

## Chapter 7

# VPLS Overview

This chapter describes the virtual private LAN service (VPLS), and contains the following sections:

- VPLS Overview on page 531
- VPLS Components on page 532
- VPLS and Transparent Bridging on page 534
- BGP Signaling for VPLS on page 535
- LDP Signaling for VPLS on page 535
- VPLS Supported Features on page 536
- VPLS Platform Considerations on page 537
- VPLS References on page 538

### VPLS Overview

---

JUNOS software enables you to configure one or more instances of VPLS, referred to as *VPLS instances*, on the router. VPLS employs an Ethernet-based layer 2 VPN to connect multiple individual LANs across a service provider's MPLS core network. The geographically dispersed multiple LANs function as a single virtual LAN.

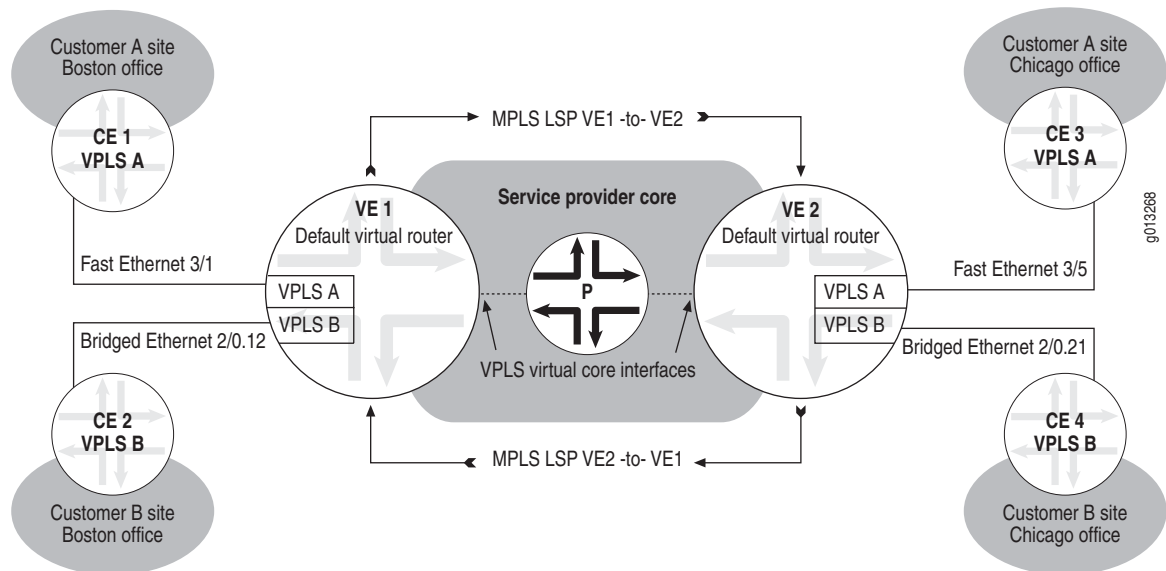
VPLS preserves the broadcast and multicast capabilities of the physical LANs. Consequently, any broadcast or multicast traffic from a given customer end station is sent to all sites that participate in the VPLS instance.

You can use either BGP or LDP to provide signaling for VPLS, as follows:

- BGP signaling—VPLS with BGP signaling, which is referred to as BGP-based VPLS, uses BGP as the protocol that signals reachability for the VPLS domain in which the VPLS instance participates. You must configure BGP on each VPLS edge (VE) device in your topology to provide signaling for each VPLS domain.
- LDP signaling—VPLS with LDP signaling, which is referred to as LDP-based VPLS, uses LDP as the protocol that signals reachability for the VPLS domain in which the VPLS instance participates. You must configure LDP on each VE device in your topology to provide signaling for each VPLS domain.

Figure 120 illustrates an example of a simple VPLS topology. The basic topology of a VPLS network is the same regardless of whether BGP signaling or LDP signaling is used.

**Figure 120: VPLS Sample Topology**



## Related Topics

- BGP Signaling for VPLS on page 535
- Configuration Tasks for VPLS with BGP Signaling in *Chapter 8, Configuring VPLS*
- LDP Signaling for VPLS on page 535
- Configuration Tasks for VPLS with LDP Signaling in *Chapter 8, Configuring VPLS*
- *Chapter 3, Configuring BGP-MPLS Applications*
- *Chapter 11, Configuring L2VPNs*

## VPLS Components

---

As illustrated in Figure 120, a typical VPLS topology consists of the following components.

### VPLS Domains

Typically, a *VPLS domain* is associated with customers who want to use Ethernet-based layer 2 VPNs to connect geographically dispersed sites in their organization across an MPLS-based service provider core, also known as an MPLS backbone. Each VPLS domain consists of the set of VPLS edge routers running the corresponding VPLS instance that participates in that domain.

Figure 120 depicts two VPLS domains: VPLS A and VPLS B. The VPLS A domain connects Customer A's Boston and Chicago offices, and consists of VPLS edge routers VE 1 and VE 2, each of which runs a VPLS instance named *vplsA*. Similarly, the VPLS B domain connects Customer B's Boston and Chicago offices, and consists of VPLS edge routers VE 1 and VE 2, each of which also runs a VPLS instance named *vplsB*.

### Customer Edge Devices

Figure 120 on page 532 shows four customer edge (CE) devices: CE 1, CE 2, CE 3, and CE 4. Each CE device is located at the edge of a customer site, and participates in one or more VPLS domains. In the sample topology, CE 1 and CE 3 are members of the VPLS A domain, and CE 2 and CE 4 are members of the VPLS B domain.

A CE device can be a single host, a switch, or, most typically, a router. Each CE device is directly connected to a VPLS edge router by means of an Ethernet or bridged Ethernet network interface, but does not run VPLS. From the perspective of the CE device, the entire VPLS network appears to be a single layer 2 switch that can switch layer 2 packets, learn and filter on media access control (MAC) addresses, and flood packets that have unknown MAC destination addresses (DAs).

### VPLS Edge Devices

In a VPLS configuration, E-series routers function as VPLS edge (VE) devices, which are also referred to as VE routers or, simply, VEs. A VE router is analogous to a provider edge (PE) router in BGP, LDP, and MPLS configurations, and performs similar functions.

Figure 120 on page 532 depicts two VE routers: VE 1, which is the local router, and VE 2, which is the remote router located at the other side of the service provider core. Each VE router must have a VPLS instance configured for each VPLS domain in which it participates. Consequently, the sample topology comprises a total of four separate VPLS instances: instances *vplsA* and *vplsB* configured on VE 1, and instances *vplsA* and *vplsB* configured with matching route target values on VE 2.

Each VPLS instance configured on the router is associated with two types of interfaces, also known as ports. The CE-facing interface is an Ethernet or bridged Ethernet network interface that directly connects the VE router to each CE device. The VPLS virtual core interface, although not an actual physical interface, is automatically generated by the router for each VPLS instance and represents all of the MPLS tunnels from the router to the remote VE devices. The router encapsulates Ethernet frames from the CE device in an MPLS packet and then forwards the encapsulated frames to the service provider core through the provider (P) router. This encapsulation is identical to Martini encapsulation for Ethernet layer 2 services over MPLS.

Each VE router in the sample topology has a total of two network interfaces and two VPLS virtual core interfaces configured, one interface of each type per VPLS instance.

## VPLS and Transparent Bridging

A single VPLS instance is analogous to a distributed learning bridge (also known as a bridge group) used for transparent bridging, and performs similar functions. In effect, a VPLS instance is a new or existing bridge group that has additional VPLS attributes configured.

A bridge group is a collection of bridge interfaces stacked on Ethernet layer 2 interfaces to form a broadcast domain. Similarly, a VPLS instance is a collection of network interfaces stacked on Ethernet layer 2 interfaces that transmits packets between the router, or VE device, and the CE device located at the edge of the customer's network. In addition, the VPLS virtual core interface enables a VPLS instance to forward traffic not only between bridge interfaces, like a bridge group, but also between a bridge (network) interface and the service provider core.

Like a bridge group, each VPLS instance maintains its own set of forwarding tables and filters that enables it to learn the network topology by examining the media access control (MAC) source address of every incoming packet. The VPLS instance then creates an entry in its forwarding table that includes the MAC address and associated network interface where the packet was received. For traffic on the VPLS virtual core interface, the VPLS instance captures additional information that includes an outgoing MPLS label used to reach the remote site and an incoming MPLS label used to process traffic received from the remote site.

Table 44 through Table 47 represent the forwarding tables on VE 1 and VE 2 for the sample VPLS topology illustrated in Figure 120 on page 532.

**Table 44: VPLS Forwarding Table on VE 1 for VPLS A**

Interface	MAC Address	Outgoing Label	Received Label
Fast Ethernet 3/1	1a1a.1a1a.1a1a	–	–
VPLS virtual core interface	3a3a.3a3a.3a3a	18	324

**Table 45: VPLS Forwarding Table on VE 1 for VPLS B**

Interface	MAC Address	Outgoing Label	Received Label
Bridged Ethernet 2/0.12	2b2b.2b2b.2b2b	–	–
VPLS virtual core interface	4b4b.4b4b.4b4b	25	526

**Table 46: VPLS Forwarding Table on VE 2 for VPLS A**

Interface	MAC Address	Outgoing Label	Received Label
Fast Ethernet 3/5	3a3a.3a3a.3a3a	–	–
VPLS virtual core interface	1a1a.1a1a.1a1a	42	107

**Table 47: VPLS Forwarding Table on VE 2 for VPLS B**

Interface	MAC Address	Outgoing Label	Received Label
Bridged Ethernet 2/0.21	4b4b.4b4b.4b4b	–	–
VPLS virtual core interface	2b2b.2b2b.2b2b	63	872

## BGP Signaling for VPLS

BGP multiprotocol extensions (MP-BGP) enable BGP to support IPv4 services such as BGP/MPLS VPNs, which are sometimes known as RFC 2547bis VPNs. VPLS with BGP signaling is actually a BGP-MPLS application that has much in common with BGP/MPLS VPNs.

The procedures for configuring BGP signaling for BGP/MPLS VPNs and for VPLS are similar except, for VPLS, you must configure both of the following BGP address families:

- L2VPN—The L2VPN address family enables you to configure the VE router to exchange layer 2 network layer reachability information (NLRI) for all VPLS instances. Optionally, you can use the **signaling** keyword for the L2VPN address family to specify BGP signaling of L2VPN reachability information. Currently, you can omit the **signaling** keyword with no adverse effects.
- VPLS—The VPLS address family enables you to configure the VE router to exchange layer 2 NLRI for a specified VPLS instance.

BGP can exchange information in a VPLS topology within these address families. Specifically, BGP builds a full mesh of label-switched paths (LSPs) among all of the VPLS instances on each of the VPLS edge routers participating in a particular VPLS domain.

## Related Topics

- Configuring BGP Signaling for VPLS on page 552

- *Chapter 1, Configuring BGP Routing*
- *Chapter 3, Configuring BGP-MPLS Applications*

## LDP Signaling for VPLS

---

When you configure VPLS with LDP signaling, LDP supports a full mesh of pseudowires among the participating VE routers. This is analogous to BGP signaling, in which BGP builds a full mesh of label-switched paths (LSPs) among all of the VPLS instances on each of the VE routers participating in a particular VPLS domain.

### Targeted Sessions

LDP establishes targeted sessions to the remote VEs configured at the edge of the service provider's MPLS core network. The number of targeted sessions supported for a local VE router is equal to the total number of other VE routers that participate in the VPLS instances configured on the local VE. As is the case with Martini encapsulation for Ethernet layer 2 services over MPLS, a targeted session to a remote VE can have many pseudowires that terminate at the same remote VE.

To enable LDP to establish targeted sessions with remote VEs across the MPLS core, you must issue both the **mpls ldp vpls-id** command to configure a VPLS identifier for the VPLS instance, and the **mpls ldp vpls neighbor** command to configure a list of neighbor (peer) addresses to which LDP can send or from which LDP can receive targeted hello messages.

### PWid FEC Element TLV

LDP signaling information for VPLS is carried in a label mapping message. The label mapping message contains the Generic Label type-length-value (TLV), and the pseudowire identifier (PWid) forwarding equivalence class (FEC) element. A FEC is a group of IP packets forwarded over the same path with the same path attributes applied.

The PWid FEC element (FEC Type 128 or 0x80) contains the VPLS identifier information configured for your VPLS instance with the **mpls ldp vpls-id** command. Taken together, the pseudowire type field and the PWid field in the TLV represent a unique VPLS instance. The pseudowire type field is Ethernet to identify the pseudowires that carry Ethernet traffic for multipoint connectivity between the local and remote VEs. The PWid field is a nonzero 32-bit integer that contains the VPLS identifier, which is a globally unique identifier for a VPLS domain. All VEs that participate in the same VPLS domain must use the same VPLS identifier.

Martini encapsulation for Ethernet layer 2 services over MPLS also uses the PWid FEC Element TLV. As a result, the PWid for Martini configurations must not be the same as the VPLS identifier configured for a VPLS instance. To prevent this conflict from occurring, the JUNOS software displays an error and rejects the configuration if you attempt to configure the same value for the Martini PWid and the VPLS identifier.

### Related Topics

- [Configuring LDP Signaling for VPLS on page 559](#)

- *Chapter 2, Configuring MPLS.*

## VPLS Supported Features

---

The JUNOS implementation of VPLS provides the following features:

- Single-level VPLS hierarchy within a single autonomous system (AS) using MPLS tunneling technology for the core
- Support for the following types of network interfaces between the VE router and the CE device:
  - Bridged Ethernet over ATM1483 subinterfaces
  - Fast Ethernet
  - Gigabit Ethernet
  - 10-Gigabit Ethernet
  - VLAN and S-VLAN subinterfaces over bridged Ethernet, Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet interfaces
- Autodiscovery of VPLS instance members using MP-BGP
- VPLS signaling using MP-BGP to set up and tear down the pseudowires that constitute a VPLS instance
- VPLS signaling using LDP and the PWh FEC element (FEC Type 128) to set up and tear down the pseudowires that constitute a VPLS instance
- Interworking of the VPLS instance and the VPN routing and forwarding instance (VRF) using an external cable connection
- Class of service (CoS)
- Inter-AS option A, inter-AS option B, and inter-AS option C services
- Minimal filtering and policing support

As with L2VPNs, VPLS does not support BGP multipaths.

## VPLS Platform Considerations

---

VPLS is supported on all E-series routers.

## Module Requirements

You can configure VPLS network interfaces on all E-series module combinations that support transparent bridging. The VPLS virtual core interface can exist on all E-series module combinations that support MPLS tunnels.

For information about the modules that support VPLS network interfaces and VPLS virtual core interfaces on ERX-14xx models, ERX-7xx models, and ERX-310 routers:

- See *ERX Module Guide, Table 1, Module Combinations* for detailed module specifications.
- See *ERX Module Guide, Appendix A, Module Protocol Support* for information about the modules that support VPLS network interfaces and VPLS virtual core interfaces.

For information about the modules that support VPLS network interfaces and VPLS virtual core interfaces on E120 routers and E320 routers:

- See *E120 and E320 Module Guide, Table 1, Modules and IOAs* for detailed module specifications.
- See *E120 and E320 Module Guide, Appendix A, IOA Protocol Support* for information about the modules that support VPLS network interfaces and VPLS virtual core interfaces.

## Interface Specifiers

The configuration task examples in this chapter use the *slot/port[.subinterface]* format to specify the physical interface on which to configure a VPLS network interface. However, the interface specifier format that you use depends on the router that you are using.

For ERX-7xx models, ERX-14xx models, and ERX-310 routers, use the *slot/port[.subinterface]* format. For example, the following command specifies Fast Ethernet subinterface 6 on port 2 of the I/O module installed in slot 3 of an ERX-7xx model, ERX-14xx model, or ERX-310 router.

```
host1(config)#interface fastEthernet 3/2.6
```

For E120 and E320 routers, use the *slot/adaptor/port[.subinterface]* format, which includes an identifier for the bay in which the I/O adapter (IOA) resides. In the software, the upper IOA bay is identified as adaptor 0; the lower IOA bay is identified as adaptor 1. For example, the following command specifies Gigabit Ethernet subinterface 20 on port 1 of the IOA installed in the upper adaptor bay (adaptor 0) of slot 4 in an E320 router.

```
host1(config)#interface gigabitEthernet 4/0/1.20
```



## Related Topics

- For more information about supported interface types and specifiers on E-series routers, see *Interface Types and Specifiers* in *JUNOS Command Reference Guide, About This Guide*.

## VPLS References

---

For more information about VPLS, consult the following resources:

- *JUNOS Release Notes, Appendix A, System Maximums*—Refer to the Release Notes corresponding to your software release for information about the maximum values supported for VPLS configuration.
- RFC 3036—LDP Specification (January 2001)
- RFC 4447—Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP) (April 2006)
- RFC 4762—Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling (January 2007)
- Virtual Private LAN Service—draft-ietf-l2vpn-vpls-bgp-05.txt (October 2005 expiration)



**NOTE:** IETF drafts are valid for only 6 months from the date of issuance. They must be considered as works in progress. Please refer to the IETF Web site at <http://www.ietf.org> for the latest drafts.

---

