

Chapter 9

Configuring L2VPNs

This chapter describes how to configure Layer 2 Virtual Private Networks (L2VPNs) on the router, and contains the following sections:

- Before You Configure L2VPNs on page 597
- L2VPN Configuration Tasks on page 598
- Configuring an L2VPN Instance on page 600
- Configuring Customer-facing Interfaces in the L2VPN Instance on page 601
- Configuring a Local Cross-Connect on page 602
- Configuring the Loopback Interface and Router ID for BGP on page 603
- Configuring BGP Signaling on page 604
- Configuring MPLS LSPs on page 606
- L2VPN Configuration Example on page 607

Before You Configure L2VPNs

The JUNOS software implementation of L2VPNs uses features of BGP, MPLS, BGP/MPLS VPNs, and layer 2 services over MPLS. We recommend you have a thorough understanding of these protocols before you configure and use L2VPNs in your network.

Related Topics

For more information about configuring BGP, MPLS, BGP/MPLS VPNs, and layer 2 services over MPLS, see the following chapters in this guide:

- *Chapter 1, Configuring BGP Routing*
- *Chapter 2, Configuring MPLS*
- *Chapter 3, Configuring BGP-MPLS Applications*
- *Chapter 4, Layer 2 Services over MPLS Overview*

- *Chapter 5, Configuring Layer 2 Services over MPLS*
- *Chapter 6, Monitoring Layer 2 Services over MPLS*
- For more information about configuring the layer 2 interfaces that support L2VPNs, see *JUNOS Physical Layer Configuration Guide, Chapter 5, Configuring Ethernet Interfaces*.

L2VPN Configuration Tasks

To configure a PE router to provide L2VPNs:

1. Configure an L2VPN instance.
 - a. Configure the encapsulation type and create an L2VPN instance on the PE router for each L2VPN in which the router participates.
 - b. Configure a customer site name and a unique site identifier for each customer site that belongs to the L2VPN instance.
 - c. Configure the maximum number of customer sites that can participate in the L2VPN.
 - d. Configure the unique two-part route distinguisher for the L2VPN instance.
 - e. Create a list of L2VPN extended communities that the router uses to determine which routes are imported by the L2VPN instance.
 - f. Configure the L2VPN local preference options for control words and sequencing.
2. Configure the customer-facing interfaces in the L2VPN instance.
 - a. Configure the layer 2 interfaces that connect the PE router to each CE device in the L2VPN.
 - b. Configure each layer 2 interface as a member of an L2VPN instance by specifying local and remote site IDs.
3. (Optional) Configure local cross-connects.
 - a. Configure two sites in the L2VPN instance that are local to the PE router.
 - b. Configure the correct local and remote site IDs on the customer-facing interfaces for the cross-connected sites.
4. Configure the loopback interface and router ID for BGP.
 - a. Configure a loopback interface to use as the update source for the TCP connection.
 - b. Assign a router ID that uses the IP address of the loopback interface.

5. Set up BGP signaling in the autonomous system that is configured to signal reachability for this L2VPN instance.
 - a. Enable BGP.
 - b. Configure the PE-to-PE BGP session.
 - c. Create the L2VPN address family to configure the router to use BGP signaling.
 - d. Activate the neighbors in the L2VPN address family for the PE-to-PE BGP session.
 - e. Create the VPWS address family to configure the router to exchange layer 2 NLRI for each L2VPN instance configured on the router.
6. Configure MPLS label-switched paths (LSPs) to connect the local and remote PE routers.
 - a. Enable MPLS on the virtual router.
 - b. Configure the core-facing interface on which you want to enable MPLS, Label Distribution Protocol (LDP), and topology-driven LSPs.
 - c. Enable MPLS on the core-facing interface.
 - d. Enable LDP and topology-driven LSPs on the core-facing interface.

Related Topics

- *Configuring BGP Signaling on page 604.*
- *Configuring a Local Cross-Connect on page 602.*
- *Configuring an L2VPN Instance on page 600.*
- *Configuring Customer-facing Interfaces in the L2VPN Instance on page 601.*
- *Configuring the Loopback Interface and Router ID for BGP on page 603.*
- *Configuring MPLS LSPs on page 606.*
- See *L2VPN Configuration Example on page 607* for a detailed sample configuration.

Configuring an L2VPN Instance

You must configure an L2VPN instance for each L2VPN in which the router participates. From a configuration standpoint, an L2VPN instance is simply a new L2VPN that you configure with additional L2VPN attributes.

Table 59 lists the commands that you use to configure a basic L2VPN instance.

Table 59: Commands to Configure Basic L2VPN Instances

l2vpn control-word	l2vpn route-target
l2vpn encapsulation-type	l2vpn sequencing
l2vpn local-site-id remote-site-id	l2vpn site-name site-id
l2vpn rd	l2vpn site-range

To configure a basic L2VPN instance on the PE router:

1. Create the L2VPN by configuring the encapsulation type for all interfaces in the L2VPN.

You must issue this command before any other **l2vpn** commands.

```
host1(config)#l2vpn exampleco encapsulation-type ethernet
```

2. Configure the maximum number of customer sites that can participate in the L2VPN.

```
host1(config)#l2vpn exampleco site-range 10
```

3. Configure the name and ID number for the customer sites in the L2VPN instance.

The site ID value must be greater than zero and be unique within the L2VPN for that customer site.

```
host1(config)#l2vpn exampleco site-name westford site-id 1
```

4. Configure a route distinguisher for the L2VPN.

In this example, the first number in the route distinguisher (100) is the number of the autonomous system (AS). The second number in the route distinguisher (11) uniquely identifies the L2VPN instance within that AS.

```
host1(config)#l2vpn exampleco rd 100:11
```

5. Create or add a route target to the import and export lists of the L2VPN's route-target extended community.

The PE router uses the lists to determine which routes are imported into the L2VPN instance.

```
host1(config)#l2vpn exampleco route-target both 100:1
```

6. Specify the local preference for use of the control word and sequencing for the layer 2 packets encapsulated in the MPLS packets that are sent to the remote PE router.

```
host1(config)#l2vpn exampleco control-word
host1(config)#l2vpn exampleco sequencing
```

Related Topics

- **l2vpn control-word** command
- **l2vpn encapsulation-type** command
- **l2vpn rd** command
- **l2vpn route-target** command
- **l2vpn sequencing** command
- **l2vpn site-name site-id** command
- **l2vpn site-range** command

Configuring Customer-facing Interfaces in the L2VPN Instance

You must configure one of the following types of interfaces as a member of the L2VPN to transmit packets between the PE router and each CE device to which the PE router is connected:

- ATM (AAL5 VCC transport or ATM VCC cell transport)
- Cisco HDLC
- Ethernet (Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet)
- Frame Relay
- PPP
- VLAN and S-VLAN subinterfaces over Fast Ethernet, Gigabit Ethernet, or 10-Gigabit Ethernet interfaces

To configure a customer-facing interface for an L2VPN instance:

1. Access Interface Configuration mode for a layer 2 interface for the L2VPN on the PE router.

```
host1(config)#interface fastEthernet 4/0
```

2. Configure the local and remote site IDs on the interface to specify the interface as a member of the L2VPN.

```
host1(config-if)#l2vpn exampleco local-site-id 1 remote-site-id 2
host1(config-if)#exit
```

3. Repeat for all customer-facing interfaces in the L2VPN.

```
host1(config)#interface fastEthernet 4/1
host1(config-if)#l2vpn exampleco local-site-id 1 remote-site-id 3
host1(config-if)#exit
```

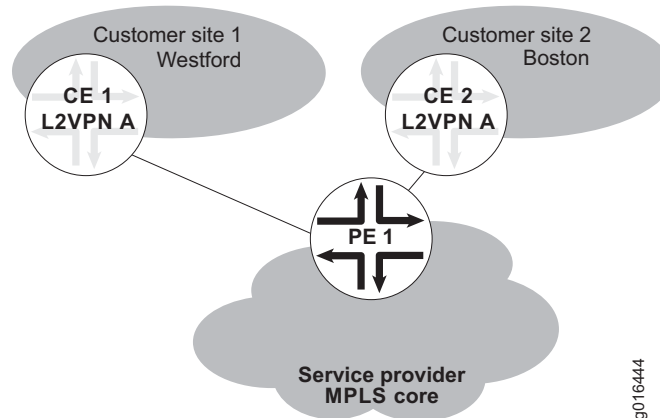
Related Topics

- `interface fastEthernet` command
- `l2vpn local-site-id remote-site-id` command

Configuring a Local Cross-Connect

You configure a local cross-connect between two local customer sites by first configuring the two local sites and then configuring the correct local and remote site IDs on the two local interfaces that you are cross-connecting. Figure 125 illustrates cross-connects by showing a portion of a sample L2VPN topology.

Figure 125: L2VPN Cross-connects



The following example shows the creation of a cross-connect between sites Westford and Boston. On one customer-facing interface, Westford is considered local and Boston is remote; on the other customer-facing interface, Boston is considered local and Westford is remote. From the perspective of the PE router, both sites are local.

To configure a local cross-connect between two local sites:

1. Configure the two local sites.

```
host1(config)#l2vpn exampleco encapsulation-type ethernet
host1(config)#l2vpn exampleco site-name westford site-id 1
host1(config)#l2vpn exampleco site-name boston site-id 2
host1(config)#l2vpn exampleco site-range 10
host1(config)#l2vpn exampleco rd 100:11
host1(config)#l2vpn exampleco route-target both 100:1
```

2. Configure the correct local and remote site IDs on the two local interfaces that are being cross-connected.

```
host1(config)#interface fastEthernet 4/0
host1(config-if)#l2vpn exampleco local-site-id 1 remote-site-id 2
host1(config-if)#exit

host1(config)#interface fastEthernet 4/1
host1(config-if)#l2vpn exampleco local-site-id 2 remote-site-id 1
host1(config-if)#exit
```

Related Topics

- *Configuring an L2VPN Instance on page 600.*
- *Configuring Customer-facing Interfaces in the L2VPN Instance on page 601.*

Configuring the Loopback Interface and Router ID for BGP

To establish a BGP session, BGP uses the IP address of the outgoing interface towards the BGP peer as the update source IP address for the TCP connection over which the BGP session runs. Typically, you configure a loopback interface as the update source interface because a loopback interface is inherently stable.

After you configure the loopback interface, use the **ip router-id** command to assign a router ID to uniquely identify the router within a BGP AS. The router ID is the IP address of the loopback interface.

To configure the loopback interface and router ID on the PE router:

1. Configure a loopback interface on the PE router and assign an IP address to the interface.

```
host1(config)#interface loopback 0
host1(config-if)#ip address 10.3.3.3 255.255.255.255
host1(config-if)#exit
```

2. Assign the router ID using the IP address you configured for the loopback interface.

```
host1(config)#ip router-id 10.3.3.3
```

Related Topics

- `interface loopback` command
- `ip address` command
- `ip router-id` command

Configuring BGP Signaling

This section describes one way to configure BGP signaling for L2VPNs, but does not provide complete details about configuring BGP and BGP/MPLS VPNs.

Table 60 lists the commands used in this section to configure BGP signaling for L2VPNs.

Table 60: Commands to Configure BGP Signaling for L2VPNs

<code>address-family l2vpn</code>	<code>neighbor next-hop-self</code>
<code>address-family vpws</code>	<code>neighbor remote-as</code>
<code>exit-address-family</code>	<code>neighbor update-source</code>
<code>neighbor activate</code>	<code>router bgp</code>

To configure BGP signaling for an L2VPN on the PE router:

1. Enable the BGP routing process on the PE router in the specified local AS.

The AS number identifies the PE router to other BGP routers.

```
host1(config)#router bgp 738
```

2. Configure the PE-to-PE BGP session. Use **neighbor** commands to specify the PE router peers to which BGP advertises routes and to configure additional BGP attributes.

```
host1(config-router)#neighbor 10.2.2.2 remote-as 738
host1(config-router)#neighbor 10.2.2.2 update-source loopback 0
host1(config-router)#neighbor 10.2.2.2 next-hop-self
```

3. Create the L2VPN address family to configure the router to use BGP signaling to exchange layer 2 NLRI to peer PE routers for all L2VPN (VPWS) instances.

Optionally, you can use the **signaling** keyword with the **address-family** command when you configure the L2VPN address family to specify BGP signaling of L2VPN reachability information. Currently, you can omit the **signaling** keyword with no adverse effects.

```
host1(config-router)#address-family l2vpn signaling
```


4. Activate the neighbors with which routes of the L2VPN address family are exchanged for this PE-to-PE BGP session. Use the **bgp dampening** command and BGP **neighbor** commands to configure additional address family parameters for the session. No other commands are supported in this address family.

```
host1(config-router-af)#neighbor 10.2.2.2 activate
host1(config-router-af)#neighbor 10.2.2.2 next-hop-self
```

5. Exit the address family.

```
host1(config-router-af)#exit-address-family
```

6. Create the VPWS address family to configure the router to exchange layer 2 NLRI for each L2VPN instance configured on the router.

You must issue the **address-family vpws** command separately for each L2VPN instance configured on the router.

```
host1(config-router)#address-family vpws l2vpnA
host1(config-router)#address-family vpws l2vpnB
```

Related Topics

- *Chapter 1, Configuring BGP Routing*
- *Chapter 3, Configuring BGP-MPLS Applications*
- **address-family l2vpn** command
- **address-family vpws** command
- **exit-address-family** command
- **neighbor activate** command
- **neighbor next-hop-self** command
- **neighbor remote-as** command
- **neighbor update-source** command
- **router bgp** command

Configuring MPLS LSPs

As part of an L2VPN configuration, you must create MPLS label-switched paths (LSPs) to connect the local PE router and the remote PE router.

This section explains one way to create a basic MPLS configuration using the **mpls** and **mpls ldp** commands.

To configure MPLS LSPs on the PE router:

1. Enable MPLS on the virtual router.

```
host1(config)#mpls
```

2. Configure the core-facing interface on which you want to enable MPLS, Label Distribution Protocol (LDP), and topology-driven LSPs.

```
host1(config)#interface atm 5/0.100
host1(config-subif)#atm pvc 100 1 100 aal5snap 0 0 0
host1(config-subif)#ip address 192.168.5.5 255.255.255.0
```

3. Enable MPLS on the core-facing interface.

```
host1(config-subif)#mpls
```

4. Enable LDP and topology-driven LSPs on the core-facing interface.

```
host1(config-subif)#mpls ldp
host1(config-subif)#exit
```

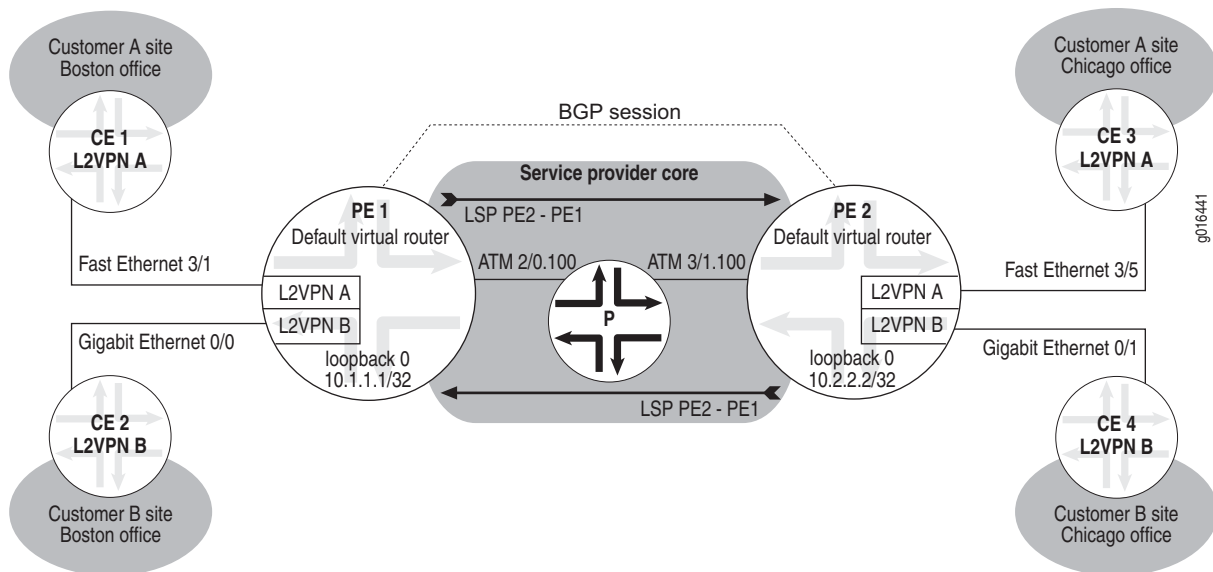
Related Topics

- *Chapter 2, Configuring MPLS*
- **atm pvc** command
- **interface atm** command
- **ip address** command
- **mpls** command
- **mpls ldp** command

L2VPN Configuration Example

The example in this section shows how to configure the L2VPN topology illustrated in Figure 126. The example includes procedures for configuring L2VPN on both the local E-series router (PE 1) and the remote E-series router (PE 2).

Figure 126: Topology for L2VPN Configuration Example



Topology Overview

The sample topology in Figure 126 includes two L2VPNs, L2VPN A and L2VPN B. L2VPN A connects CE 1, at the edge of Customer A's Boston site, with CE 3, at the edge of Customer A's Chicago site. Similarly, L2VPN B connects CE 2, at the edge of Customer B's Boston site, with CE 4, at the edge of Customer B's Chicago site.

The E-series routers in the topology, PE 1 and PE 2, each participate in both L2VPN A and L2VPN B. The example configures a total of four separate L2VPN instances, one for each L2VPN on each PE router. The instances for L2VPN A are named l2vpnA, and the instances for L2VPN B are named l2vpnB.

For each L2VPN instance, an Ethernet network interface provides a connection to the associated CE device.

Each PE router in the sample topology also has an ATM core-facing interface that connects it to the provider (P) router in the service provider core. You must configure MPLS LSPs on the core-facing interfaces to connect PE 1 and PE 2 through the P router across the service provider core. Finally, you must configure BGP on both PE 1 and PE 2 to provide signaling for both L2VPNs.

Configuration on PE 1 (Local PE Router)

Use the following commands on the local PE router (PE 1) to configure the L2VPN topology shown in Figure 126 on page 607.

```

! Configure L2VPN instance l2vpnA.
host1(config)#l2vpn l2vpnA encapsulation-type ethernet
host1(config)#l2vpn l2vpnA site-range 10
host1(config)#l2vpn l2vpnA site-name boston site-id 1
host1(config)#l2vpn l2vpnA rd 100:11
host1(config)#l2vpn l2vpnA route-target both 100:1
host1(config)#l2vpn l2vpnA control-word
host1(config)#l2vpn l2vpnA sequencing
!
! Configure L2VPN instance l2vpnB.
host1(config)#l2vpn l2vpnB encapsulation-type atm
host1(config)#l2vpn l2vpnB site-range 20
host1(config)#l2vpn l2vpnB site-name boston site-id 2
host1(config)#l2vpn l2vpnB rd 100:12
host1(config)#l2vpn l2vpnB route-target both 100:2
host1(config)#l2vpn l2vpnB control-word
host1(config)#l2vpn l2vpnB sequencing
!
! Configure the customer-facing interface between PE 1 and CE 1
! in L2VPN instance l2vpnA.
host1(config)#interface fastEthernet 4/0
host1(config-if)#l2vpn l2vpnA local-site-id 1 remote-site-id 3
host1(config-if)#exit
!
! Configure the customer-facing interface between PE 1 and CE 2
! in L2VPN instance l2vpnB.
host1(config)#interface gigabitEthernet 1/1
host1(config-subif)#l2vpn l2vpnB local-site-id 2 remote-site-id 4
host1(config-if)#exit
!
! Configure a loopback interface on PE 1 and assign it an IP address.
host1(config)#interface loopback 0
host1(config-if)#ip address 10.1.1.1 255.255.255.255
host1(config-if)#exit
!
! Assign the router ID for PE 1 using the IP address of the loopback interface.
host1(config)#ip router-id 10.3.3.3
!
! Configure BGP signaling.
host1(config)#router bgp 738
host1(config-router)#neighbor 10.1.1.1 remote-as 738
host1(config-router)#neighbor 10.1.1.1 update-source loopback 0
host1(config-router)#neighbor 10.1.1.1 next-hop-self
host1(config-router)#address-family l2vpn signaling
host1(config-router-af)#neighbor 10.1.1.1 activate
host1(config-router-af)#neighbor 10.1.1.1 next-hop-self
host1(config-router-af)#exit-address-family
host1(config-router)#address-family vpws l2vpnA
host1(config-router-af)#exit-address-family
host1(config-router)#address-family vpws l2vpnB
host1(config-router-af)#exit-address-family

```

```

!
! Enable MPLS on the default virtual router.
host1(config)#mpls
! Configure ATM core-facing interface 2/0.100 between PE 1 and the P router,
host1(config)#interface atm 2/0.100
host1(config-subif)#atm pvc 100 1 100 aal5snap 0 0 0
! and assign it an IP address.
host1(config-subif)#ip address 192.168.5.5 255.255.255.0
!
! Enable MPLS, LDP, and topology-driven LSPs on the core-facing interface.
host1(config-subif)#mpls
host1(config-subif)#mpls ldp
host1(config-subif)#exit

```

Configuration on PE 2 (Remote PE Router)

Use the following commands on the remote PE router (PE 2) to configure the L2VPN topology shown in Figure 126 on page 607.

```

! Configure L2VPN instance I2vpnA. The route target (100:1)
! matches the route target configured for I2vpnA on PE 1.
host2(config)#I2vpn I2vpnA encapsulation-type ethernet
host2(config)#I2vpn I2vpnA site-range 10
host2(config)#I2vpn I2vpnA site-name chicago site-id 3
host2(config)#I2vpn I2vpnA rd 100:11
host2(config)#I2vpn I2vpnA route-target both 100:1
host2(config)#I2vpn I2vpnA control-word
host2(config)#I2vpn I2vpnA sequencing
!
! Configure L2VPN instance I2vpnB. The route target (100:2)
! matches the route target configured for I2vpnB on PE 1.
host2(config)#I2vpn I2vpnB encapsulation-type ethernet
host2(config)#I2vpn I2vpnB site-range 20
host2(config)#I2vpn I2vpnB site-name chicago site-id 4
host2(config)#I2vpn I2vpnB rd 100:12
host2(config)#I2vpn I2vpnB route-target both 100:2
host2(config)#I2vpn I2vpnB control-word
host2(config)#I2vpn I2vpnB sequencing
!
! Configure the customer-facing interface between PE 2 and CE 3
! in L2VPN instance I2vpnA.
host2(config)#interface fastEthernet 3/5
host2(config-if)#I2vpn I2vpnA local-site-id 3 remote-site-id 1
host2(config-if)#exit
!
! Configure the customer-facing interface between PE 2 and CE 4
! in L2VPN instance I2vpnB.
host2(config)#interface gigabitEthernet 0/1
host2(config-subif)#I2vpn I2vpnB local-site-id 4 remote-site-id 2
host2(config-if)#exit
!
! Configure a loopback interface on PE 2 and assign it an IP address.
host2(config)#interface loopback 0
host2(config-if)#ip address 10.2.2.2 255.255.255.255
host2(config-if)#exit
!

```

```

! Assign the router ID for PE 2 using the IP address of the loopback interface.
host2(config)#ip router-id 10.2.2.2
!
! Configure BGP signaling.
host2(config)#router bgp 738
host2(config-router)#neighbor 10.2.2.2 remote-as 738
host2(config-router)#neighbor 10.2.2.2 update-source loopback 0
host2(config-router)#neighbor 10.2.2.2 next-hop-self
host2(config-router)#address-family l2vpn signaling
host2(config-router-af)#neighbor 10.2.2.2 activate
host2(config-router-af)#neighbor 10.2.2.2 next-hop-self
host2(config-router)#address-family vpws l2vpnA
host2(config-router-af)#exit-address-family
host2(config-router)#address-family vpws l2vpnB
host2(config-router-af)#exit-address-family
!
! Enable MPLS on the default virtual router.
host2(config)#mpls
!
! Configure ATM core-facing interface 3/1.100 between PE 2 and the P router,
! and assign it an IP address.
host2(config)#interface atm 3/1.100 point-to-point
host2(config-subif)#atm pvc 100 1 100 aal5snap 0 0 0
host2(config-subif)#ip address 192.168.4.4 255.255.255.0
!
! Enable MPLS, LDP, and topology-driven LSPs on the on the core-facing interface.
host2(config-subif)#mpls
host2(config-subif)#mpls ldp
host2(config-subif)#exit
!
! Enable MPLS, LDP, and topology-driven LSPs on the core-facing interface.
host1(config-subif)#mpls
host1(config-subif)#mpls ldp
host1(config-subif)#exit

```