.
	• **MTU**—Maximim transmission unit value of the interface.
	• **Local address**—On a point-to-point link, the address of the local side of the link. Not used for multicast links.
	• **Destination**—For a point-to-point link, the address of the remote side of the link. For multicast links, the network address.
		detail

Sample Output

show interfaces routing brief

```
user@host> show interfaces routing brief
```

```
Interface         State Addresses
so-5/0/3.0        Down  ISO   enabled
so-5/0/2.0        Up    MPLS  enabled
                        ISO   enabled
                        INET  192.168.2.120
                        INET  enabled
so-5/0/1.0        Up    MPLS  enabled
                        ISO   enabled
                        INET  192.168.2.130
                        INET  enabled
at-1/0/0.3        Up    CCC   enabled
at-1/0/0.2        Up    CCC   enabled
at-1/0/0.0        Up    ISO   enabled
                        INET  192.168.90.10
                        INET  enabled
lo0.0             Up    ISO   47.0005.80ff.f800.0000.0108.0001.1921.6800.5061.00
                        ISO   enabled
                        INET  127.0.0.1
fxp1.0            Up
fxp0.0            Up    INET  192.168.6.90
```

show interfaces routing brief (TX Matrix Plus Router)

```
user@host> show interfaces routing brief
Interface         State Addresses
...
ge-23/0/4.0       Up    INET  2.9.1.1
                        ISO   enabled
                        MPLS  enabled
ge-23/0/3.0       Up    INET  2.8.1.1
                        ISO   enabled
                        MPLS  enabled
ge-23/0/2.0       Up    INET  2.7.1.1
                        ISO   enabled
                        MPLS  enabled
ge-23/0/1.0       Up    INET  2.6.1.1
                        ISO   enabled
                        MPLS  enabled
ge-23/0/0.0       Up    INET  2.5.1.1
                        ISO   enabled
                        MPLS  enabled
ge-31/0/7.599     Up    INET  2.14.10.93
ge-31/0/7.598     Up    INET  2.14.10.89
ge-31/0/7.597     Up    INET  2.14.10.85
ge-31/0/7.596     Up    INET  2.14.10.81
ge-31/0/7.595     Up    INET  2.14.10.77
ge-31/0/7.594     Up    INET  2.14.10.73
...
ixgbe1.0          Up    INET  10.34.0.4
                        INET  162.0.0.4
                        INET6 fe80::200:1ff:fe22:4
                        INET6 fec0::a:22:0:4
ixgbe0.0          Up    INET  10.34.0.4
                        INET  162.0.0.4
                        INET6 fe80::200:ff:fe22:4
                        INET6 fec0::a:22:0:4
em0.0             Up    INET  192.168.178.11
```

show interfaces routing detail

```
user@host> show interfaces routing detail
```

```
so-5/0/3.0
  Index: 15, Refcount: 2, State: Up <Broadcast PointToPoint Multicast> Change:<>

  Metric: 0, Up/down transitions: 0, Full-duplex
  Link layer: HDLC serial line Encapsulation: PPP Bandwidth: 155Mbps
  ISO address (null)
    State: <Broadcast PointToPoint Multicast> Change: <>
    Preference: 0 (120 down), Metric: 0, MTU: 4470 bytes
so-5/0/2.0
  Index: 14, Refcount: 7, State: <Up Broadcast PointToPoint Multicast> Change:<>

  Metric: 0, Up/down transitions: 0, Full-duplex
  Link layer: HDLC serial line Encapsulation: PPP Bandwidth: 155Mbps
  MPLS address (null)
    State: <Up Broadcast PointToPoint Multicast> Change: <>
    Preference: 0 (120 down), Metric: 0, MTU: 4458 bytes
  ISO address (null)
    State: <Up Broadcast PointToPoint Multicast> Change: <>
    Preference: 0 (120 down), Metric: 0, MTU: 4470 bytes
  INET address 192.168.2.120
    State: <Up Broadcast PointToPoint Multicast Localup> Change: <>
    Preference: 0 (120 down), Metric: 0, MTU: 4470 bytes
    Local address: 192.168.2.120
    Destination: 192.168.2.110/32
  INET address (null)
    State: <Up Broadcast PointToPoint Multicast> Change: <>
    Preference: 0 (120 down), Metric: 0, MTU: 4470 bytes
...
```

show interfaces routing detail (TX Matrix Plus Router)

```
user@host> show interfaces routing detail
ge-23/0/4.0
  Index: 77, Refcount: 5, State: <Up Broadcast Multicast> Change: <>
  0 metric, 0 up/down transitions, reth state 0, full-duplex
  Link layer: Ethernet Encapsulation: Ethernet Bandwidth: 1000Mbps
  Link address #0 0.1d.b5.14.da.2d
  INET address 2.9.1.1
    State: <Up Broadcast Multicast Localup> Change: <> Flags: <RT-Change>
    Preference 0, metric 0, MTU 1500 bytes
    Broadcast address 2.9.1.3
    Destination: 2.9.1.0/30
    System flags: <Is-Preferred Is-Primary>
  ISO address (null)
    State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
    Preference 0, metric 0, MTU 1497 bytes
    System flags: <>
  MPLS address (null)
    State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
    Preference 0, metric 0, MTU 1488 bytes
    System flags: <>
ge-23/0/3.0
  Index: 76, Refcount: 5, State: <Up Broadcast Multicast> Change: <>
  0 metric, 0 up/down transitions, reth state 0, full-duplex
  Link layer: Ethernet Encapsulation: Ethernet Bandwidth: 1000Mbps
  Link address #0 0.1d.b5.14.da.2c
  INET address 2.8.1.1
    State: <Up Broadcast Multicast Localup> Change: <> Flags: <RT-Change>
    Preference 0, metric 0, MTU 1500 bytes
    Broadcast address 2.8.1.3
    Destination: 2.8.1.0/30
```

```
    System flags: <Is-Preferred Is-Primary>
  ISO address (null)
    State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
    Preference 0, metric 0, MTU 1497 bytes
    System flags: <>
  MPLS address (null)
    State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
    Preference 0, metric 0, MTU 1488 bytes
    System flags: <>
ge-23/0/2.0
  Index: 75, Refcount: 5, State: <Up Broadcast Multicast> Change: <>
  0 metric, 0 up/down transitions, reth state 0, full-duplex
  Link layer: Ethernet Encapsulation: Ethernet Bandwidth: 1000Mbps
  Link address #0 0.1d.b5.14.da.2b
  INET address 2.7.1.1
    State: <Up Broadcast Multicast Localup> Change: <> Flags: <RT-Change>
    Preference 0, metric 0, MTU 1500 bytes
    Broadcast address 2.7.1.3
    Destination: 2.7.1.0/30
    System flags: <Is-Preferred Is-Primary>
  ISO address (null)
    State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
    Preference 0, metric 0, MTU 1497 bytes
    System flags: <>
  MPLS address (null)
    State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
    Preference 0, metric 0, MTU 1488 bytes
    System flags: <>
ge-23/0/1.0
  Index: 74, Refcount: 5, State: <Up Broadcast Multicast> Change: <>
  0 metric, 0 up/down transitions, reth state 0, full-duplex
  Link layer: Ethernet Encapsulation: Ethernet Bandwidth: 1000Mbps
  Link address #0 0.1d.b5.14.da.2a
  INET address 2.6.1.1
    State: <Up Broadcast Multicast Localup> Change: <> Flags: <RT-Change>
    Preference 0, metric 0, MTU 1500 bytes
    Broadcast address 2.6.1.3
...
ixgbe1.0
  Index: 5, Refcount: 5, State: <Up Broadcast Multicast> Change: <>
  0 metric, 0 up/down transitions, reth state 0, full-duplex
  Link layer: Ethernet Encapsulation: Ethernet Bandwidth: 1000Mbps
  Link address #0 2.0.1.22.0.4
  INET address 10.34.0.4
    State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
    Preference 0, metric 0, MTU 1500 bytes
    Broadcast address 10.255.255.255
    Destination: 10.0.0.0/8
    System flags: <Is-Preferred>
  INET address 162.0.0.4
    State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
    Preference 0, metric 0, MTU 1500 bytes
    Broadcast address 191.255.255.255
    Destination: 128.0.0.0/2
    System flags: <Primary Is-Preferred Is-Primary>
  INET6 address fe80::200:1ff:fe22:4
    State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
    Preference 0, metric 0, MTU 1500 bytes
    Destination: fe80::/64
    System flags: <Is-Preferred>
  INET6 address fec0::a:22:0:4
```



```
    State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
    Preference 0, metric 0, MTU 1500 bytes
    Destination: fec0::/64
    System flags: <Is-Preferred Is-Primary>
ixgbe0.0
  Index: 4, Refcount: 5, State: <Up Broadcast Multicast> Change: <>
  0 metric, 0 up/down transitions, reth state 0, full-duplex
  Link layer: Ethernet Encapsulation: Ethernet Bandwidth: 1000Mbps
  Link address #0 2.0.0.22.0.4
  INET address 10.34.0.4
    State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
    Preference 0, metric 0, MTU 1500 bytes
    Broadcast address 10.255.255.255
    Destination: 10.0.0.0/8
    System flags: <Is-Preferred>
  INET address 162.0.0.4
    State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
    Preference 0, metric 0, MTU 1500 bytes
    Broadcast address 191.255.255.255
    Destination: 128.0.0.0/2
    System flags: <Primary Is-Default Is-Preferred Is-Primary>
  INET6 address fe80::200:ff:fe22:4
    State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
    Preference 0, metric 0, MTU 1500 bytes
    Destination: fe80::/64
    System flags: <Is-Preferred>
  INET6 address fec0::a:22:0:4
    State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
    Preference 0, metric 0, MTU 1500 bytes
    Destination: fec0::/64
    System flags: <Is-Default Is-Preferred Is-Primary>
em0.0
  Index: 3, Refcount: 2, State: <Up Broadcast Multicast> Change: <>
  0 metric, 0 up/down transitions, reth state 0, full-duplex
  Link layer: Ethernet Encapsulation: Ethernet Bandwidth: 100Mbps
  Link address #0 0.80.f9.26.0.c0
  INET address 192.168.178.11
    State: <Up Broadcast Multicast Localup> Change: <> Flags: <>
    Preference 0, metric 0, MTU 1500 bytes
    Broadcast address 192.168.178.127
    Destination: 192.168.178.0/25
    System flags: <Is-Preferred Is-Primary>
```

show interfaces routing-instance

Syntax show interfaces routing-instance (*instance-name* | all)

Release Information Command introduced in Junos OS Release 9.1.

Description Display information about the interfaces configured for either a specific routing instance or for all of the routing instances.

Options **all**—Display information about all of the interfaces configured for all of the routing instances on the router.

instance-name—Display information about the interfaces configured for the specified routing instance.

Required Privilege Level view

List of Sample Output
show interfaces routing-instance terse on page 152
show interfaces routing-instance all on page 152
show interfaces routing-instance extensive on page 152

Output Fields The output fields from the **show interfaces routing-instance** command are identical to those produced by the **show interfaces *interface-name*** command. For a description of output fields, see the other chapters in this manual.

Sample Output

show interfaces routing-instance terse

```
user@host> show interfaces routing-instance sample terse
Interface       Admin   Link      Proto    Local                 Remote
ge-0/0/0.0      up      up        inet     192.168.4.28/24
```

Sample Output

show interfaces routing-instance all

```
user@host> show interfaces terse routing-instance all
Interface   Admin   Link   Proto    Local             Remote Instance
at-0/0/1    up      up     inet     10.0.0.1/24
ge-0/0/0.0  up      up     inet      192.168.4.28/24          sample-a
at-0/1/0.0  up      up     inet6     fe80::a:0:0:4/64         sample-b
so-0/0/0.0  up      up     inet     10.0.0.1/32
```

show interfaces routing-instance extensive

```
user@hostshow interfaces fe-0/1/3 routing-instance instance2 extensive
Logical interface fe-0/1/3.0 (Index 70) (SNMP ifIndex 53) (Generation 211)
    Flags: SNMP-Traps Encapsulation: ENET2
    Traffic statistics:
     Input  bytes :                  0
     Output bytes :                 42
     Input packets:                  0
     Output packets:                 1
```



```
     IPv6 transit statistics:
      Input bytes :                  0
      Output bytes  :                0
      Input packets:                 0
      Output packets:                0
    Local statistics:
     Input bytes :                   0
     Output bytes :                 42
     Input packets:                  0
     Output packets:                 1
    Transit statistics:
     Input bytes :                   0                    0 bps
     Output bytes :                  0                    0 bps
     Input packets:                  0                    0 pps
     Output packets:                 0                    0 pps
     IPv6 transit statistics:
      Input bytes :                  0
      Output bytes :                 0
      Input packets:                 0
      Output packets:                0
    Protocol inet, MTU: 1500, Generation: 252, Route table: 4
      Flags: Is-Primary
      Addresses, Flags: Is-Default Is-Preferred Is-Primary
      Destination: 150.1.1/24, Local: 150.1.1.1, Broadcast: 150.1.1.255,
Generation: 263
```

CHAPTER 10

Subscriber Management Subscriber CLI Commands

show subscribers

Syntax

show subscribers
<detail | extensive | terse>
<aci-interface-set-name *aci-interface-set-name*>
<address *address*>
<agent-circuit-identifier *agent-circuit-identifier-substring*>
<client-type *client-type*>
<count>
<interface *interface*>
<logical-system *logical-system*>
<mac-address *mac-address*>
<physical-interface *physical-interface-name*>
<profile-name *profile-name*>
<routing-instance *routing-instance*>
<stacked-vlan-id *stacked-vlan-id*>
<subscriber-state *subscriber-state*>
<user-name *user-name*>
<vci *vci-identifier*>
<vpi *vpi-identifier*>
<vlan-id *vlan-id*>

Release Information

Command introduced in Junos OS Release 9.3.
Command introduced in Junos OS Release 9.3 for EX Series switches.
client-type, **mac-address**, **subscriber-state**, and **extensive** options introduced in Junos OS Release 10.2.
count option usage with other options introduced in Junos OS Release 10.2.
Command introduced in Junos OS Release 11.1 for the QFX Series.
Options **aci-interface-set-name** and **agent-circuit-identifier** introduced in Junos OS Release 12.2.
The **physical-interface** and **user-name** options introduced in Junos OS Release 12.3.
Options **vci** and **vpi** introduced in Junos OS Release 12.3R3 and supported in later 12.3R*x* releases.
Options **vci** and **vpi** supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)

Description

Display information for active subscribers.

Options

detail | extensive | terse—(Optional) Display the specified level of output.

aci-interface-set-name—(Optional) Display all dynamic subscriber sessions that use the specified agent circuit identifier (ACI) interface set. Use the ACI interface set name generated by the router, such as aci-1003-ge-1/0/0.4001, and not the actual ACI value found in the DHCP or PPPoE control packets.

address—(Optional) Display subscribers whose IP address matches the specified address. You must specify the IPv4 or IPv6 address prefix without a netmask (for example, 192.168.17.1). If you specify the IP address as a prefix with a netmask (for example, 192.168.17.1/32), the router displays a message that the IP address is invalid, and rejects the command.

agent-circuit-identifier-substring—(Optional) Display all dynamic subscriber sessions whose ACI value matches the specified substring.

client-type—(Optional) Display subscribers whose client type matches the specified client type (DHCP, L2TP, PPP, PPPOE, VLAN, or static).

count—(Optional) Display the count of total subscribers and active subscribers for any specified option. You can use the **count** option alone or with the **address**, **client-type**, **interface**, **logical-system**, **mac-address**, **profile-name**, **routing-instance**, **stacked-vlan-id**, **subscriber-state**, or **vlan-id** options.

id—(Optional) Display a specific subscriber session whose session id matches the specified subscriber ID. You can display subscriber IDs by using the **show subscribers extensive** or the **show subscribers interface extensive** commands.

interface—(Optional) Display subscribers whose interface matches the specified interface.

logical-system—(Optional) Display subscribers whose logical system matches the specified logical system.

mac-address—(Optional) Display subscribers whose MAC address matches the specified MAC address.

physical-interface-name—(M120, M320, and MX Series routers only) (Optional) Display subscribers whose physical interface matches the specified physical interface.

profile-name—(Optional) Display subscribers whose dynamic profile matches the specified profile name.

routing-instance—(Optional) Display subscribers whose routing instance matches the specified routing instance.

subscriber-state—(Optional) Display subscribers whose subscriber state matches the specified subscriber state (ACTIVE, CONFIGURED, INIT, TERMINATED, or TERMINATING).

user-name—(M120, M320, and MX Series routers only) (Optional) Display subscribers whose username matches the specified subscriber name.

vci-identifier—(MX Series routers with MPCs and ATM MICs with SFP only) (Optional) Display active ATM subscribers whose ATM virtual circuit identifier (VCI) matches the specified VCI identifier. The range of values is **0** through **255**.

vpi-identifier—(MX Series routers with MPCs and ATM MICs with SFP only) (Optional) Display active ATM subscribers whose ATM virtual path identifier (VPI) matches the specified VPI identifier. The range of values is **0** through **65535**.

vlan-id—(Optional) Display subscribers whose VLAN ID matches the specified VLAN ID.

stacked-vlan-id—(Optional) Display subscribers whose stacked VLAN ID matches the specified stacked VLAN ID.

NOTE: Due to display limitations, logical system and routing instance output values are truncated when necessary.

Required Privilege Level view

Related Documentation

- show subscribers summary on page 174
- *Verifying and Managing Agent Circuit Identifier-Based Dynamic VLAN Configuration*

List of Sample Output

show subscribers vlan-id detail on page 173
show subscribers vpi vci extensive (PPPoE-over-ATM Subscriber Session) on page 173

Output Fields Table 13 on page 159 lists the output fields for the **show subscribers** command. Output fields are listed in the approximate order in which they appear.

Table 13: show subscribers Output Fields

Field Name	Field Description
Interface	Interface associated with the subscriber. The router or switch displays subscribers whose interface matches or begins with the specified interface. The * character indicates a continuation of addresses for the same session.
IP Address/VLAN ID	Subscriber IP address or VLAN ID associated with the subscriber in the form *tpid.vlan-id* No IP address or VLAN ID is assigned to an L2TP tunnel-switched session. For these subscriber sessions the value is **Tunnel-switched**.
User Name	Name of subscriber.
LS:RI	Logical system and routing instance associated with the subscriber.
Type	Subscriber client type (DHCP, L2TP, PPP, PPPoE, STATIC-INTERFACE, VLAN).
IP Address	Subscriber IPv4 address.
IP Netmask	Subscriber IP netmask.
Primary DNS Address	IP address of primary DNS server.
Secondary DNS Address	IP address of secondary DNS server.
Primary WINS Address	IP address of primary WINS server.
Secondary WINS Address	IP address of secondary WINS server.
IPv6 Address	Subscriber IPv6 address, or multiple addresses.
IPv6 Prefix	Subscriber IPv6 prefix. If you are using DHCPv6 prefix delegation, this is the delegated prefix.
IPv6 User Prefix	IPv6 prefix obtained through ND/RA.
IPv6 Address Pool	Subscriber IPv6 address pool. The IPv6 address pool is used to allocate IPv6 prefixes to the DHCPv6 clients.
IPv6 Network Prefix Length	Length of the network portion of the IPv6 address.
IPv6 Prefix Length	Length of the subscriber IPv6 prefix.

Table 13: show subscribers Output Fields *(continued)*

Field Name	Field Description
Logical System	Logical system associated with the subscriber.
Routing Instance	Routing instance associated with the subscriber.
Interface Type	Whether the subscriber interface is **Static** or **Dynamic**.
Interface Set	Internally generated name of the dynamic ACI interface set used by the subscriber session.
Interface Set Type	Interface type of the ACI interface set: **Dynamic**. This is the only ACI interface set type currently supported.
Interface Set Session ID	Identifier of the dynamic ACI interface set entry in the session database.
Underlying Interface	Name of the underlying interface for the subscriber session.
Dynamic Profile Name	Dynamic profile used for the subscriber.
Dynamic Profile Version	Version number of the dynamic profile used for the subscriber.
MAC Address	MAC address associated with the subscriber.
State	Current state of the subscriber session (**Init**, **Configured**, **Active**, **Terminating**, **Tunneled**).
L2TP State	Current state of the L2TP session, **Tunneled** or **Tunnel-switched**. When the value is **Tunnel-switched**, two entries are displayed for the subscriber; the first entry is at the LNS interface on the LTS and the second entry is at the LAC interface on the LTS.
Tunnel switch Profile Name	Name of the L2TP tunnel switch profile that initiates tunnel switching.
Local IP Address	IP address of the local gateway (LAC).
Remote IP Address	IP address of the remote peer (LNS).
VLAN Id	VLAN ID associated with the subscriber in the form *tpid.vlan-id*.
Stacked VLAN Id	Stacked VLAN ID associated with the subscriber in the form *tpid.vlan-id*.
RADIUS Accounting ID	RADIUS accounting ID associated with the subscriber.
Agent Circuit ID	Option 82 agent circuit ID associated with the subscriber. The ID is displayed as an ASCII string unless the value has nonprintable characters, in which case it is displayed in hexadecimal format.
Agent Remote ID	Option 82 agent remote ID associated with the subscriber. The ID is displayed as an ASCII string unless the value has nonprintable characters, in which case it is displayed in hexadecimal format.
DHCP Relay IP Address	IP address used by the DHCP relay agent.

Table 13: show subscribers Output Fields *(continued)*

Field Name	Field Description
ATM VPI	(MX Series routers with MPCs and ATM MICs with SFP only) ATM virtual path identifier (VPI) on the subscriber's physical interface.
ATM VCI	(MX Series routers with MPCs and ATM MICs with SFP only) ATM virtual circuit identifier (VCI) for each VPI configured on the subscriber interface.
Login Time	Date and time at which the subscriber logged in.
Effective shaping-rate	Actual downstream traffic shaping rate for the subscriber, in kilobits per second.
IPv4 rpf-check Fail Filter Name	Name of the filter applied by the dynamic profile to IPv4 packets that fail the RPF check.
IPv6 rpf-check Fail Filter Name	Name of the filter applied by the dynamic profile to IPv6 packets that fail the RPF check.
DHCP Options	**len** = number of hex values in the message. The hex values specify the type, length, value (TLV) for DHCP options, as defined in RFC 2132.
Session ID	ID number for a subscriber service session.
Underlying Session ID	For DHCPv6 subscribers on a PPPoE network, displays the session ID of the underlying PPPoE interface.
Service Sessions	Number of service sessions (that is, a service activated using RADIUS CoA) associated with the subscribers.
Service Session Name	Service session profile name.
Session Timeout (seconds)	Number of seconds of access provided to the subscriber before the session is automatically terminated.
Idle Timeout (seconds)	Number of seconds subscriber can be idle before the session is automatically terminated.
IPv6 Delegated Address Pool	Name of the pool used for DHCPv6 prefix delegation.
IPv6 Delegated Network Prefix Length	Length of the prefix configured for the IPv6 delegated address pool.
IPv6 Interface Address	Address assigned by the Framed-Ipv6-Prefix AAA attribute.
IPv6 Framed Interface Id	Interface ID assigned by the Framed-Interface-Id AAA attribute.
ADF IPv4 Input Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv4 input filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.

Table 13: show subscribers Output Fields *(continued)*

Field Name	Field Description
ADF IPv4 Output Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv4 output filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
ADF IPv6 Input Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv6 input filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
ADF IPv6 Output Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv6 output filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
IPv4 Input Filter Name	Name assigned to the IPv4 input filter (client or service session).
IPv4 Output Filter Name	Name assigned to the IPv4 output filter (client or service session).
IPv6 Input Filter Name	Name assigned to the IPv6 input filter (client or service session).
IPv6 Output Filter Name	Name assigned to the IPv6 output filter (client or service session).
IFL Input Filter Name	Name assigned to the logical interface input filter (client or service session).
IFL Output Filter Name	Name assigned to the logical interface output filter (client or service session).

Sample Output

show subscribers (IPv4)

```
user@host> show subscribers
Interface               IP Address/VLAN ID   User Name         LS:RI
ge-1/3/0.1073741824     100                                    default:default
demux0.1073741824       100.0.0.10           WHOLESALER-CLIENT default:default
demux0.1073741825       101.0.0.3            RETAILER1-CLIENT  test1:retailer1
demux0.1073741826       102.0.0.3            RETAILER2-CLIENT  test1:retailer2
```

show subscribers (IPv6)

```
user@host> show subscribers
Interface          IP Address/VLAN ID   User Name           LS:RI
ge-1/0/0.0         2001::c0:0:0:0/74    WHOLESALER-CLIENT   default:default
     *             2002::1/128          subscriber-25       default:default
```

show subscribers (IPv4 and IPv6 Dual Stack)

```
user@host> show subscribers
Interface           IP Address/VLAN ID         User Name
LS:RI
demux0.1073741834   0x8100.1002 0x8100.1
default:default
demux0.1073741835   0x8100.1001 0x8100.1
default:default
pp0.1073741836      61.1.1.1                dualstackuser1@ISP1.com
```

```
default:ASP-1
*                   2041:1:1::/48
*                   2061:1:1:1::/64
pp0.1073741837      23.1.1.3                dualstackuser2@ISP1.com
default:ASP-1
*                   2001:1:2:5::/64
```

show subscribers (LNS on MX Series Routers)

```
user@host> show subscribers
Interface          IP Address/VLAN ID   User Name         LS:RI
si-4/0/0.1         192.168.4.1          xyz@example.com   default:default
```

show subscribers (L2TP Switched Tunnels)

```
user@host> show subscribers
Interface           IP Address/VLAN ID    User Name             LS:RI
si-2/1/0.1073741842 Tunnel-switched       ap@lts.com        default:default

si-2/1/0.1073741843 Tunnel-switched       ap@lts.com        default:default
```

show subscribers client-type dhcp detail

```
user@host> show subscribers client-type dhcp detail
Type: DHCP
IP Address: 100.20.9.7
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:10:95:00:00:98
State: Active
Radius Accounting ID: jnpr :2304
Login Time: 2009-08-25 14:43:52 PDT

Type: DHCP
IP Address: 100.20.10.7
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073744383
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:10:94:00:01:f3
State: Active
Radius Accounting ID: jnpr :2560
Login Time: 2009-08-25 14:43:56 PDT
```

show subscribers count

```
user@host> show subscribers count
Total Subscribers: 188, Active Subscribers: 188
```

show subscribers address detail (IPv6)

```
user@host> show subscribers address 100.16.12.137 detail
```

```
Type: PPPoE
User Name: pppoeTerV6User1Svc
IP Address: 100.16.12.137
IP Netmask: 255.0.0.0
IPv6 User Prefix: 1016:0:0:c88::/64
Logical System: default
Routing Instance: default
Interface: pp0.1073745151
Interface type: Dynamic
Underlying Interface: demux0.8201
Dynamic Profile Name: pppoe-client-profile
MAC Address: 00:0d:02:01:00:01
Session Timeout (seconds): 31622400
Idle Timeout (seconds): 86400
State: Active
Radius Accounting ID: jnpr demux0.8201:6544
Session ID: 6544
Agent Circuit ID: ifl3720
Agent Remote ID: ifl3720
Login Time: 2012-05-21 13:37:27 PDT
Service Sessions: 1
```

show subscribers detail (IPv4)

```
user@host> show subscribers detail
Type: DHCP
IP Address: 100.20.9.7
IP Netmask: 255.255.0.0
Primary DNS Address: 192.168.17.1
Secondary DNS Address: 192.168.17.2
Primary WINS Address: 192.168.22.1
Secondary WINS Address: 192.168.22.2
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:10:95:00:00:98
State: Active
Radius Accounting ID: jnpr :2304
Session Timeout (seconds): 3600
Idle Timeout (seconds): 600
Login Time: 2009-08-25 14:43:52 PDT
DHCP Options: len 52
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 08 33 04 00 00
00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 36 2f
33 2d 37 2d 30 37 05 01 06 0f 21 2c
Service Sessions: 2
```

show subscribers detail (IPv6)

```
user@host> show subscribers detail
Type: DHCP
User Name: pd-user1
IPv6 Prefix: 2002:db2:ffff:1::/64
Logical System: default
Routing Instance: default
Interface: ge-3/1/3.2
Interface type: Static
MAC Address: 00:51:ff:ff:00:03
State: Active
```

```
Radius Accounting ID: 1
Session ID: 1
Login Time: 2011-08-25 12:12:26 PDT
DHCP Options: len 42
00 08 00 02 00 00 00 01 00 0a 00 03 00 01 00 51 ff ff 00 03
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
```

show subscribers detail (IPv6 Static Demux Interface)

```
user@host> show subscribers detail
Type: STATIC-INTERFACE
User Name: demux0.1@jnpr.net
IPv6 Prefix: 1:2:3:4:5:6:7:aa/128
Logical System: default
Routing Instance: default
Interface: demux0.1
Interface type: Static
Dynamic Profile Name: junos-default-profile
State: Active
Radius Accounting ID: 185
Login Time: 2010-05-18 14:33:56 EDT
```

show subscribers detail (L2TP LNS Subscribers on MX Series Routers)

```
user@host> show subscribers detail
Type: L2TP
User Name: user1@jnpr.net
IP Address: 10.1.32.58
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: si-5/2/0.1073749824
Interface type: Dynamic
Dynamic Profile Name: dyn-lns-profile2
Dynamic Profile Version: 1
State: Active
Radius Accounting ID: 8001
Session ID: 8001
Login Time: 2011-04-25 20:27:50 IST
```

show subscribers detail (L2TP Switched Tunnels)

```
user@host> show subscribers detail
Type: L2TP
User Name: ap@example.com
Logical System: default
Routing Instance: default
Interface: si-2/1/0.1073741842
Interface type: Dynamic
Dynamic Profile Name: dyn-lts-profile
State: Active
L2TP State: Tunnel-switched
Tunnel switch Profile Name: ce-lts-profile
Local IP Address: 10.50.1.1
Remote IP Address: 192.168.20.3
Radius Accounting ID: 21
Session ID: 21
Login Time: 2013-01-18 03:01:11 PST

Type: L2TP
User Name: ap@example.com
```

```
Logical System: default
Routing Instance: default
Interface: si-2/1/0.1073741843
Interface type: Dynamic
Dynamic Profile Name: dyn-lts-profile
State: Active
L2TP State: Tunnel-switched
Tunnel switch Profile Name: ce-lts-profile
Local IP Address: 10.30.1.1
Remote IP Address: 172.20.1.10
Session ID: 22
Login Time: 2013-01-18 03:01:14 PST
```

show subscribers detail (Tunneled Subscriber)

```
user@host> show subscribers detail
Type: PPPoE
User Name: user1@example.com
Logical System: default
Routing Instance: default
Interface: pp0.1
State: Active, Tunneled
Radius Accounting ID: 512
```

show subscribers detail (IPv4 and IPv6 Dual Stack)

```
user@host> show subscribers detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlanProfile
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.1001
VLAN Id: 0x8100.1
Login Time: 2011-11-30 00:18:04 PST

Type: PPPoE
User Name: dualstackuser1@ISP1.com
IP Address: 61.1.1.1
IPv6 Prefix: 2041:1:1::/48
IPv6 User Prefix: 2061:1:1:1::/64
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: dualStack-Profile1
MAC Address: 00:00:64:03:01:02
State: Active
Radius Accounting ID: 2
Session ID: 2
Login Time: 2011-11-30 00:18:05 PST

Type: DHCP
IPv6 Prefix: 2041:1:1::/48
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Static
```

```
MAC Address: 00:00:64:03:01:02
State: Active
Radius Accounting ID: jnpr :3
Session ID: 3
Underlying Session ID: 2
Login Time: 2011-11-30 00:18:35 PST
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 00 64 03 01 02
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
```

show subscribers detail (ACI Interface Set Session)

```
user@host> show subscribers detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0
Interface Set: aci-1001-ge-1/0/0.2800
Interface Set Session ID: 0
Underlying Interface: ge-1/0/0.2800
Dynamic Profile Name: aci-vlan-set-profile-2
Dynamic Profile Version: 1
State: Active
Session ID: 1
Agent Circuit ID: aci-ppp-dhcp-20
Login Time: 2012-05-26 01:54:08 PDT
```

show subscribers detail (PPPoE Subscriber Session with ACI Interface Set)

```
user@host> show subscribers detail
Type: PPPoE
User Name: ppphint2
IP Address: 10.10.1.5
Logical System: default
Routing Instance: default
Interface: pp0.1073741825
Interface type: Dynamic
Interface Set: aci-1001-demux0.1073741824
Interface Set Type: Dynamic
Interface Set Session ID: 2
Underlying Interface: demux0.1073741824
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:64:39:01:02
State: Active
Radius Accounting ID: 3
Session ID: 3
Agent Circuit ID: aci-ppp-dhcp-dvlan-50
Login Time: 2012-03-07 13:46:53 PST
```

show subscribers extensive

```
user@host> show subscribers extensive
Type: DHCP
User Name: pd-user1
IPv6 Prefix: 2002:db2:ffff:1::/64
Logical System: default
Routing Instance: default
Interface: ge-3/1/3.2
Interface type: Static
```

```
MAC Address: 00:51:ff:ff:00:03
State: Active
Radius Accounting ID: 1
Session ID: 1
Login Time: 2011-08-25 12:12:26 PDT
DHCP Options: len 42
00 08 00 02 00 00 00 01 00 0a 00 03 00 01 00 51 ff ff 00 03
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
IPv6 Address Pool: pd_pool
IPv6 Network Prefix Length: 48
```

show subscribers extensive (RPF Check Fail Filter)

```
user@host> show subscribers extensive
...
Type: VLAN
  Logical System: default
  Routing Instance: default
  Interface: ae0.1073741824
  Interface type: Dynamic
  Dynamic Profile Name: vlan-prof
  State: Active
  Session ID: 9
  VLAN Id: 100
  Login Time: 2011-08-26 08:17:00 PDT
  IPv4 rpf-check Fail Filter Name: rpf-allow-dhcp
  IPv6 rpf-check Fail Filter Name: rpf-allow-dhcpv6
...
```

show subscribers extensive (L2TP LNS Subscribers on MX Series Routers)

```
user@host> show subscribers extensive
Type: L2TP
User Name: user1@jnpr.net
IP Address: 10.1.32.58
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: si-5/2/0.1073749824
Interface type: Dynamic
Dynamic Profile Name: dyn-lns-profile2
Dynamic Profile Version: 1
State: Active
Radius Accounting ID: 8001
Session ID: 8001
Login Time: 2011-04-25 20:27:50 IST
IPv4 Input Filter Name: classify-si-5/2/0.1073749824-in
IPv4 Output Filter Name: classify-si-5/2/0.1073749824-out
```

show subscribers extensive (IPv4 and IPv6 Dual Stack)

```
user@host> show subscribers extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlanProfile
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.1001
```

```
VLAN Id: 0x8100.1
Login Time: 2011-11-30 00:18:04 PST

Type: PPPoE
User Name: dualstackuser1@ISP1.com
IP Address: 61.1.1.1
IPv6 Prefix: 2041:1:1::/48
IPv6 User Prefix: 2061:1:1:1::/64
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: dualStack-Profile1
MAC Address: 00:00:64:03:01:02
State: Active
Radius Accounting ID: 2
Session ID: 2
Login Time: 2011-11-30 00:18:05 PST
IPv6 Delegated Network Prefix Length: 48
IPv6 Interface Address: 2061:1:1:1::1/64
IPv6 Framed Interface Id: 1:1:2:2
IPv4 Input Filter Name: FILTER-IN-pp0.1073741825-in
IPv4 Output Filter Name: FILTER-OUT-pp0.1073741825-out
IPv6 Input Filter Name: FILTER-IN6-pp0.1073741825-in
IPv6 Output Filter Name: FILTER-OUT6-pp0.1073741825-out

Type: DHCP
IPv6 Prefix: 2041:1:1::/48
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Static
MAC Address: 00:00:64:03:01:02
State: Active
Radius Accounting ID: jnpr :3
Session ID: 3
Underlying Session ID: 2
Login Time: 2011-11-30 00:18:35 PST
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 00 64 03 01 02
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00
IPv6 Delegated Network Prefix Length: 48
```

show subscribers extensive (Effective Shaping-Rate)

```
user@host> show subscribers extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741837
Interface type: Dynamic
Interface Set: ifset-1
Underlying Interface: ae1
Dynamic Profile Name: svlan-dhcp-test
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.201
VLAN Id: 0x8100.201
Login Time: 2011-11-30 00:18:04 PST
```

```
Effective shaping-rate: 31000000k
...
```

show subscribers aci-interface-set-name detail (Subscriber Sessions Using Specified ACI Interface Set)

```
user@host> show subscribers aci-interface-set-name aci-1003-ge-1/0/0.4001 detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-set-profile
Dynamic Profile Version: 1
State: Active
Session ID: 13
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:56 PDT

Type: PPPoE
User Name: ppphint2
IP Address: 10.10.1.7
Logical System: default
Routing Instance: default
Interface: pp0.1073741834
Interface type: Dynamic
Interface Set: aci-1003-ge-1/0/0.4001
Interface Set Type: Dynamic
Interface Set Session ID: 13
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:65:26:01:02
State: Active
Radius Accounting ID: 14
Session ID: 14
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:57 PDT
```

show subscribers agent-circuit-identifier detail (Subscriber Sessions Using Specified ACI Substring)

```
user@host> show subscribers agent-circuit-identifier aci-ppp-vlan detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-set-profile
Dynamic Profile Version: 1
State: Active
Session ID: 13
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:56 PDT

Type: PPPoE
User Name: ppphint2
IP Address: 10.10.1.7
Logical System: default
Routing Instance: default
Interface: pp0.1073741834
Interface type: Dynamic
Interface Set: aci-1003-ge-1/0/0.4001
```

```
Interface Set Type: Dynamic
Interface Set Session ID: 13
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:65:26:01:02
State: Active
Radius Accounting ID: 14
Session ID: 14
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:57 PDT
```

show subscribers interface extensive

```
user@host> show subscribers interface demux0.1073741826 extensive
Type: VLAN
User Name: test1@test.com
Logical System: default
Routing Instance: testnet
Interface: demux0.1073741826
Interface type: Dynamic
Dynamic Profile Name: profile-vdemux-relay-23qos
MAC Address: 00:00:6e:56:01:04
State: Active
Radius Accounting ID: 12
Session ID: 12
Stacked VLAN Id: 0x8100.1500
VLAN Id: 0x8100.2902
Login Time: 2011-10-20 16:21:59 EST

Type: DHCP
User Name: test1@test.com
IP Address: 172.16.200.6
IP Netmask: 255.255.255.0
Logical System: default
Routing Instance: testnet
Interface: demux0.1073741826
Interface type: Static
MAC Address: 00:00:6e:56:01:04
State: Active
Radius Accounting ID: 21
Session ID: 21
Login Time: 2011-10-20 16:24:33 EST
Service Sessions: 2

Service Session ID: 25
Service Session Name: SUB-QOS
State: Active

Service Session ID: 26
Service Session Name: service-cb-content
State: Active
IPv4 Input Filter Name: content-cb-in-demux0.1073741826-in
IPv4 Output Filter Name: content-cb-out-demux0.1073741826-out
```

show subscribers logical-system terse

```
user@host> show subscribers logical-system test1 terse
```

```
Interface           IP Address/VLAN ID   User Name         LS:RI
demux0.1073741825     101.0.0.3            RETAILER1-CLIENT  test1:retailer1
demux0.1073741826     102.0.0.3            RETAILER2-CLIENT  test1:retailer2
```

show subscribers physical-interface count

```
user@host> show subscribers physical-interface ge-1/0/0 count
Total subscribers: 3998, Active Subscribers: 3998
```

show subscribers routing-instance inst1 count

```
user@host> show subscribers routing-instance inst1 count
Total Subscribers: 188, Active Subscribers: 183
```

show subscribers stacked-vlan-id detail

```
user@host> show subscribers stacked-vlan-id 101 detail
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT
```

show subscribers stacked-vlan-id vlan-id detail (Combined Output)

```
user@host> show subscribers stacked-vlan-id 101 vlan-id 100 detail
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT
```

show subscribers stacked-vlan-id vlan-id interface detail (Combined Output for a Specific Interface)

```
user@host> show subscribers stacked-vlan-id 101 vlan-id 100 interface ge-1/2/0.* detail
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT
```

show subscribers user-name detail

```
user@host> show subscribers user-name larry1 detail
Type: DHCP
User Name: larry1
IP Address: 100.0.0.37
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.1
Interface type: Static
Dynamic Profile Name: foo
```

```
MAC Address: 00:10:94:00:00:01
State: Active
Radius Accounting ID: 1
Session ID: 1
Login Time: 2011-11-07 08:25:59 PST
DHCP Options: len 52
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 01 33 04 00 00
00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 32 2f
37 2d 30 2d 30 37 05 01 06 0f 21 2c
```

show subscribers vlan-id

```
user@host> show subscribers vlan-id 100
Interface           IP Address                              User Name
ge-1/0/0.1073741824
ge-1/2/0.1073741825
```

show subscribers vlan-id detail

```
user@host> show subscribers vlan-id 100 detail
Type: VLAN
Interface: ge-1/0/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: vlan-prof-tpid
State: Active
VLAN Id: 100
Login Time: 2009-03-11 06:48:54 PDT

Type: VLAN
Interface: ge-1/2/0.1073741825
Interface type: Dynamic
Dynamic Profile Name: vlan-prof-tpid
State: Active
VLAN Id: 100
Login Time: 2009-03-11 06:48:54 PDT
```

show subscribers vpi vci extensive (PPPoE-over-ATM Subscriber Session)

```
user@host> show subscribers vpi 40 vci 50 extensive
Type: PPPoE
User Name: testuser
IP Address: 100.0.0.2
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: pp0.0
Interface type: Static
MAC Address: 00:00:65:23:01:02
State: Active
Radius Accounting ID: 2
Session ID: 2
ATM VPI: 40
ATM VCI: 50
Login Time: 2012-12-03 07:49:26 PST
IP Address Pool: pool_1
IPv6 Framed Interface Id: 200:65ff:fe23:102
```

show subscribers summary

Syntax

show subscribers summary
< detail | extensive | terse>
<count>
physical-interface *physical-interface-name*
<all | logical-system *logical-system* pic | port | routing-instance *routing-instance* |slot>

Release Information

Command introduced in Junos OS Release 10.2.

Description

Display summary information for subscribers.

Options

detail | extensive | terse—(Optional) Display the specified level of output.

count—(Optional) Display the count of total subscribers and active subscribers for any specified option.

logical-system—(Optional) Display subscribers whose logical system matches the specified logical system.

physical-interface-name—(M120, M320, and MX Series routers only) (Optional) Display a count of subscribers whose physical interface matches the specified physical interface, by subscriber state, client type and LS:RI.

pic—(M120, M320, and MX Series routers only) (Optional) Display a count of subscribers by PIC number and the total number of subscribers.

port—(M120, M320, and MX Series routers only) (Optional) Display a count of subscribers by port number and the total number of subscribers.

routing-instance—(Optional) Display subscribers whose routing instance matches the specified routing instance.

slot—(M120, M320, and MX Series routers only) (Optional) Display a count of subscribers by FPC slot number and the total number of subscribers.

NOTE: **Due to display limitations, logical system and routing instance output values are truncated when necessary.**

Required Privilege Level

view

Related Documentation

- show subscribers on page 156

List of Sample Output

show subscribers summary physical-interface port on page 177
show subscribers summary physical-interface slot on page 177
show subscribers summary pic on page 177
show subscribers summary pic (Aggregated Ethernet Interfaces) on page 178
show subscribers summary port on page 178
show subscribers summary slot on page 178
show subscribers summary terse on page 178

Output Fields Table 14 on page 175 lists the output fields for the **show subscribers** command. Output fields are listed in the approximate order in which they appear.

Table 14: show subscribers Output Fields

Field Name	Field Description
Subscribers by State	Number of subscribers summarized by state. The summary information includes the following: • Init—Number of subscriber currently in the initialization state. • Configured—Number of configured subscribers. • Active—Number of active subscribers. • Terminating—Number of subscribers currently terminating. • Terminated—Number of terminated subscribers. • Total—Total number of subscribers for all states.
Subscribers by Client Type	Number of subscribers summarized by client type. Client types can include DHCP, L2TP, PPP, PPPOE, STATIC-INTERFACE, and VLAN. Also displays the total number of subscribers for all client types (Total).
Subscribers by LS:RI	Number of subscribers summarized by logical system:routing instance (LS:RI) combination. Also displays the total number of subscribers for all LS:RI combinations (Total).
Interface	Interface associated with the subscriber. The router or switch displays subscribers whose interface matches or begins with the specified interface. The * character indicates a continuation of addresses for the same session. For aggregated Ethernet interfaces, the output of the **summary (pic | port | slot)** options prefixes the interface name with **ae0:**.
Count	Count of subscribers displayed for each PIC, port, or slot when those options are specified with the **summary** option. For an aggregated Ethernet configuration, the total subscriber count does not equal the sum of the individual PIC, port, or slot counts, because each subscriber can be in more than one aggregated Ethernet link.
Total Subscribers	Total number of subscribers for all physical interfaces, all PICS, all ports, or all LS:RI slots.
IP Address/VLAN ID	Subscriber IP address or VLAN ID associated with the subscriber in the form *tpid.vlan-id*
User Name	Name of subscriber.
LS:RI	Logical system and routing instance associated with the subscriber.

Sample Output

show subscribers summary

```
user@host> show subscribers summary

Subscribers by State
 Init      3
 Configured    2
 Active   183
 Terminating    2
 Terminated    1

 TOTAL        191

Subscribers by Client Type
 DHCP     107
 PPP       76
 VLAN       8

 TOTAL        191
```

show subscribers summary all

```
user@host> show subscribers summary all
Subscribers by State
 Init         3
 Configured       2
 Active      183
 Terminating       2
 Terminated       1

 TOTAL          191

Subscribers by Client Type
 DHCP      107
 PPP          76
 VLAN          8

 TOTAL         191

Subscribers by LS:RI
 default:default   1
 default:ri1     28
 default:ri2     16
 ls1:default    22
 ls1:riA     38
 ls1:riB     44
 logsysX:routinstY  42

 TOTAL     191
```

show subscribers summary physical-interface

```
user@host> show subscribers summary physical-interface ge-1/0/0
Subscribers by State
   Active: 3998
   Total: 3998

Subscribers by Client Type
   DHCP: 3998
```

```
   Total: 3998

Subscribers by LS:RI
   default:default: 3998
   Total: 3998
```

show subscribers summary physical-interface pic

```
user@host> show subscribers summary physical-interface ge-0/2/0 pic
Subscribers by State
   Active: 4825
   Total: 4825

Subscribers by Client Type
   DHCP: 4825
   Total: 4825

Subscribers by LS:RI
   default:default: 4825
   Total: 4825
```

show subscribers summary physical-interface port

```
user@host> show subscribers summary physical-interface ge-0/3/0 port
Subscribers by State
   Active: 4825
   Total: 4825

Subscribers by Client Type
   DHCP: 4825
   Total: 4825

Subscribers by LS:RI
   default:default: 4825
   Total: 4825
```

show subscribers summary physical-interface slot

```
user@host> show subscribers summary physical-interface ge-2/0/0 slot
Subscribers by State
   Active: 4825
   Total: 4825

Subscribers by Client Type
   DHCP: 4825
   Total: 4825

Subscribers by LS:RI
   default:default: 4825
   Total: 4825
```

show subscribers summary pic

```
user@host> show subscribers summary pic
Interface           Count
ge-1/0              1000
ge-1/3              1000

Total Subscribers: 2000
```

show subscribers summary pic (Aggregated Ethernet Interfaces)

```
user@host> show subscribers summary pic
Interface           Count
ae0: ge-1/0         801
ae0: ge-1/3         801

Total Subscribers: 801
```

show subscribers summary port

```
user@host> show subscribers summary port
Interface           Count
ge-1                2000

Total Subscribers: 2000
```

show subscribers summary slot

```
user@host> show subscribers summary slot
Interface           Count
ge-1                2000

Total Subscribers: 2000
```

show subscribers summary terse

```
user@host> show subscribers summary terse
Interface           IP Address/VLAN ID   User Name         LS:RI
ge-1/3/0.1073741824   100                                   default:default
demux0.1073741824     100.0.0.10           WHOLESALER-CLIENT default:default
demux0.1073741825     101.0.0.3            RETAILER1-CLIENT  test1:retailer1
demux0.1073741826     102.0.0.3            RETAILER2-CLIENT  test1:retailer2
```

CHAPTER 11

Subscriber Management VPLS CLI Commands

show vpls connections

Syntax

show vpls connections
<brief | extensive>
<down | up | up-down>
<history>
<instance *instance-name* local-site *local-site-name* remote-site *remote-site-name*>
<instance-history>
<logical-system (all | *logical-system-name*)>
<status>
<summary>

Release Information

Command introduced before Junos OS Release 7.4.
instance-history option introduced in Junos OS Release 12.3R2.

Description

(T Series and M Series routers, except for the M160 router) Display virtual private LAN service (VPLS) connection information.

Options

none—Display information about all VPLS connections for all routing instances.

brief | extensive—(Optional) Display the specified level of output.

down | up | up-down—(Optional) Display nonoperational, operational, or both types of connections.

history—(Optional) Display information about connection history.

instance *instance-name*—(Optional) Display the VPLS connections for the specified routing instance only.

instance-history—(Optional) Display information about connection history for a particular instance.

local-site *local-site-name*—(Optional) Display the VPLS connections for the specified local site name or ID only.

remote-site *remote-site-name*—(Optional) Display the VPLS connections for the specified remote site name or ID only.

logical-system (all | *logical-system-name*)—(Optional) Perform this operation on all logical systems or on a particular logical system.

status—(Optional) Display information about the connection and interface status.

summary—(Optional) Display summary of all VPLS connections information.

Required Privilege Level

view

List of Sample Output

show vpls connections on page 186
show vpls connections extensive (Static VPLS Neighbors) on page 188

Output Fields Table 15 on page 181 lists the output fields for the **show vpls connections** command. Output fields are listed in the approximate order in which they appear.

Table 15: show vpls connections Output Fields

Field Name	Field Description
Instance	Name of the VPLS instance.
Local site	Name of the local site.
VPLS-id	Idenitfier for the VPLS site.
Number of local interfaces	Number of interfaces configured for the local site.
Number of local interfaces up	Number of interfaces configured for the local site that are currently up.
IRB interface present	Indicates whether or not an integrated routing and bridging (IRB) interface is present (**yes** or **no**).
Intf	List of all of the interfaces configured for the local site. The types of interfaces can include VPLS virtual loopback tunnel interfaces and label-switched interfaces. Any interface that supports VPLS could be listed here. Virtual loopback tunnel interfaces are displayed using the **vt-*fpc/pic/port.nnnnn*** format. Label-switched interfaces are displayed using the **lsi.*nnnnn*** format. In both cases, ***nnnnn*** is a dynamically generated virtual port used to transport and receive packets from other provider edge (PE) routers in the VPLS domain. Each interface might include the following information: • Identification as a VPLS interface • Name of the associated VPLS routing instance • Local site number • Remote site number • VPLS neighbor address • VPLS identifier
Interface flags	Flag associated with the interface. Can include the following: • **VC-Down**—The virtual circuit associated with this interface is down.
Label-base	First label in a block of labels. A remote PE router uses this first label when sending traffic toward the advertising PE router.
Offset	Displays the VPLS Edge (VE) block offset in the Layer 2 VPN NLRI. The VE block offset is used to identify a label block from which a particular label value is selected to setup a pseduowire for a remote site. The block offset value itself indicates the starting VE ID that maps to the label base contained in the VPLS NLRI advertisement.
Size	Label block size.

Table 15: show vpls connections Output Fields *(continued)*

Field Name	Field Description
Range	Label block range.
Preference	Preference value advertised for a VPLS site. When multiple PE routers are assigned the same VE ID for multihoming, you might need to specify that a particular PE router acts as the designated forwarder by configuring the site preference value. The site preference indicates the degree of preference for a particular customer site. The site preference is one of the tie-breaking criteria used in a designated forwarder election.
status-vector	Bit vector advertising the state of local PE-CE circuits to remote PE routers. A bit value of **0** indicates that the local circuit and LSP tunnel to the remote PE router are up, whereas a value of **1** indicates either one or both are down.
connection-site	Name of the connection site.
Neighbor	IP address and VPLS identifier for the VPLS neighbor.
Type	Type of connection: **loc** (local) or **rmt** (remote).

Table 15: show vpls connections Output Fields *(continued)*

Field Name	Field Description
St	

Table 15: show vpls connections Output Fields *(continued)*

Field Name	Field Description
	Status of the VPLS connection (corresponds with Legend for Connection Status): • **EI**—The local VPLS interface is configured with an encapsulation that is not supported. • **EM**—The encapsulation type received on this VPLS connection from the neighbor does not match the local VPLS connection interface encapsulation type. • **VC-Dn**—The virtual circuit is currently down. • **CM**—The two routers do not agree on a control word, which causes a control word mismatch. • **CN**—The virtual circuit is not provisioned properly. • **OR**—The label associated with the virtual circuit is out of range. • **OL**—No advertisement has been received for this virtual circuit from the neighbor. There is no outgoing label available for use by this virtual circuit. • **LD**—All of the CE-facing interfaces to the local site are down. Therefore, the connection to the local site is signaled as down to the other PE routers. No pseudowires can be established. • **RD**—All the interfaces to the remote neighbor are down. Therefore, the remote site has been signaled as down to the other PE routers. No pseudowires can be established. • **LN**—The local site has lost path selection to the remote site and therefore no pseduowires can be established from this local site. • **RN**—The remote site has lost path selection to a local site or other remote site and therefore no pseudowires are established to this remote site. • **XX**—The VPLS connection is down for an unn reason. This is a programming error. • **MM**—The MTU for the local site and the remote site do not match. • **BK**—The router is using a backup connection. • **PF**—Profile parse failure. • **RS**—The remote site is in a standby state. • **NC**—The interface encapsulation is not configured as an appropriate CCC, TCC, or VPLS encapsulation. • **WE**—The encapsulation configured for the interface does not match the encapsulation configured for the associated connection within the VPLS routing instance. • **NP**—The router detects that interface hardware is not present. The hardware might be offline, a PIC might not be of the desired type, or the interface might be configured in a different routing instance. • **->**—Only the outbound connection is up. • **<-**—Only the inbound connection is up. • **Up**—The VPLS connection is operational. • **Dn**—The VPLS connection is down. • **CF**—The router cannot find enough bandwidth to the remote router to satisfy the VPLS connection bandwidth requirement. • **SC**—The local site identifier matches the remote site identifier. No pseudowire can be established between these two sites. You should configure different values for the local and remote site identifiers. • **LM**—The local site identifier is not the minimum designated, meaning it is not

Table 15: show vpls connections Output Fields *(continued)*

Field Name	Field Description
	the lowest. There is another local site with a lower site identifier. Pseudowires are not being established to this local site. and the associated local site identifier is not being used to distribute VPLS label blocks. However, this is not an error state. Traffic continues to be forwarded to the PE router interfaces connected to the local sites when the local sites are in this state. • **RM**—The remote site identifier is not the minimum designated, meaning it is not the lowest. There is another remote site connected to the same PE router which has lower site identifier. The PE router cannot established a pseduowire to this remote site and the associated remote site identifier cannot be used to distribute VPLS label blocks. However, this is not an error state. Traffic can continue to be forwarded to the PE router interface connected to this remote site when the remote site is in this state. • **IL**—The incoming packets for the VPLS connection have no MPLS label. • **MI**—The configured mesh group identifier is in use by another system in the network. • **ST**—The router has switched to a standby connection. • **PB**—Profile busy. • **SN**—The VPLS neighbor is static.
Time last up	Time connection was last in the **Up** condition.
# Up trans	Number of transitions from **Down** to **Up** condition.
Status	Status of the (local or remote circuit) local interface: • **Up**—Operational • **Dn**—Down • **NP**—Not present • **DS**—Disabled • **WE**—Wrong encapsulation • **UN**—Uninitialized
Encapsulation	Type of encapsulation: **VPLS**.
Remote PE	Address of the remote provider edge router.
Negotiated control-word	Whether a control word has been negotiated: **Yes** or **No**.
Incoming label	Name of the incoming label.
Outgoing label	Name of the outgoing label.
Negotiated PW status TLV	Indicates whether or not the pseudowire status TLV has been negotiated for the VPLS connection.

Table 15: show vpls connections Output Fields *(continued)*

Field Name	Field Description
Local interface	Provides the following information about the local interface configured for the VPLS neighbor: • Name of the local interface • **Status**—Interface status (**Up** or **Down**) • **Encapsulation**—Interface encapsulation (for example, **ETHERNET**) • **Description**—Includes the VPLS instance name, the VPLS neighbor address, and the VPLS identifier
Time	Date and time of VPLS connection event.
Event	Type of event.
Interface/Lbl/PE	Interface, label, or PE router.
Connection History	Each entry can include the date, time, year, and the connection event. Connection events include any of a variety of events related to VPLS connections, such as route changes, label updates, and interfaces going down or coming up.

Sample Output

show vpls connections

```
user@host> show vpls connections
Layer-2 VPN connections:

Legend for connection status (St)
EI -- encapsulation invalid      NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch     WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down    NP -- interface hardware not present
CM -- control-word mismatch      -< -- only outbound connection is up
CN -- circuit not provisioned    >- -- only inbound connection is up
OR -- out of range               Up -- operational
OL -- no outgoing label          Dn -- down
LD -- local site signaled down   CF -- call admission control failure
RD -- remote site signaled down  SC -- local and remote site ID collision
LN -- local site not designated  LM -- local site ID not minimum designated
RN -- remote site not designated RM -- remote site ID not minimum designated
XX -- unn connection status  IL -- no incoming label
MM -- MTU mismatch               MI -- Mesh-Group ID not availble
BK -- Backup connection          ST -- Standby connection
PF -- Profile parse failure      PB -- Profile busy

Legend for interface status
Up -- operational
Dn -- down

Instance: vpls-1
  Local site: 1 (11)
    Number of local interfaces: 1
    Number of local interfaces up: 1
    IRB interface present: no
    lt-1/3/0.10496
```

```
    vt-1/3/0.1048588    1         Intf - vpls vpls-1 local site 11 remote site 1

    vt-1/2/0.1048591    2         Intf - vpls vpls-1 local site 11 remote site 2

    vt-1/2/0.1048585    3         Intf - vpls vpls-1 local site 11 remote site 3

    vt-1/2/0.1048587    4         Intf - vpls vpls-1 local site 11 remote site 4

    vt-1/2/0.1048589    5         Intf - vpls vpls-1 local site 11 remote site 5

    vt-1/3/0.1048586    6         Intf - vpls vpls-1 local site 11 remote site 6

    vt-1/3/0.1048590    7         Intf - vpls vpls-1 local site 11 remote site 7

    vt-1/3/0.1048584    8         Intf - vpls vpls-1 local site 11 remote site 8

    Label-base        Offset     Size  Range     Preference
+   800256            1          16     16        100
    Timer Values:
        Startup wait time: 120 seconds
        New site wait-time: 20 seconds
        Collision detect time: 30 seconds
        Reclaim wait time: 748 milliseconds
    connection-site           Type  St     Time last up          # Up trans
    1                         rmt   Up     Apr 28 13:28:24 2009           2
      Remote PE: 124.1.2.1, Negotiated control-word: No
      Incoming label: 800256, Outgoing label: 800026
      Local interface: vt-1/3/0.1048588, Status: Up, Encapsulation: VPLS
        Description: Intf - vpls vpls-1 local site 11 remote site 1
    Connection History:
        Apr 28 13:28:24 2009  status update timer
        Apr 28 13:28:24 2009  PE route down
        Apr 28 13:24:27 2009  status update timer
        Apr 28 13:24:27 2009  loc intf up             vt-1/3/0.1048588
        Apr 28 13:24:27 2009  PE route changed
        Apr 28 13:24:27 2009  Out lbl Update                    800026
        Apr 28 13:24:27 2009  In lbl Update                     800256
        Apr 28 13:24:27 2009  loc intf down
    2                         rmt   Up     Apr 28 13:28:24 2009           2
      Remote PE: 124.1.7.1, Negotiated control-word: No
      Incoming label: 800257, Outgoing label: 800034
      Local interface: vt-1/2/0.1048591, Status: Up, Encapsulation: VPLS
        Description: Intf - vpls vpls-1 local site 11 remote site 2
    Connection History:
        Apr 28 13:28:24 2009  status update timer
        Apr 28 13:28:24 2009  PE route down
        Apr 28 13:24:28 2009  status update timer
        Apr 28 13:24:28 2009  loc intf up             vt-1/2/0.1048591
        Apr 28 13:24:28 2009  PE route changed
        Apr 28 13:24:28 2009  Out lbl Update                    800034
        Apr 28 13:24:28 2009  In lbl Update                     800257
        Apr 28 13:24:28 2009  loc intf down
    3                         rmt   Up     Apr 28 13:28:24 2009           2
      Remote PE: 124.1.4.1, Negotiated control-word: No
      Incoming label: 800258, Outgoing label: 800026
      Local interface: vt-1/2/0.1048585, Status: Up, Encapsulation: VPLS
        Description: Intf - vpls vpls-1 local site 11 remote site 3
    Connection History:
        Apr 28 13:28:24 2009  status update timer
        Apr 28 13:28:24 2009  PE route down
        Apr 28 13:24:26 2009  status update timer
```

```
    Apr 28 13:24:26 2009  loc intf up            vt-1/2/0.1048585
    Apr 28 13:24:26 2009  PE route changed
    Apr 28 13:24:26 2009  Out lbl Update                  800026
    Apr 28 13:24:26 2009  In lbl Update                   800258
    Apr 28 13:24:26 2009  loc intf down
4                         rmt   Up     Apr 28 13:28:24 2009          2
  Remote PE: 124.1.6.1, Negotiated control-word: No
  Incoming label: 800259, Outgoing label: 800026
  Local interface: vt-1/2/0.1048587, Status: Up, Encapsulation: VPLS
    Description: Intf - vpls vpls-1 local site 11 remote site 4
  Connection History:
    Apr 28 13:28:24 2009  status update timer
    Apr 28 13:28:24 2009  PE route down
    Apr 28 13:24:27 2009  status update timer
    Apr 28 13:24:27 2009  loc intf up            vt-1/2/0.1048587
    Apr 28 13:24:27 2009  PE route changed
    Apr 28 13:24:27 2009  Out lbl Update                  800026
    Apr 28 13:24:27 2009  In lbl Update                   800259
    Apr 28 13:24:27 2009  loc intf down
5                         rmt   Up     Apr 28 13:28:24 2009          2
  Remote PE: 124.1.3.1, Negotiated control-word: No
  Incoming label: 800260, Outgoing label: 800034
  Local interface: vt-1/2/0.1048589, Status: Up, Encapsulation: VPLS
    Description: Intf - vpls vpls-1 local site 11 remote site 5
  Connection History:
    Apr 28 13:28:24 2009  status update timer
    Apr 28 13:28:24 2009  PE route down
    Apr 28 13:24:28 2009  status update timer
    Apr 28 13:24:28 2009  loc intf up            vt-1/2/0.1048589
    Apr 28 13:24:28 2009  PE route changed
    Apr 28 13:24:28 2009  Out lbl Update                  800034
    Apr 28 13:24:27 2009  In lbl Update                   800260
    Apr 28 13:24:27 2009  loc intf down
```

show vpls connections extensive (Static VPLS Neighbors)

```
user@host> show vpls connections extensive instance red
Layer-2 VPN connections:

Legend for connection status (St)
EI -- encapsulation invalid      NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch     WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down    NP -- interface hardware not present
CM -- control-word mismatch      -> -- only outbound connection is up
CN -- circuit not provisioned    <- -- only inbound connection is up
OR -- out of range              Up -- operational
OL -- no outgoing label          Dn -- down
LD -- local site signaled down   CF -- call admission control failure
RD -- remote site signaled down  SC -- local and remote site ID collision
LN -- local site not designated  LM -- local site ID not minimum designated
RN -- remote site not designated RM -- remote site ID not minimum designated
XX -- unn connection status  IL -- no incoming label
MM -- MTU mismatch              MI -- Mesh-Group ID not availble
BK -- Backup connection                ST -- Standby connection
PF -- Profile parse failure      PB -- Profile busy
RS -- remote site standby       SN -- Static Neighbor

Legend for interface status
Up -- operational
Dn -- down
```

```
Instance: static
  VPLS-id: 1
   Number of local interfaces: 1
   Number of local interfaces up: 1
   ge-0/0/5.0
   lsi.1049344                 Intf - vpls static neighbor 10.255.114.3 vpls-id
 1
   Neighbor                Type  St     Time last up          # Up trans
   10.255.114.3(vpls-id 1)(SN) rmt Up     Mar  4 08:48:41 2010           1
     Remote PE: 10.255.114.3, Negotiated control-word: No
     Incoming label: 29696, Outgoing label: 29697
     Negotiated PW status TLV: No
     Local interface: lsi.1049344, Status: Up, Encapsulation: ETHERNET
       Description: Intf - vpls static neighbor 10.255.114.3 vpls-id 1
   Connection History:
       Mar  4 08:48:41 2010  status update timer
       Mar  4 08:48:41 2010  PE route changed
       Mar  4 08:48:41 2010  Out lbl Update                   29697
       Mar  4 08:48:41 2010  In lbl Update                    29696
       Mar  4 08:48:41 2010  loc intf up                lsi.1049344

user@PE1> show vpls connections extensive (Multihoming with FEC 129)
Layer-2 VPN connections:

Legend for connection status (St)
EI -- encapsulation invalid      NC -- interface encapsulation not CCC/TCC/VPLS
EM -- encapsulation mismatch     WE -- interface and instance encaps not same
VC-Dn -- Virtual circuit down    NP -- interface hardware not present
CM -- control-word mismatch      -> -- only outbound connection is up
CN -- circuit not provisioned    <- -- only inbound connection is up
OR -- out of range               Up -- operational
OL -- no outgoing label          Dn -- down
LD -- local site signaled down   CF -- call admission control failure
RD -- remote site signaled down  SC -- local and remote site ID collision
LN -- local site not designated  LM -- local site ID not minimum designated
RN -- remote site not designated RM -- remote site ID not minimum designated
XX -- unknown connection status  IL -- no incoming label
MM -- MTU mismatch               MI -- Mesh-Group ID not available
BK -- Backup connection          ST -- Standby connection
PF -- Profile parse failure      PB -- Profile busy
RS -- remote site standby        SN -- Static Neighbor
LB -- Local site not best-site   RB -- Remote site not best-site
VM -- VLAN ID mismatch

Legend for interface status
Up -- operational
Dn -- down

Instance: green
  L2vpn-id: 100:100
  Local-id: 1.1.1.2
    Number of local interfaces: 2
    Number of local interfaces up: 2
    ge-0/3/1.0
    ge-0/3/3.0
    lsi.101711873                Intf - vpls green local-id 1.1.1.2 remote-id
1.1.1.4 neighbor 1.1.1.4
    Remote-id               Type  St     Time last up          # Up trans
    1.1.1.4                 rmt   Up     Jan 31 13:49:52 2012           1
      Remote PE: 1.1.1.4, Negotiated control-word: No
      Incoming label: 262146, Outgoing label: 262146
```

```
    Local interface: lsi.101711873, Status: Up, Encapsulation: ETHERNET
     Description: Intf - vpls green local-id 1.1.1.2 remote-id 1.1.1.4 neighbor
1.1.1.4
   Connection History:
       Jan 31 13:49:52 2012  status update timer
       Jan 31 13:49:52 2012  PE route changed
       Jan 31 13:49:52 2012  Out lbl Update                    262146
       Jan 31 13:49:52 2012  In lbl Update                     262146
       Jan 31 13:49:52 2012  loc intf up               lsi.101711873
 Multi-home:
   Local-site               Id     Pref   State
   test                     1      100    Up
     Number of interfaces: 1
     Number of interfaces up: 1
       ge-0/3/1.0
     Received multi-homing advertisements:
       Remote-PE         Pref   flag   Description
       1.1.1.4           100    0x0
```

show vpls flood event-queue

Syntax show vpls flood event-queue

Release Information Command introduced in Junos OS Release 8.0.

Description Display the pending events in the VPLS flood queue.

Options This command has no options.

Required Privilege Level view

List of Sample Output show vpls flood event-queue on page 191

Output Fields Table 16 on page 191 lists the output fields for the **show vpls flood event-queue** command. Output fields are listed in the approximate order in which they appear.

Table 16: show vpls flood event-queue Output Fields

Field Name	Field Description
Current Pending Event	Provides information on the current event in the VPLS flood event queue.
Name	Name of the event.
Owner Name	Name of the interface associated with the flood event.
Pending Op	Pending operation for the event.
Last Error	Name of the last error encountered.
Number of Retries	Number of attempts made to update the event queue.
Pending Event List	List of the events awaiting processing.
Event Name	Name of the event.
Pending Op	Pending operation for the event.
Event Identifier	Name of the interface associated with the flood event.

Sample Output

show vpls flood event-queue

```
user@host> show vpls flood event-queue
Current Pending Event
    Name:          Flood Nexthop
    Owner Name:ge-4/3/0.0
    Pending Op: ADD
```

```
Last Error:ENOMEM
Number of Retries:3
Pending Event List:
Event Name      Pending Op      Event Identifier
Flood Nexthop   ADD             ge-4/3/0.0
Flood Route     ADD             ge-4/3/0.0
```

show vpls flood instance

Syntax

show vpls flood instance
<brief | detail | extensive>
<instance-name>
<logical-system *logical-system-name*>

Release Information

Command introduced in Junos OS Release 8.0.

Description

Display VPLS information related to the flood process.

Options

none—Display VPLS information related to the flood process for all routing instances.

brief | detail | extensive—(Optional) Display the specified level of output.

instance-name—(Optional) Display VPLS information related to the flood process for the specified routing instance.

logical-system *logical-system-name*—(Optional) Display VPLS information related to the flood process for the specified logical system.

Required Privilege Level

view

List of Sample Output

show vpls flood instance on page 194
show vpls flood instance logical-system-name on page 194
show vpls flood instance detail on page 194

Output Fields

Table 17 on page 193 lists the output fields for the **show vpls flood instance** command. Output fields are listed in the approximate order in which they appear.

Table 17: show vpls flood instance Output Fields

Field Name	Field Description
Logical system	Name of the logical system.
Name	Name of the VPLS routing instance.
CEs	Number of CE routers connected to the VPLS instance.
VEs	Number of VE routers connected to the VPLS instance.
Flood routes	List of all flood routes associated with the VPLS instance.
Prefix	Prefix for the route.
Type	Type of route.
Owner	VPLS routing instance or interface associated with the route.
Nhtype	Next-hop type. For example, **flood** for a flood route.

Table 17: show vpls flood instance Output Fields *(continued)*

Field Name	Field Description
Nhindex	Next-hop index number for the route.

Sample Output

show vpls flood instance

```
user@host> show vpls flood instance

Logical system: __juniper_ls1__
Name: green
CEs: 1
VEs: 1
Flood Routes:
  Prefix    Type          Owner               NhType          NhIndex
  default   ALL_CE_FLOOD  green               flood           383
  0x47/16   CE_FLOOD      fe-1/2/1.0          flood           388
```

show vpls flood instance logical-system-name

```
user@host:__juniper_ls1__> show vpls flood instance juniper_ls1


Logical system: __juniper_ls1__
Name: green
CEs: 1
VEs: 1
Flood Routes:
  Prefix    Type          Owner               NhType          NhIndex
  default   ALL_CE_FLOOD  green               flood           383
  0x47/16   CE_FLOOD      fe-1/2/1.0          flood           388
```

show vpls flood instance detail

```
user@host:__juniper_ls1__> show vpls flood instance detail


Logical system: __juniper_ls1__
Name: green
CEs: 1
VEs: 1
Flood Routes:
  Prefix    Type          Owner               NhType          NhIndex
  default   ALL_CE_FLOOD  green               flood           383
  0x47/16   CE_FLOOD      fe-1/2/1.0          flood           388
```

show vpls flood route

Syntax

show vpls flood route
(all-ce-flood instance-name *instance-name* <logical-system-name *logical-system-name*>
|
ce-flood interface *interface-name*)

Release Information

Command introduced in Junos OS Release 8.0.

Description

Display VPLS route information related to the flood process for either the specified routing instance or the specified interface.

Options

all-ce-flood—Display the flood next-hop route for all customer edge routers for traffic coming from the core of the network.

ce-flood interface *interface-name*—Display the flood next-hop route for traffic coming from the specified customer edge interface.

instance-name *instance-name*—Display the flood routes for the specified instance.

logical-system-name *logical-system-name*—(Optional) Specify the logical system whose flood routes you want to display. You can only specify the default logical system name for VPLS. The default logical system name is **__juniper_ls1__** (the name must be entered in the command with the underscore characters).

Required Privilege Level

view

List of Sample Output

show vpls flood route all-ce-flood on page 196
show vpls flood route ce-flood on page 196

Output Fields

Table 18 on page 195 lists the output for the **show vpls flood route** command. Output fields are listed in the approximate order in which they appear.

Table 18: show vpls flood route Output Fields

Field Name	Field Description
Flood route prefix	Prefix for the flood route.
Flood route type	Type of flood route (either **CE_FLOOD** or **ALL_CE_FLOOD**).
Flood route owner	VPLS routing instance or interface associated with the flood route.
Nexthop type	Next-hop type. For example, **flood** for a flood route.
Nexthop index	Next-hop index number for the route.
Interfaces flooding to	Interfaces to which VPLS routes are being flooded.
Name	Name of the interface.

Table 18: show vpls flood route Output Fields *(continued)*

Field Name	Field Description
Type	Type of VPLS router (**CE** or **VE**).
Nh type	Next-hop type.
Index	Index number for the flood route.

Sample Output

show vpls flood route all-ce-flood

```
user@host:__juniper_ls1__> show vpls flood route all-ce-flood logical-system-name
__juniper_ls1__instance-name green


  Flood route prefix: default
  Flood route type: ALL_CE_FLOOD
  Flood route owner: green
  Nexthop type: flood
  Nexthop index: 383
    Interfaces Flooding to:
    Name             Type          NhType          Index
    fe-1/2/1.0       CE
```

show vpls flood route ce-flood

```
user@host:__juniper_ls1__> show vpls flood route ce-flood interface fe-1/2/1.0


  Flood route prefix: 0x47/16
  Flood route type: CE_FLOOD
  Flood route owner: fe-1/2/1.0
  Nexthop type: flood
  Nexthop index: 388
    Interfaces Flooding to:
    Name             Type          NhType          Index
    lsi.49152        VE             indr            262142
```

show vpls mac-table

Syntax

show vpls mac-table
<**brief | detail | extensive | summary**>
<**bridge-domain** *bridge-domain-name*>
<**instance** *instance-name*>
<**interface** *interface-name*>
<**logical-system (all |** *logical-system-name***)**>
<*mac-address*>
<**vlan-id** *vlan-id-number*>

Release Information

Command introduced in Junos OS Release 8.5.

Description

(MX960 routers only) Display learned VPLS MAC address information.

Options

none—Display all learned VPLS MAC address information.

brief | detail | extensive | summary—(Optional) Display the specified level of output.

bridge-domain ***bridge-domain-name***—(Optional) Display learned VPLS MAC addresses for the specified bridge domain.

instance ***instance-name***—(Optional) Display learned VPLS MAC addresses for the specified instance.

interface ***interface-name***—(Optional) Display learned VPLS MAC addresses for the specified instance.

logical-system (all | ***logical-system-name*****)**—(Optional) Display learned VPLS MAC addresses for all logical systems or for the specified logical system.

mac-address—(Optional) Display the specified learned VPLS MAC address information..

vlan-id ***vlan-id-number***—(Optional) Display learned VPLS MAC addresses for the specified VLAN.

Required Privilege Level

view

List of Sample Output

show vpls mac-table on page 198
show vpls mac-table count on page 199
show vpls mac-table detail on page 199
show vpls mac-table extensive on page 200

Output Fields

Table 19 on page 197 describes the output fields for the **show bridge mac-table** command. Output fields are listed in the approximate order in which they appear.

Table 19: show vpls mac-table Output fields

Field Name	Field Description
Routing instance	Name of the routing instance.

Table 19: show vpls mac-table Output fields *(continued)*

Field Name	Field Description
Bridging domain	Name of the bridging domain.
MAC address	MAC address or addresses learned on a logical interface.
MAC flags	Status of MAC address learning properties for each interface: • **S**—Static MAC address configured. • **D**—Dynamic MAC address learned. • **SE**—MAC accounting is enabled. • **NM**—Nonconfigured MAC.
Logical interface	Name of the logical interface.
MAC count	Number of MAC addresses learned on a specific routing instance or interface.
Learning interface	Logical interface or logical Label Switched Interface (LSI) the address is learned on.
Learn VLAN ID/VLAN	VLAN ID of the routing instance or bridge domain in which the MAC address was learned.
Layer 2 flags	Debugging flags signifying that the MAC address is present in various lists.
Epoch	Spanning Tree Protocol epoch number identifying when the MAC address was learned. Used for debugging.
Sequence number	Sequence number assigned to this MAC address. Used for debugging.
Learning mask	Mask of Packet Forwarding Engines where this MAC address was learned. Used for debugging.
IPC generation	Creation time of the logical interface when this MAC address was learned. Used for debugging.

Sample Output

show vpls mac-table

```
user@host> show vpls mac-table
MAC flags (S -static MAC, D -dynamic MAC,
           SE -Statistics enabled, NM -Non configured MAC)

Routing instance : vpls_ldp1
VLAN : 223
   MAC                MAC      Logical
   address            flags    interface
   00:90:69:9c:1c:5d  D        ge-0/2/5.400

MAC flags (S -static MAC, D -dynamic MAC,
           SE -Statistics enabled, NM -Non configured MAC)

Routing instance : vpls_red
VLAN : 401
   MAC                MAC      Logical
```

```
  address             flags    interface
  00:00:aa:12:12:12   D        lsi.1051138
  00:05:85:74:9f:f0   D        lsi.1051138
```

show vpls mac-table count

```
user@host> show vpls mac-table count
0 MAC address learned in routing instance __juniper_private1__

  MAC address count per interface within routing instance:
    Logical interface        MAC count
    lc-0/0/0.32769                   0
    lc-0/1/0.32769                   0
    lc-0/2/0.32769                   0
    lc-2/0/0.32769                   0
    lc-0/3/0.32769                   0
    lc-2/1/0.32769                   0
    lc-9/0/0.32769                   0
    lc-11/0/0.32769                  0
    lc-2/2/0.32769                   0
    lc-9/1/0.32769                   0
    lc-11/1/0.32769                  0
    lc-2/3/0.32769                   0
    lc-9/2/0.32769                   0
    lc-11/2/0.32769                  0
    lc-11/3/0.32769                  0
    lc-9/3/0.32769                   0

  MAC address count per learn VLAN within routing instance:
    Learn VLAN ID            MAC count
                0                    0

1 MAC address learned in routing instance vpls_ldp1

  MAC address count per interface within routing instance:
    Logical interface        MAC count
    lsi.1051137                      0
    ge-0/2/5.400                     1

  MAC address count per learn VLAN within routing instance:
    Learn VLAN ID            MAC count
                0                    1

1 MAC address learned in routing instance vpls_red

  MAC address count per interface within routing instance:
    Logical interface        MAC count
    ge-0/2/5.300                     1

  MAC address count per learn VLAN within routing instance:
    Learn VLAN ID            MAC count
                0                    1
```

show vpls mac-table detail

```
user@host> show vpls mac-table detail
MAC address: 00:90:69:9c:1c:5d
  Routing instance: vpls_ldp1
   Learning interface: ge-0/2/5.400
   Layer 2 flags: in_ifd, in_ifl, in_vlan, kernel
   Epoch: 0                          Sequence number: 1
```

```
   Learning mask: 0x1                  IPC generation: 0

MAC address: 00:90:69:9c:1c:5d
  Routing instance: vpls_red
   Learning interface: ge-0/2/5.300
   Layer 2 flags: in_ifd, in_ifl, in_vlan, kernel
   Epoch: 0                            Sequence number: 1
   Learning mask: 0x1                  IPC generation: 0
```

show vpls mac-table extensive

```
user@host> show vpls mac-table extensive
MAC address: 00:00:aa:12:12:12
  Routing instance: vpls_ldp1
   Learning interface: lsi.1051137
   Layer 2 flags: in_ifd, in_ifl, in_vlan, kernel
   Epoch: 0                            Sequence number: 1
   Learning mask: 0x1                  IPC generation: 0

MAC address: 00:05:85:74:9f:f0
  Routing instance: vpls_ldp1
   Learning interface: lsi.1051137
   Layer 2 flags: in_ifd, in_ifl, in_vlan, kernel
   Epoch: 0                            Sequence number: 1
   Learning mask: 0x1                  IPC generation: 0

MAC address: 00:90:69:9c:1c:5d
  Routing instance: vpls_ldp1
   Learning interface: ge-0/2/5.400
   Layer 2 flags: in_ifd, in_ifl, in_vlan, kernel
   Epoch: 0                            Sequence number: 1
   Learning mask: 0x1                  IPC generation: 0

MAC address: 00:00:aa:12:12:12
  Routing instance: vpls_red
   Learning interface: lsi.1051138
   Layer 2 flags: in_ifd, in_ifl, in_vlan, kernel
   Epoch: 0                            Sequence number: 0
   Learning mask: 0x1                  IPC generation: 0

MAC address: 00:05:85:74:9f:f0
  Routing instance: vpls_red
   Learning interface: lsi.1051138
   Layer 2 flags: in_ifd, in_ifl, in_vlan, kernel
   Epoch: 0                            Sequence number: 0
   Learning mask: 0x1                  IPC generation: 0
```

show vpls statistics

Syntax

show vpls statistics
<instance *instance-name*>
<logical-system (all | *logical-system-name*)>

Release Information

Command introduced before Junos OS Release 7.4.

Description

(T Series and M Series routers, except for the M160 router) Display virtual private LAN service (VPLS) statistics.

Options

none—Display VPLS statistics for all routing instances.

instance *instance-name*—(Optional) Display VPLS statistics for a specific VPLS routing instance only.

logical-system (all | *logical-system-name*)—(Optional) Perform this operation on all logical systems or on a particular logical system.

Required Privilege Level

view

List of Sample Output

show vpls statistics on page 202
show vpls statistics instance on page 202

Output Fields

Table 20 on page 201 lists the output fields for the **show vpls statistics** command. Output fields are listed in the approximate order in which they appear.

Table 20: show vpls statistics Output Fields

Field Name	Field Description
Instance	Name of the VPLS instance.
Local interface	Name of the local VPLS virtual loopback tunnel interface, **vt-*fpc/pic/port.nnnnn***, where ***nnnnn*** is a dynamically generated virtual port used to transport and receive packets from other provider edge (PE) routers in the VPLS domain.
Index	Number associated with the next hop.
Remote provider edge router	Address of the remote provider edge router.
Multicast packets	Number of multicast packets received.
Multicast bytes	Number of multicast bytes received.
Flood packets	Number of VPLS flood packets received.
Flood bytes	Number of VPLS flood bytes received.

Table 20: show vpls statistics Output Fields *(continued)*

Field Name	Field Description
Current MAC count	Number of MAC addresses learned by the interface and the configured maximum limit on the number of MAC addresses that can be learned.

Sample Output

show vpls statistics

```
user@host> show vpls statistics

VPLS statistics:

Instance: green

   Local interface: fe-2/2/1.0, Index: 69
     Multicast packets:                     1
     Multicast bytes  :                    60
     Flooded packets  :                    18
     Flooded bytes    :                  2556
     Current MAC count:                     1

   Local interface: lt-0/3/0.2, Index: 72
     Multicast packets:                     3
     Multicast bytes  :                   153
     Flooded packets  :                     1
     Flooded bytes    :                    51
     Current MAC count:                     1

   Local interface: lsi.32769, Index: 75
     Current MAC count:                     0

   Local interface: lsi.32771, Index: 77
   Remote PE: 10.255.14.222
     Current MAC count:                     2

Instance: red

   Local interface: vt-0/3/0.32768, Index: 74
     Multicast packets:                     0
     Multicast bytes  :                     0
     Flooded packets  :                     0
     Flooded bytes    :                     0
     Current MAC count:                     0

   Local interface: vt-0/3/0.32770, Index: 76
     Multicast packets:                     0
     Multicast bytes  :                     0
     Flooded packets  :                     0
     Flooded bytes    :                     0
     Current MAC count:                     0
```

show vpls statistics instance

```
user@host> show vpls statistics instance red
```

```
Layer-2 VPN Statistics:
Instance: red

   Local interface: vt-3/2/0.32768, Index: 73
   Remote provider edge router: 10.255.17.35
     Multicast packets:                     0
     Multicast bytes  :                     0
     Flood packets    :                     0
     Flood bytes      :                     0
     Current MAC count:                     1 (Limit 20)
```

PART 4

Index

Index

P

R

S

T

U

V

W