Broadband Subscriber Management Layer 2 Wholesale Solution

Published: 2012-02-28

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

Broadband Subscriber Management Layer 2 Wholesale Solution

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.

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 *Junos OS 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`
Italic text like this	• Introduces 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*

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

Convention	Description	Examples
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; interface names; 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.	
J-Web GUI Conventions		
Bold text like this	Represents J-Web 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 J-Web 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 Broadband Subscriber Management Solutions Guide* relies heavily on existing configuration documentation. In particular, this guide references configuration material presented in the *Junos OS Subscriber Access Configuration Guide*. 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 Access Configuration Guide*
- *Junos OS Layer 2 Configuration Guide*
- *Junos OS Multicast Protocols Configuration Guide*
- *Junos OS Network Interfaces Configuration Guide*
- *Junos OS Policy Framework Configuration Guide*

For other solution examples, see the following Junos OS solutions guides:

- *Junos OS MX Series 3D Universal Edge Routers Solutions Guide*
- *Session Border Control Solutions Guide Using BGF and IMSG*

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 Access Configuration Guide*.

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 Configuration Guide* or the *Junos OS MX Series 3D Universal Edge Routers Solutions Guide*.

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 Configuration Guide* or the *Junos OS MX Series 3D Universal Edge Routers Solutions Guide*.

- **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.

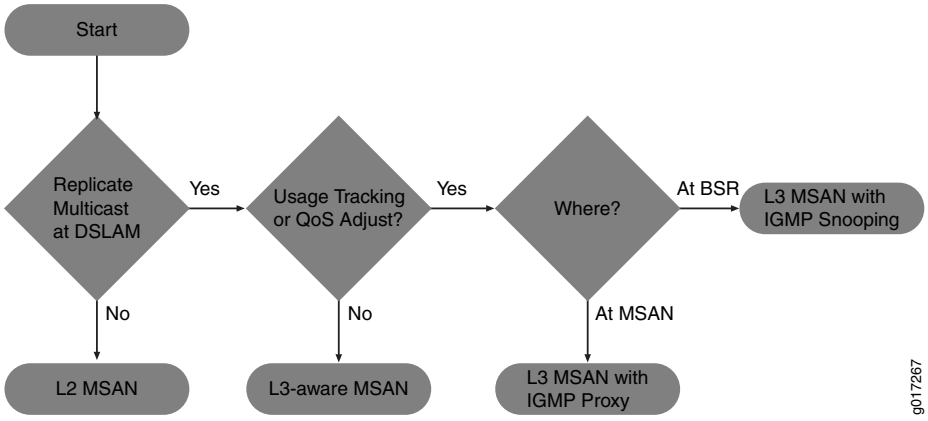
  Layer 2 DSLAMs cannot interpret IGMP, so they cannot selectively replicate IPTV channels.

- **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 Configuration Guide* or the *Junos OS MX Series 3D Universal Edge Routers Solutions Guide*.

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 Configuration Guide* or the *Junos OS MX Series 3D Universal Edge Routers Solutions Guide*.

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 Access Configuration Guide*.

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 Access Configuration Guide*.
- RADIUS-Initiated Change of Authorization (CoA) Overview in the *Junos OS Subscriber Access Configuration Guide*.

- RADIUS-Initiated Disconnect Overview in the *Junos OS Subscriber Access Configuration Guide*.

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 Hardware and JUNOS software. For information about subscriber management hardware support, see Subscriber Access Support Considerations in the *Junos OS Subscriber Access Configuration Guide*. The general configuration options, and considerations for each, are provided below:

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 Access Configuration Guide*.

PART 2

Configuration

CHAPTER 5

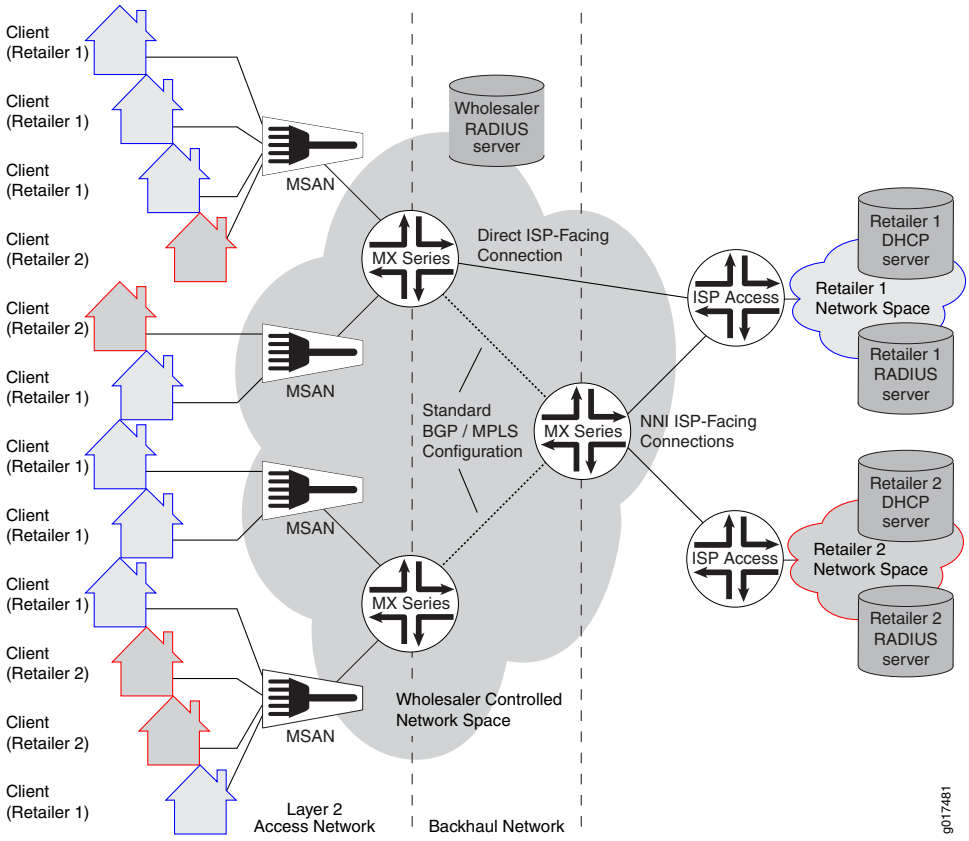
Broadband Subscriber Management Layer 2 Wholesale Network Configuration

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.

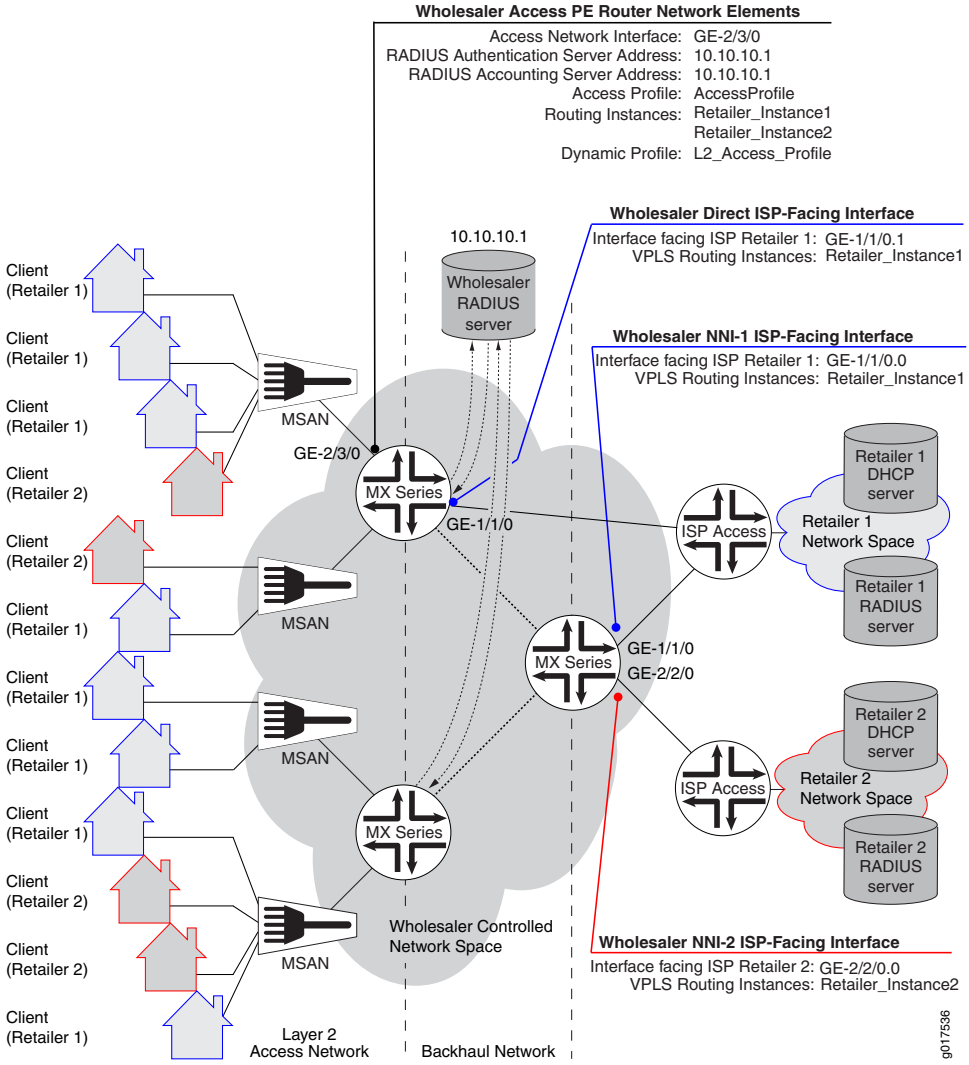
NOTE: You can have more than one ISP router connecting to a single VPLS NNI router with VPLS interfaces configured with routing instances specific to each different ISP-facing interfaces.

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 Configuration Guide* for information about BGP configuration. See the *Junos OS MPLS Applications Configuration Guide* 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 Access Configuration Guide*.

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

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

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;
}
```

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;
        }
      }
    }
  }
}
```

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;
}
```

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;
    }
  }
}
```

PART 3

Administration

CHAPTER 7

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

List of Sample Output
show network-access aaa statistics accounting on page 52
show network-access aaa statistics address-assignment client on page 52
show network-access aaa statistics address-assignment pool on page 52
show network-access aaa statistics dynamic-requests on page 52
show network-access aaa statistics radius on page 52

Output Fields Table 8 on page 50 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.
Requests timedout	Number of accounting requests to the accounting server that timed out.
Client	Client type; for example, DHCP, Mobile IP, PPP.

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

Field Name	Field Description
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.
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

List of Sample Output show network-access aaa statistics authentication on page 55
show network-access aaa statistics authentication detail on page 55

Output Fields Table 9 on page 53 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
Malformed reply	Number of malformed replies received from the RADIUS authentication server.	Detail

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

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

Sample Output

show network-access aaa statistics authentication

```
user@host> show network-access aaa statistics authentication
Authentication module statistics
  Requests received: 2118
  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

List of Sample Output
show network-access aaa subscribers logical-system on page 57
show network-access aaa subscribers logical-system routing-instance on page 57
show network-access aaa subscribers statistics username on page 57
show network-access aaa subscribers username on page 58

Output Fields Table 10 on page 56 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.
INTERIM sent successfully	Number of accounting interim requests generated by the AAA framework for this subscriber.

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

Field Name	Field Description
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 8

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 Switches 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 *Junos OS Policy Framework Configuration Guide*. For related operational mode commands, see the *Junos OS Routing Protocols and Policies Command Reference*.

Required Privilege Level view

List of Sample Output
show interfaces filters on page 61
show interfaces filters interface-name on page 61
show interfaces filters (PTX Series Packet Transport Switches) on page 61

Output Fields Table 11 on page 60 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 Switches)

```
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 Configuration Guide*. For information about related operational mode commands for routing instances and protocols, see the *Junos OS Routing Protocols and Policies Command Reference*.

Required Privilege Level
view

List of Sample Output
show interfaces routing brief on page 63
show interfaces routing brief (TX Matrix Plus Router) on page 64
show interfaces routing detail on page 64
show interfaces routing detail (TX Matrix Plus Router) on page 65

Output Fields
Table 12 on page 62 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 68
show interfaces routing-instance all on page 68
show interfaces routing-instance extensive on page 68

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 9

Subscriber Management Subscriber CLI Commands

show subscribers

Syntax

show subscribers
<address *address*>
<client-type *client-type*>
<interface *interface*>
<logical-system *logical-system*>
<mac-address *mac-address*>
<profile-name *profile-name*>
<routing-instance *routing-instance*>
<stacked-vlan-id *stacked-vlan-id*>
<subscriber-state *subscriber-state*>
<vlan-id *vlan-id*>
<count | detail | extensive | summary (all | logical-system *logical-system* | routing-instance *routing-instance*) | terse>

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**, **extensive**, and **summary** 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.

Description

Display information for active subscribers.

Options

address—(Optional) Display subscribers whose IP address matches the specified address.

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.

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).

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.

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

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

Required Privilege Level view

List of Sample Output

Output Fields Table 13 on page 74 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
User Name	Name of subscriber.
Type	Subscriber client type (DHCP, L2TP, PPP, PPPoE, STATIC-INTERFACE, VLAN).
IP Address	Subscriber IPv4 address.
IP Netmask	Subscriber IP netmask.
IPv6 Address	Subscriber IPv6 address, or multiple addresses.
IPv6 Prefix	Subscriber IPv6 prefix.
IPv6 Address Pool	Subscriber IPv6 address pool. The IPv6 address pool is used to allocate IPv6 prefixes to the DHCPv6 clients.
IPv6 Network Prefix Length	Length of the network portion of the IPv6 address.
IPv6 Prefix Length	Length of the subscriber IPv6 prefix.
Logical System	Logical system associated with the subscriber.
Routing Instance	Routing instance associated with the subscriber.
Interface	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.
Interface Type	Whether the subscriber interface is **Static** or **Dynamic**.
Dynamic Profile Name	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**).
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.

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

Field Name	Field Description
DHCP Relay IP Address	IP address used by the DHCP relay agent.
Login Time	Date and time at which the subscriber logged in.
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.
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.
ADF IPv4 Input Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv4 input filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
ADF IPv4 Output Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv4 output filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
ADF IPv6 Input Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv6 input filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
ADF IPv6 Output Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv6 output filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
IPv4 Input Filter Name	Name assigned to the IPv4 input filter (client or service session).
IPv4 Output Filter Name	Name assigned to the IPv4 output filter (client or service session).
IPv6 Input Filter Name	Name assigned to the IPv6 input filter (client or service session).
IPv6 Output Filter Name	Name assigned to the IPv6 output filter (client or service session).
IFL Input Filter Name	Name assigned to the logical interface input filter (client or service session).
IFL Output Filter Name	Name assigned to the logical interface output filter (client or service session).

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

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. Summary information includes subscriber counts per state and the total number of subscribers.
Subscribers by Client Type	Number of subscribers summarized by client type. Client types can include DHCP, VLAN, PPP, PPPOE, L2TP, and static. Summary information includes subscriber counts per client type and the total number of subscribers.
Subscribers by LS:RI	Number of subscribers summarized by logical system:routing instance (LS:RI) combination. Summary information includes subscriber counts per LS:RI and the total number of subscribers.

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 suscribers (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 detail (IPv4)

```
user@host> show subscribers 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
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 (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 interface

```
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

```
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 count

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

show subscribers routing-instance inst1 count

```
user@host> show subscribers routing-instance inst1 count
Total Subscribers: 188, Active Subscribers: 183
```

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 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 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 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 (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 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 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 10

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*>
<logical-system (all | *logical-system-name*)>
<status>
<summary>

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) 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.

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 90
show vpls connections extensive (Static VPLS Neighbors) on page 92

Output Fields

Table 14 on page 85 lists the output fields for the **show vpls connections** command. Output fields are listed in the approximate order in which they appear.

Table 14: 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.
Range	Label block range.

Table 14: show vpls connections Output Fields *(continued)*

Field Name	Field Description
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 14: show vpls connections Output Fields *(continued)*

Field Name	Field Description
St	

Table 14: 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 14: 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 14: 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
```

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 94

Output Fields Table 15 on page 94 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 15: 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 97
show vpls flood instance logical-system-name on page 97
show vpls flood instance detail on page 97

Output Fields

Table 16 on page 96 lists the output fields for the **show vpls flood instance** command. Output fields are listed in the approximate order in which they appear.

Table 16: 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 16: 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 99
show vpls flood route ce-flood on page 99

Output Fields

Table 17 on page 98 lists the output for the **show vpls flood route** command. Output fields are listed in the approximate order in which they appear.

Table 17: 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 17: 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 101
show vpls mac-table count on page 102
show vpls mac-table detail on page 102
show vpls mac-table extensive on page 103

Output Fields Table 18 on page 100 describes the output fields for the **show bridge mac-table** command. Output fields are listed in the approximate order in which they appear.

Table 18: show vpls mac-table Output fields

Field Name	Field Description
Routing instance	Name of the routing instance.

Table 18: 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 105
show vpls statistics instance on page 105

Output Fields

Table 19 on page 104 lists the output fields for the **show vpls statistics** command. Output fields are listed in the approximate order in which they appear.

Table 19: 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 19: 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

Symbols

A

B

C

D

E

F

H

I

L