



## CHAPTER 3

# Configuring Remote Access to MPLS VPN

---

The Cisco 10000 series router supports the IP virtual private network (VPN) feature for Multiprotocol Label Switching (MPLS). MPLS-based VPNs allow service providers to deploy a scalable and cost-effective VPN service that provides a stable and secure path through the network. An enterprise or Internet service provider (ISP) can connect to geographically dispersed sites through the service provider's network. Using the MPLS backbone, a set of sites are interconnected to create an MPLS VPN.

The remote access (RA) to MPLS VPN feature on the Cisco 10000 series router allows the service provider to offer a scalable end-to-end VPN service to remote users. The RA to MPLS VPN feature integrates the MPLS-enabled backbone with broadband access capabilities. By integrating access VPNs with MPLS VPNs, a service provider can:

- Enable remote users and offices to seamlessly access their corporate networks
- Offer equal access to a set of different ISPs or retail service providers
- Integrate their broadband access networks with the MPLS-enabled backbone
- Provide an end-to-end VPN service to enterprise customers with remote access users and offices
- Separate network access and connectivity functions from ISP functions

The RA to MPLS VPN feature is described in the following topics:

- [MPLS VPN Architecture, page 3-2](#)
- [Access Technologies, page 3-3](#)
- [Feature History for RA to MPLS VPN, page 3-10](#)
- [Restrictions for RA to MPLS VPN, page 3-10](#)
- [Prerequisites for RA to MPLS VPN, page 3-11](#)
- [Configuration Tasks for RA to MPLS VPN, page 3-12](#)
- [Verifying VPN Operation, page 3-30](#)
- [Configuration Examples for RA to MPLS VPN, page 3-30](#)
- [Monitoring and Maintaining an MPLS Configuration, page 3-39](#)
- [Monitoring and Maintaining the MPLS VPN, page 3-43](#)
- [Monitoring and Maintaining PPPoX to MPLS VPN, page 3-47](#)
- [Monitoring and Maintaining RBE to MPLS VPN, page 3-48](#)

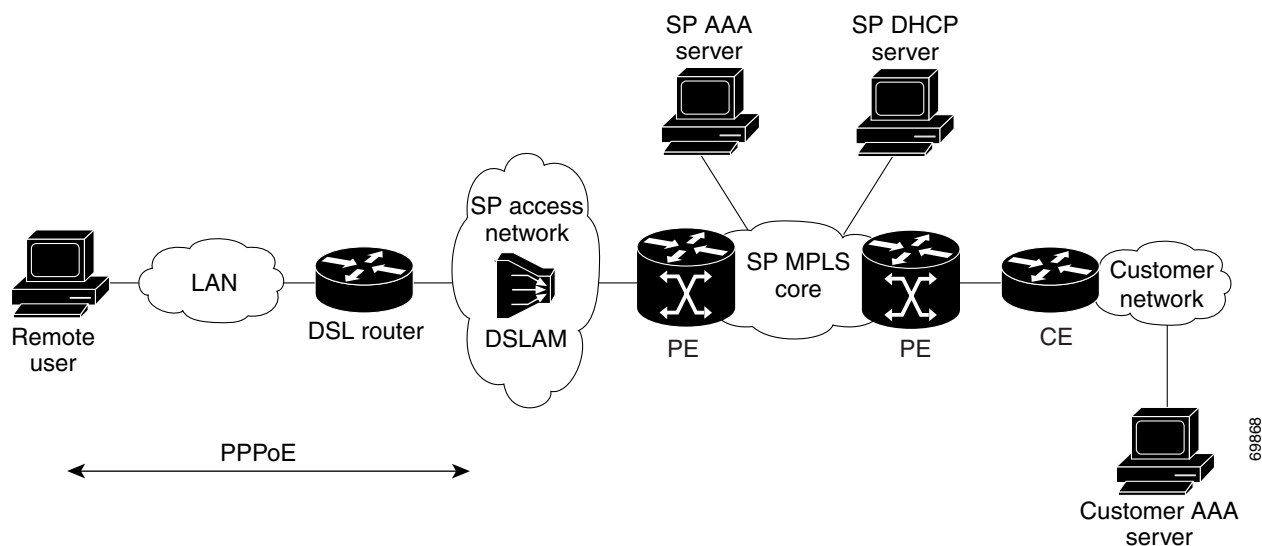
# MPLS VPN Architecture

The MPLS VPN architecture enables the service provider to build the MPLS VPN network one time and add VPNs for new customers as needed, including them in the already established network. The elements that comprise the MPLS VPN are:

- Customer edge (CE) routers—The CPE devices to which subscribers in a customer's network connect. The CE router connects to a service provider's edge router (PE router). The CE router initiates the remote access session to the PE router.
- Provider edge (PE) routers—The router, such as the Cisco 10000 series router, located at the edge of the service provider's MPLS core network. The PE router connects to one or more CE routers and has full knowledge of the routes to the VPNs associated with those CE routers. The PE router does not have knowledge of the routes to VPNs whose associated CE routers are not connected to it.
- Provider (P) routers—The service provider routers that comprise the provider's core network. The P routers do not assign VPN information and they do not have any knowledge of CE routers. Instead, the main focus of the P router is on label switching.

Figure 3-1 shows an example of the MPLS VPN architecture.

**Figure 3-1** MPLS VPN Network—Example



# Access Technologies

The Cisco 10000 series router supports routed bridge encapsulation (RBE) protocol. Point-to-point protocol (PPP) access-based permanent virtual circuits (PVCs) is supported by using the following PPP access encapsulation methods:

- PPP over ATM (PPPoA)
- PPP over Ethernet (PPPoE)

By using these PPP access technologies, the Cisco 10000 series router can terminate up to 32,000 sessions and support many features, including:

- Per session authentication based on Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP)
- Per session accounting
- Per session quality of service

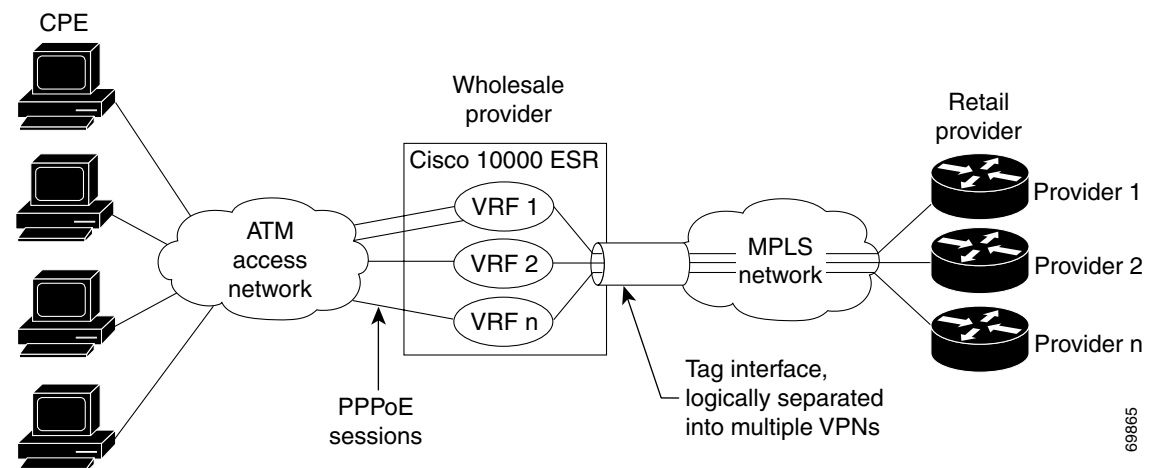


## Note

The Cisco 10000 series router can terminate up to 32,000 ATM RBE sessions.

Figure 3-2 shows the topology of an integrated PPPoX (PPPoE or PPPoA) access to a multiprotocol label switching virtual private network (MPLS VPN) solution.

**Figure 3-2** *PPPoX Access to MPLS VPN Topology*

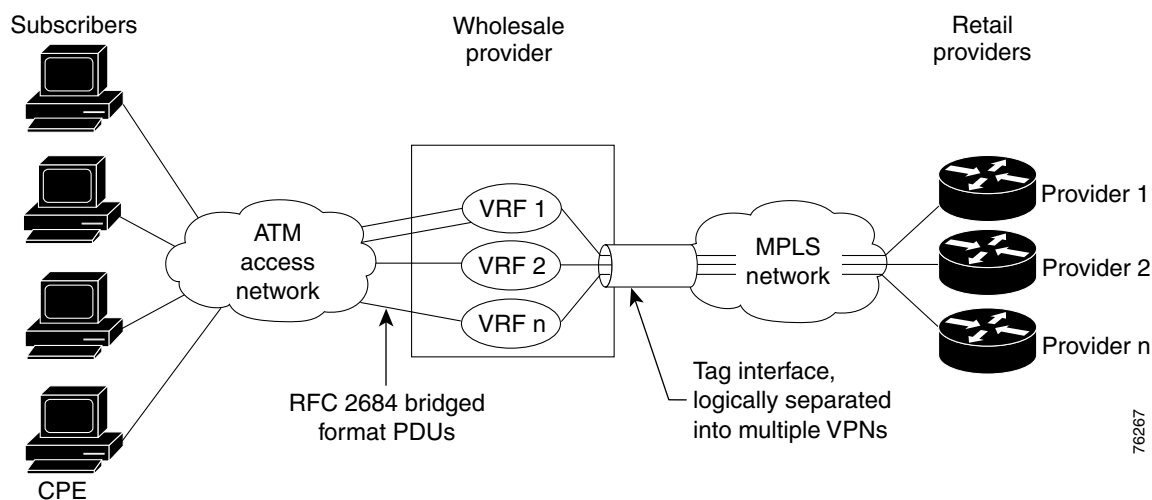


In the figure, the service provider operates an MPLS VPN that interconnects all customer sites. The service provider's core network is an MPLS backbone with VPN service capability. The service provider provides all remote access operations to its customer. The network side interfaces are tagged interfaces, logically separated into multiple VPNs.

69865

Figure 3-3 shows the topology of an RBE to MPLS VPN solution.

**Figure 3-3 RBE to MPLS VPN Topology**



In the figure, the wholesale provider uses VPNs to separate the subscribers of different retail providers. The subscribers are uniquely placed in VRFs on the access side. A tag interface separates traffic for the different retail providers on the network side. The MPLS VPN technology is used to assign tags in a VPN-aware manner.

## PPP over ATM to MPLS VPN

The Cisco 10000 series router supports a PPP over ATM (PPPoA) connection to an MPLS VPN architecture. In this model, when a remote user attempts to establish a connection with a corporate network, a PPPoA session is initiated and is terminated on the service provider's virtual home gateway (VHG) or provider edge (PE) router. All remote hosts connected to a particular CE router must be part of the same VPN to which the CE router is connected.

The following events occur when the remote user attempts to access the corporate network or ISP:

1. A PPPoA session is initiated over the broadband access network.
2. The VHG/PE router accepts and terminates the PPPoA session.
3. The VHG/PE router obtains virtual access interface (VAI) configuration information.
  - a. The VHG/PE obtains virtual template interface configuration information, which typically includes virtual routing and forwarding (VRF) mapping for sessions.
  - b. The VHG/PE sends a separate request to either the customer's or service provider's RADIUS server for the VPN to authenticate the remote user.
  - c. The VPN's VRF instance was previously instantiated on the VHG or PE. The VPN's VRF contains a routing table and other information associated with a specific VPN.

Typically, the customer RADIUS server is located within the customer VPN. To ensure that transactions between the VHG/PE router and the customer RADIUS server occur over routes within the customer VPN, the VHG/PE router is assigned at least one IP address that is valid within the VPN.

4. The VHG/PE router forwards accounting records to the service provider's proxy RADIUS server, which in turn logs the accounting records and forwards them to the appropriate customer RADIUS server.
5. The VHG/PE obtains an IP address for the CPE. The address is allocated from one of the following:
  - Local address pool
  - Service provider's RADIUS server, which either specifies the address pool or directly provides the address
  - Service provider's DHCP server
6. The CPE is now connected to the customer VPN. Packets can flow to and from the remote user.

Use virtual template interfaces to map sessions to VRFs. The Cisco 10000 series router can then scale to 32,000 sessions. In Cisco IOS Release 12.2(16)BX1 and later releases, when you map sessions to VRFs by using the RADIUS server, use the syntax **ip:vrf-id** or **ip:ip-unnumbered**. These vendor specific attributes (VSAs) enhance the scalability of per-user configurations because a new full virtual access interface is not required. For more information, see the [“Enhancing Scalability of Per-User Configurations”](#) section on page 2-17.

**Note**

In releases earlier than Cisco IOS Release 12.2(16)BX1, to map sessions to VRFs by using the RADIUS server, use the syntax **lcp:interface-config**. This configuration forces the Cisco 10000 series router to use full access virtual interfaces, which decreases scaling. We recommend that you do not use this configuration. Upgrading to Cisco IOS Release 12.2(16)BX1 or later eliminates this restriction.

## PPP over Ethernet to MPLS VPN

The Cisco 10000 series router supports a PPP over Ethernet (PPPoE) connection to an MPLS VPN architecture. In this model, when a remote user attempts to establish a connection with a corporate network, a PPPoE session is initiated and is terminated on the service provider's virtual home gateway (VHG) or provider edge (PE) router. All remote hosts connected to a particular CE router must be part of the VPN to which the CE router is connected.

The PPPoE to MPLS VPN architecture is a flexible architecture with the following characteristics:

- A remote host can create multiple concurrent PPPoE sessions, each to a different VPN.
- If multiple remote hosts exist behind the same CE router, each remote host can log in to a different VPN.
- Any remote host can log in to any VPN at any time because each VHG or PE router has the VRFs for all possible VPNs pre-instantiated on it. This configuration requires that the VRF be applied through the RADIUS server, which can cause scalability issues (see the following note).

Use virtual template interfaces to map sessions to VRFs. The Cisco 10000 series router can then scale to 32,000 sessions. In Cisco IOS Release 12.2(16)BX1 and later releases, when you map sessions to VRFs by using the RADIUS server, use the syntax **ip:vrf-id** or **ip:ip-unnumbered**. These vendor specific attributes (VSAs) enhance the scalability of per-user configurations because a new full virtual access interface is not required. For more information, see the [“Enhancing Scalability of Per-User Configurations”](#) section on page 2-17.

**Note**

For releases earlier than Cisco IOS Release 12.2(16)BX1, to map sessions to VRFs by using the RADIUS server, use the syntax **lcp:interface-config**. This configuration forces the Cisco 10000 series router to use full access virtual interfaces, which decreases scaling. We recommend that you do not use this configuration. Upgrading to Cisco IOS Release 12.2(16)BX1 or later releases will eliminate this restriction.

The following events occur as the VHG or PE router processes the incoming PPPoE session:

1. A PPPoE session is initiated over the broadband access network.
2. The VHG/PE router accepts and terminates the PPPoE session.
3. The VHG/PE router obtains virtual access interface (VAI) configuration information.
  - a. The VHG/PE obtains virtual template interface configuration information, which typically includes VRF mapping for sessions.
  - b. The VHG/PE sends a separate request to either the customer's or service provider's RADIUS server for the VPN to authenticate the remote user.
  - c. The VPN's VRF instance was previously instantiated on the VHG or PE. The VPN's VRF contains a routing table and other information associated with a specific VPN.

Use virtual template interfaces to map sessions to VRFs. The Cisco 10000 series router can then scale to 32,000 sessions. In Cisco IOS Release 12.2(16)BX1 and later releases, when you map sessions to VRFs by using the RADIUS server, use the syntax **ip:vrf-id** or **ip:ip-unnumbered**. These vendor specific attributes (VSAs) enhance the scalability of per-user configurations because a new full virtual access interface is not required. For more information, see the [“Enhancing Scalability of Per-User Configurations”](#) section on page 2-17.

**Note**

For releases earlier than Cisco IOS Release 12.2(16)BX1, to map sessions to VRFs by using the RADIUS server, use the syntax **lcp:interface-config**. This configuration forces the Cisco 10000 series router to use full access virtual interfaces, which decreases scaling. We recommend that you do not use this configuration. Upgrading to Cisco IOS Release 12.2(16)BX1 or later releases will eliminate this restriction.

Typically, the customer RADIUS server is located within the customer VPN. To ensure that transactions between the VHG/PE router and the customer RADIUS server occur over routes within the customer VPN, the VHG/PE router is assigned at least one IP address that is valid within the VPN.

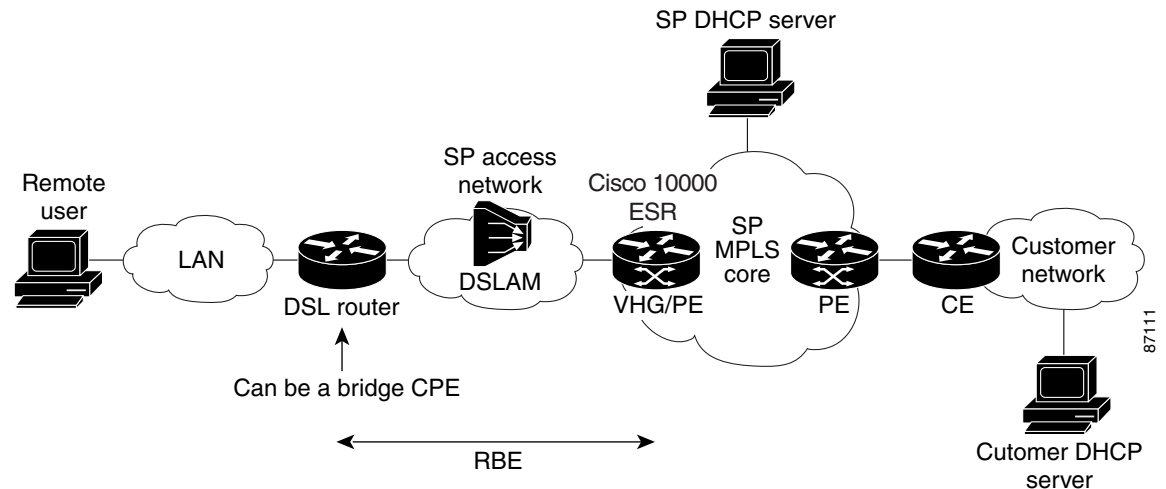
4. The VHG/PE router forwards accounting records to the service provider's proxy RADIUS server, which in turn logs the accounting records and forwards them to the appropriate customer RADIUS server.
5. The VHG/PE obtains an IP address for the CPE. The address is allocated from one of the following:
  - Local address pool
  - Service provider's RADIUS server, which either specifies the address pool or directly provides the address
  - Service provider's DHCP server
6. The CPE is now connected to the customer VPN. Packets can flow to and from the remote user.

## RBE over ATM to MPLS VPN

The Cisco 10000 series router supports an ATM RBE to MPLS VPN connection. RBE is used to route IP over bridged RFC 1483 Ethernet traffic from a stub-bridged LAN. The ATM connection appears like a routed connection; however, the packets received on the interface are bridged IP packets. RBE looks at the IP header of the packets arriving at an ATM interface and routes the packets instead of bridging them.

In Figure 3-4, RBE is configured between the DSL router and the Cisco 10000 series router, acting as the VHG/PE router.

**Figure 3-4 DSL RBE to MPLS VPN Integration**



The DSL router can be set up as a pure bridge or it can be set up for integrated routing and bridging (IRB) where multiple LAN interfaces are bridged through the bridge group virtual interface (BVI). Each of the DSL routers terminates on a separate point-to-point subinterface on the VHG/PE, which is statically configured with a specific VRF. Remote user authentication or authorization is available with Option 82 for DSL RBE remote access. RBE treats the VHG/PE subinterface as if it is connected to an Ethernet LAN, but avoids the disadvantages of pure bridging, such as broadcast storms, IP hijacking, and ARP spoofing issues. Address management options include static and VRF-aware DHCP servers.



### Note

For more information, see the “DSL Access to MPLS VPN Integration” chapter in the *Cisco Remote Access to MPLS VPN Solution Overview and Provisioning Guide, Release 2.0*, located at the following URL.

[http://www.cisco.com/univercd/cc/td/doc/product/vpn/solution/ramp2/ovprov/ra\\_op\\_05.htm](http://www.cisco.com/univercd/cc/td/doc/product/vpn/solution/ramp2/ovprov/ra_op_05.htm)

## MPLS VPN ID

The MPLS VPN ID is a 14-digit hexadecimal number that uniquely identifies a VPN and its associated VRF across all VHGs and PE routers in the network. In a router with multiple VPNs configured, you can use a VPN ID to identify a particular VPN. The VPN ID follows a standard specification (RFC 2685). The configuration of a VPN ID is optional.

You can configure a VRF instance for each VPN configured on the Cisco 10000 series router. By using the **vpn id** VRF configuration command, you can assign a VPN ID to a VPN. The router stores the VPN ID in the corresponding VRF structure for the VPN (see the “[Configuring Virtual Routing and Forwarding Instances](#)” section on page 3-13).

**Note**

---

The VPN ID is used for provisioning only. BGP routing updates do not include the VPN ID.

---

DHCP servers use the VPN ID to identify a VPN and allocate resources as the following describes:

1. A VPN DHCP client requests a connection to the Cisco 10000 series router (PE router) from a VRF interface.
2. The PE router determines the VPN ID associated with that interface.
3. The PE router sends a request with the VPN ID and other information for assigning an IP address to the DHCP server.
4. The DHCP server uses the VPN ID and IP address information to process the request.
5. The DHCP server sends a response back to the PE router, allowing the VPN DHCP client access to the VPN.

The RADIUS server uses the VPN ID to assign dialin users to the proper VPN. Typically, a user login consists of the following packets:

- Access-Request packet—A query from the network access server (NAS) that contains the user name, encrypted password, NAS IP address, VPN ID, and port. The format of the request also provides information on the type of session that the user wants to initiate.
- Access-Accept or Access-Reject packet—A response from the RADIUS server. The server returns an Access-Accept response if it finds the user name and verifies the password. The response includes a list of attribute-value (AV) pairs that describe the parameters to be used for this session. If the user is not authenticated, the RADIUS server returns an Access-Reject packet, and access is denied.

**Note**

---

For more information, see the *MPLS VPN ID, Release 12.2(4)B* feature module, located at the following URL.

[http://www.cisco.com/en/US/docs/ios/12\\_2/12\\_2b/12\\_2b4/feature/guide/12b\\_vpn.html](http://www.cisco.com/en/US/docs/ios/12_2/12_2b/12_2b4/feature/guide/12b_vpn.html)

---

## DHCP Relay Agent Information Option—Option 82

The Cisco 10000 series router supports the Dynamic Host Configuration Protocol (DHCP) relay agent information option (Option 82) feature when ATM routed bridge encapsulation (RBE) is used to configure DSL access. This feature communicates information to the DHCP server by using a suboption of the DHCP relay agent information option called *agent remote ID*. The information sent in the agent remote ID includes an IP address identifying the relay agent, information about the ATM interface, and information about the PVC over which the DHCP request came in. The DHCP server can use this information to make IP address assignments and security policy decisions.

Acting as the DHCP relay agent, the Cisco 10000 series router can also include VPN ID information in the agent remote ID suboption when forwarding client-originated DHCP packets to a DHCP server that has knowledge of existing VPNs. The VPN-aware DHCP server receives the DHCP packets and uses the VPN ID information to determine from which VPN to allocate an address. The DHCP server responds to the DHCP relay agent and includes information that identifies the originating client.

**Note**

For more information, see the *DHCP Option 82 Support for Routed Bridge Encapsulation, Release 12.2(2)T* feature module.

## DHCP Relay Support for MPLS VPN Suboptions

The DHCP relay agent information option (Option 82) enables a Dynamic Host Configuration Protocol (DHCP) relay agent to include information about itself when forwarding client-originated DHCP packets to a DHCP server. In some environments, the relay agent has access to one or more MPLS VPNs. A DHCP server that wants to offer service to DHCP clients on those different VPNs needs to know the VPN where each client resides. The relay agent typically knows about the VPN association of the DHCP client and includes this information in the relay agent information option.

The DHCP relay support for MPLS VPN suboptions feature allows the Cisco 10000 series router, acting as the DHCP relay agent, to forward VPN-related information to the DHCP server by using the following three suboptions of the DHCP relay agent information option:

- VPN identifier
- Subnet selection
- Server identifier override

The DHCP relay agent uses the VPN identifier suboption to tell the DHCP server the VPN for each DHCP request that it passes on to the DHCP server, and also uses the suboption to properly forward any DHCP reply that the DHCP server sends back to the relay agent. The VPN identifier suboption contains the VPN ID configured on the incoming interface to which the client is connected. If you configure the VRF name but not the VPN ID, the VRF name is used as the VPN identifier suboption. If the interface is in global routing space, the router does not add the VPN suboptions.

The subnet selection suboption allows the separation of the subnet where the client resides from the IP address that is used to communicate with the relay agent. In some situations, the relay agent needs to specify the subnet on which a DHCP client resides that is different from the IP address the DHCP server can use to communicate with the relay agent. The DHCP relay agent includes the subnet selection suboption in the relay agent information option, which the relay agent passes on to the DHCP server.

The server identifier override suboption contains the incoming interface IP address, which is the IP address on the relay agent that is accessible from the client. By using this information, the DHCP client sends all renew and release packets to the relay agent. The relay agent adds all the VPN suboptions and then forwards the renew and release packets to the original DHCP server.

After adding these suboptions to the DHCP relay agent information option, the gateway address changes to the relay agent's outgoing interface on the DHCP server side. The DHCP server uses this gateway address to send reply packets back to the relay agent. The relay agent then removes the relay agent information options and forwards the packets to the DHCP client on the correct VPN.

**Note**

For more information, see the *DHCP Relay Support for MPLS VPN Suboptions, Release 12.2(4)B* feature module, located at the following URL.

[http://www.cisco.com/en/US/docs/ios/12\\_2/12\\_2b/12\\_2b4/feature/guide/12b\\_dhc.html](http://www.cisco.com/en/US/docs/ios/12_2/12_2b/12_2b4/feature/guide/12b_dhc.html)

## Feature History for RA to MPLS VPN

| Cisco IOS Release | Description                                                    | Required PRE |
|-------------------|----------------------------------------------------------------|--------------|
| 12.2(4)BZ1        | This feature was integrated into Cisco IOS Release 12.2(4)BZ1. | PRE1         |
| 12.3(7)XI1        | This feature was integrated into Cisco IOS Release 12.3(7)XI1. | PRE2         |
| 12.2(28)SB        | This feature was integrated into Cisco IOS Release 12.2(28)SB. | PRE2         |

## Restrictions for RA to MPLS VPN

The RA to MPLS VPN feature has the following restrictions:

- When BGP aggregates customer routes, the received packets that match the aggregate route require an additional feedback in the PXF forwarding engine, which reduces performance.
- RBE to MPLS VPN does not support MAC-layer access lists; only IP access lists are supported.
- Before configuring DHCP relay support for MPLS VPN suboptions, you must configure standard MPLS VPNs. For more information, see the “[Configuring Virtual Private Networks](#)” section on [page 3-28](#) and the “[Configuring the MPLS Core Network](#)” section on [page 3-12](#), or see the *Cisco IOS Switching Services Configuration Guide, Release 12.2*, located at the following URL [http://www.cisco.com/en/US/docs/ios/12\\_2/switch/configuration/guide/fswtch\\_c.html](http://www.cisco.com/en/US/docs/ios/12_2/switch/configuration/guide/fswtch_c.html).
- The VPN ID is not used to control the distribution of routing information or to associate IP addresses with VPN IDs in routing updates.

## Prerequisites for RA to MPLS VPN

The RA to MPLS VPN feature has the following requirements:

- Your network must be running the following Cisco IOS services before you configure VPN operation:
  - MPLS in the service provider backbone routers
  - Tag distribution protocol (TDP) or the label distribution protocol (LDP)
  - BGP in all routers providing a VPN service
  - Cisco Express Forwarding (CEF) switching in each MPLS-enabled router

**Note**

---

IP CEF is on by default on the Cisco 10000 series router and it cannot be turned off. If you attempt to enable IP CEF, an error appears.

---

- For PPPoX to MPLS VPN networks, the Cisco 10000 series router must be running Cisco IOS Release 12.2(4)BZ1 or later releases and the performance routing engine must be installed in the router's chassis.
- For ATM RBE to MPLS VPN networks, the Cisco 10000 series router must be running Cisco IOS Release 12.2(15)BX or later releases and the performance routing engine must be installed in the router's chassis.
- You must configure DHCP option 82 support on the DHCP relay agent by using the **ip dhcp relay information option** command before you can use the DHCP Option 82 support for the RBE feature.
- Configure all the PE routers that belong to the same VPN with the same VPN ID. Make sure that the VPN ID is unique to the service provider network.

# Configuration Tasks for RA to MPLS VPN

To configure the RA to MPLS VPN feature, perform the following configuration tasks:

- [Configuring the MPLS Core Network, page 3-12](#)
- [Configuring Access Protocols and Connections, page 3-16](#)
- [Configuring and Associating Virtual Private Networks, page 3-28](#)
- [Configuring RADIUS User Profiles for RADIUS-Based AAA, page 3-30](#)

## Configuring the MPLS Core Network

To configure an MPLS core network, perform the following tasks:

- [Enabling Label Switching of IP Packets on Interfaces, page 3-12](#)
- [Configuring Virtual Routing and Forwarding Instances, page 3-13](#)
- [Associating VRFs, page 3-13](#)
- [Configuring Multiprotocol BGP PE to PE Routing Sessions, page 3-14](#)

### Enabling Label Switching of IP Packets on Interfaces

Enable label switching of IP packets on each PE router interface on the MPLS side of the network. The Cisco 10000 series router MPLS network side interface is a tagged interface. The packets passing through the interface are tagged packets.

  
**Note**

Multiple interfaces require a Label Switch Router (LSR).

To enable label switching of IP packets on interfaces, enter the following command in interface configuration mode:

| Command                           | Purpose                                                 |
|-----------------------------------|---------------------------------------------------------|
| Router(config-if)# <b>mpls ip</b> | Enables label switching of IP packets on the interface. |

  
**Note**

The Cisco 10000 series router supports the PPP Terminated Aggregation (PTA) to VRF feature, which terminates incoming PPP sessions and places them into the appropriate VRF for transport to the customer network. Unlike the RA to MPLS VPN model, the network side interface is not a tagged interface and there are no tagged packets. In the PTA to VRF model, the network side interface is an IP interface with IP packets. In this case, the traffic for the different VRFs is typically separated at Layer 2.

## Configuring Virtual Routing and Forwarding Instances

Configure VRF instances on each PE router in the provider network. Create one VRF for each VPN connected using the **ip vrf** command in global configuration mode or router configuration mode.

To create the VRF, do the following:

- Specify the correct route distinguisher (RD) used for that VPN using the **rd** command in VRF configuration submode. The RD is used to extend the IP address so that you can identify the VPN to which it belongs.
- Set up the import and export policies for the MP-BGP extended communities using the **route-target** command in VRF configuration submode. These policies are used for filtering the import and export process.

To configure a VRF, enter the following commands on the PE router beginning in global configuration mode:

|               | Command                                                                                                                   | Purpose                                                                                                                                                                                                                                        |
|---------------|---------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>ip vrf</b> <i>vrf-name</i>                                                                             | Enters VRF configuration mode and defines the virtual routing instance by assigning a VRF name.                                                                                                                                                |
| <b>Step 2</b> | Router(config-vrf)# <b>rd</b> <i>route-distinguisher</i>                                                                  | Creates routing and forwarding tables.                                                                                                                                                                                                         |
| <b>Step 3</b> | Router(config-vrf)# <b>route-target</b> { <b>import</b>   <b>export</b>   <b>both</b> } <i>route-target-ext-community</i> | Creates a list of import and export route target communities for the specified VRF.                                                                                                                                                            |
| <b>Step 4</b> | Router(config-vrf)# <b>vpn id</b> <i>oui:vpn-index</i>                                                                    | Assigns or updates a VPN ID on the VRF. The VPN ID uniquely identifies a VPN and VRF across all VHG and PE routers in the network.<br><br><b>Note</b> The VPN ID is used for provisioning only. BGP routing updates do not include the VPN ID. |

## Associating VRFs

After you define and configure the VRFs on the PE routers, associate each VRF with:

- An interface or subinterface
- A virtual template interface

The virtual template interface is used to create and configure a virtual access interface (VAI). For information about configuring a virtual template interface, see the [“Configuring a Virtual Template Interface” section on page 3-17](#).

To associate a VRF, enter the following commands on the PE router beginning in interface configuration mode:

|               | Command                                                            | Purpose                                               |
|---------------|--------------------------------------------------------------------|-------------------------------------------------------|
| <b>Step 1</b> | Router(config-if)# <b>ip vrf forwarding</b> <i>vrf-name</i>        | Associates a VRF with an interface or subinterface.   |
| <b>Step 2</b> | Router(config-if)# <b>ip address</b> <i>ip-address</i> <i>mask</i> | Sets a primary or secondary address for an interface. |
| <b>Step 3</b> | Router(config-if)# <b>exit</b>                                     | Returns to global configuration mode.                 |

|               | Command                                                         | Purpose                                                                       |
|---------------|-----------------------------------------------------------------|-------------------------------------------------------------------------------|
| <b>Step 4</b> | Router(config)# <b>interface virtual-template</b> <i>number</i> | Creates a virtual template interface and enters interface configuration mode. |
| <b>Step 5</b> | Router(config-if)# <b>ip vrf forwarding</b> <i>vrf-name</i>     | Associates a VRF with a virtual template interface.                           |

**Note**

Apply the **ip vrf forwarding** command and then the **ip address** command. If you do not, the **ip vrf forwarding** command removes the existing IP address on the interface.

**Example 3-1 Associating a VRF with an Interface**

```
interface GigabitEthernet7/0/0.1
 encapsulation dot1Q 11
 ip vrf forwarding vpn1
 ip address 192.168.1.1 255.255.255.0
!
```

**Example 3-2 Associating a VRF with a Virtual Template Interface**

```
interface Virtual-Template1
 ip vrf forwarding vpn1
 ip unnumbered Loopback1
 no peer default ip address
 ppp authentication chap vpn1
 ppp authorization vpn1
 ppp accounting vpn1
```

## Configuring Multiprotocol BGP PE to PE Routing Sessions

To configure multiprotocol BGP (MP-BGP) routing sessions between the PE routers, enter the following commands on the PE routers beginning in global configuration mode:

|               | Command                                                                                                                          | Purpose                                                                                                                                                                      |
|---------------|----------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>router bgp</b> <i>autonomous-system</i>                                                                       | Configures the internal BGP (iBGP) routing process with the autonomous system number passed along to other iBGP routers.                                                     |
| <b>Step 2</b> | Router(config-router)# <b>no bgp default ipv4-unicast</b>                                                                        | Disables IPv4 BGP routing.                                                                                                                                                   |
| <b>Step 3</b> | Router(config-router)# <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i>          | Configures the neighboring PE router's IP address or iBGP peer group and identifies it to the local autonomous system. The MP-BGP neighbors must use the loopback addresses. |
| <b>Step 4</b> | Router(config-router)# <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>update-source</b> <i>interface-type</i> | Allows iBGP sessions to use any operational interface for TCP connections.                                                                                                   |
| <b>Step 5</b> | Router(config-router)# <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>activate</b>                            | Activates route exchanges with the global BGP neighbors.                                                                                                                     |

|                | Command                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|----------------|--------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 6</b>  | Router(config-router)# <b>address-family ipv4 vrf</b> <i>vrf-name</i>                                                          | Enters address family configuration mode and configures the VRF routing table for BGP routing sessions that use standard IPv4 address prefixes.<br><br>The <i>vrf-name</i> argument specifies the name of the virtual routing and forwarding (VRF) instance to associate with subsequent IPv4 address family configuration mode commands.                                                                                                                                                            |
| <b>Step 7</b>  | Router(config-router-af)# <b>redistribute</b> <i>protocol</i>                                                                  | Redistributes routes from one routing domain into another routing domain.<br><br>The <i>protocol</i> argument is the source protocol from which routes are being redistributed. It can be one of the following keywords: <b>bgp</b> , <b>connected</b> , <b>egp</b> , <b>igrp</b> , <b>isis</b> , <b>ospf</b> , <b>static</b> [ <b>ip</b> ], or <b>rip</b> .<br><br>The <b>connected</b> keyword refers to routes that are established automatically by virtue of having enabled IP on an interface. |
| <b>Step 8</b>  | Router(config-router-af)# <b>exit-address-family</b>                                                                           | Exits address family configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Step 9</b>  | Router(config-router)# <b>address-family vpnv4</b> [ <b>unicast</b> ]                                                          | Enters address family configuration mode for configuring BGP routing sessions that use standard Virtual Private Network (VPN) Version 4 address prefixes.<br><br>(Optional) The <b>unicast</b> keyword specifies VPN Version 4 unicast address prefixes.                                                                                                                                                                                                                                             |
| <b>Step 10</b> | Router(config-router-af)# <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>activate</b>                       | Activates route exchanges with the global BGP neighbors.                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Step 11</b> | Router(config-router-af)# <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>send-community</b> [ <b>both</b> ] | Specifies that a communities attribute should be sent to a BGP neighbor.<br><br>The <b>both</b> keyword specifies that both communities attributes should be sent.                                                                                                                                                                                                                                                                                                                                   |

**Example 3-3 Configuring MP-BGP**

```

router bgp 100
  no synchronization
  no bgp default ipv4-unicast
  bgp log-neighbor-changes
  neighbor 10.1.1.4 remote-as 100
  neighbor 10.1.1.4 update-source Loopback0
  neighbor 10.1.1.4 activate
  neighbor 10.3.1.4 remote-as 100
  neighbor 10.3.1.4 update-source Loopback0
  neighbor 10.3.1.4 activate
  no auto-summary
!
address-family ipv4 vrf vrf-1
  redistribute connected
  no auto-summary
  no synchronization
  exit-address-family
!

```

```
address-family vpnv4
  neighbor 10.1.1.4 activate
  neighbor 10.1.1.4 send-community both
  neighbor 10.3.1.4 activate
  neighbor 10.3.1.4 send-community both
exit-address-family
!
```

**Note**

Typically, you enable BGP only on the PE routers. It is not necessary to enable BGP on all provider (P) core routers. However, if your network topology includes a route reflector, you may then enable BGP on a core router, which might be a P or PE router.

## Configuring Access Protocols and Connections

The Cisco 10000 series router supports the following access protocols:

- PPP over ATM
- PPP over Ethernet
- RBE over ATM

When a remote user initiates a PPPoA or PPPoE session to the Cisco 10000 series router, a predefined configuration template is used to configure a virtual interface known as a virtual access interface (VAI). The VAI is created and configured dynamically by using a virtual template interface. When the user terminates the session, the VAI goes down and the resources are freed for other client uses.

**Note**

Virtual template interfaces and VAIs do not apply to RBE over ATM.

The virtual template interface is a logical entity that the Cisco 10000 series router applies dynamically as needed to a connection. It is a configuration for an interface, but it is not tied to the physical interface. The VAI uses the attributes of the virtual template to create the session, which results in a VAI that is uniquely configured for a specific user.

After you configure a virtual template, configure the virtual connection that will use the template and then apply the template to the connection. The order in which you create virtual templates and configure the virtual connections that use the templates is not important. However, both the virtual templates and connections must exist before a remote user initiates a session to the Cisco 10000 series router.

The following sections describe how to create a virtual template and apply it to a VAI. For more information, see the “Configuring Virtual Template Interfaces” chapter in the *Cisco IOS Dial Technologies Configuration Guide, Release 12.2*.

**Note**

If you are using a RADIUS server, the RADIUS configuration takes precedence over the virtual template interface configuration. For example, the RADIUS configuration might override a number of parameters with the remainder of the configuration coming from the virtual template interface.

To configure access protocols and connections, perform the following configuration tasks. The first task listed is required and you can perform any of the remaining tasks as needed:

- [Configuring a Virtual Template Interface, page 3-17](#)
- [Configuring PPP over ATM Virtual Connections and Applying Virtual Templates, page 3-18](#)
- [Configuring PPPoE over ATM Virtual Connections and Applying Virtual Templates, page 3-18](#)

- [Configuring PPPoE over Ethernet Virtual Connections and Applying Virtual Templates, page 3-20](#)
- [Configuring RBE over ATM Virtual Connections, page 3-22](#)

## Configuring a Virtual Template Interface

To create and configure a virtual template interface, enter the following commands beginning in global configuration mode:

|               | Command                                                         | Purpose                                                                                                                |
|---------------|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>interface virtual-template</b> <i>number</i> | Creates a virtual template interface and enters interface configuration mode.                                          |
| <b>Step 2</b> | Router(config)# <b>ip unnumbered ethernet</b> <i>number</i>     | Enables IP without assigning a specific IP address on the LAN.                                                         |
| <b>Step 3</b> | Router(config-if)# <b>ppp authentication chap</b>               | Enables PPP authentication on the virtual template interface.                                                          |
| <b>Step 4</b> | Router(config-if)# <b>ppp ipcp ip address required</b>          | Required for legacy dial up and DSL networks. Prevents a PPP session from being set up with 0.0.0.0 remote ip address. |

### Example 3-4 Configuring a Virtual Template Interface

```
interface virtual-template 1
ip unnumbered Loopback1
no peer default ip address
ppp authentication chap vpn1
ppp ipcp ip address required
ppp authorization vpn1
ppp accounting vpn1
```

## Monitoring and Maintaining a Virtual Access Interface

When a virtual template interface is applied dynamically to an incoming user session, a virtual access interface (VAI) is created. You cannot use the command line interface (CLI) to directly create or configure a VAI, but you can display and clear the VAI by using the following commands in privileged EXEC mode:

| Command                                                                              | Purpose                                                                                                                                                                                  |
|--------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router# <b>show interfaces virtual-access</b> <i>number</i> [ <b>configuration</b> ] | Displays the configuration of the active VAI that was created using a virtual template interface.<br><br>The <b>configuration</b> keyword restricts output to configuration information. |
| Router# <b>clear interface virtual-access</b> <i>number</i>                          | Tears down the live sessions and frees the memory for other client uses.                                                                                                                 |

### Example 3-5 Displaying the Active VAI Configuration

```
Router# show interfaces virtual-access 1.1 configuration
!
interface virtual-access1.1
ip vrf forwarding vrf-1
ip unnumbered Loopback1
no ip proxy-arp
```

```
peer default ip address pool vrf-1
ppp authentication chap
end
```



**Note**

Virtual-access 1.1 is a PPPoE subinterface.

**Example 3-6 Clearing Live Sessions**

```
Router# clear interface virtual-access 1.1
Router#
```

## Configuring PPP over ATM Virtual Connections and Applying Virtual Templates

To configure a range of PVC connections and apply a virtual template interface to them, perform the following configuration task:

- [Configuring Encapsulated PPP over ATM Permanent Virtual Circuits, page 3-18](#)



**Note**

For more information, see the “Configuring Broadband Access: PPP and Routed Bridge Encapsulation” chapter in the *Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2*.

### Configuring Encapsulated PPP over ATM Permanent Virtual Circuits

Configure ATM permanent virtual circuits (PVCs) for encapsulated PPP over ATM on either point-to-point or multipoint subinterfaces. Using point-to-multipoint PVCs significantly increases the maximum number of PPPoA sessions that you can run on the Cisco 10000 series router.

To configure a PVC range with encapsulated PPPoA, enter the following commands beginning in global configuration mode:

|               | Command                                                                                                           | Purpose                                                                                                                              |
|---------------|-------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>interface atm</b><br><i>slot/port.subinterface-number multipoint</i>                           | Specifies an ATM multipoint subinterface.                                                                                            |
| <b>Step 2</b> | Router(config-subif)# <b>range</b> [ <i>range-name</i> ] <b>pvc</b><br><i>start-vpi/start-vci end-vpi/end-vci</i> | Creates a range of PVCs.                                                                                                             |
| <b>Step 3</b> | Router(config-if-atm-range)# <b>encapsulation</b><br><i>aal5encap ppp virtual-template number</i>                 | Configures the ATM adaptation layer (AAL) and encapsulation type on an ATM PVC range and links it to the virtual template interface. |

## Configuring PPPoE over ATM Virtual Connections and Applying Virtual Templates

To configure PPPoE over ATM, perform the following configuration tasks:

- Configure a virtual template (see the “Configuring a Virtual Template Interface” section on [page 3-17](#)).
- [Configuring a VPDN Group for PPPoE over ATM, page 3-19](#)
- [Configuring PPPoE on ATM Permanent Virtual Circuits, page 3-19](#)
- [Configuring PPPoE on ATM PVCs Using a Different MAC Address, page 3-20](#)

**Note**

For more information, see the “Configuring Broadband Access: PPP and Routed Bridge Encapsulation” chapter in the *Cisco IOS Wide-Area Networking Configuration Guide, Release 12.2*.

### Configuring a VPDN Group for PPPoE over ATM

To configure the physical interface that will carry the PPPoE session and link it to the appropriate virtual template interface, enter the following commands beginning in global configuration mode:

|               | Command                                                                    | Purpose                                                                                    |
|---------------|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>vpdn enable</b>                                         | Enables virtual private dial network (VPDN) configuration on this router.                  |
| <b>Step 2</b> | Router(config)# <b>vpdn group</b> <i>name</i>                              | Associates a VPDN group with a customer or VPDN profile.                                   |
| <b>Step 3</b> | Router(config-vpdn)# <b>accept-dialin</b>                                  | Creates an accept dial-in VPDN group.                                                      |
| <b>Step 4</b> | Router(config-vpdn-acc-in)# <b>protocol pppoe</b>                          | Specifies the VPDN group to be used to establish PPPoE sessions.                           |
| <b>Step 5</b> | Router(config-vpdn-acc-in)# <b>virtual-template</b> <i>template-number</i> | Specifies the virtual template interface to use to clone virtual access interfaces (VAIs). |
| <b>Step 6</b> | Router(config-vpdn)# <b>pppoe limit per-vc</b> <i>number</i>               | Specifies the maximum number of PPPoE sessions to be established over a virtual circuit.   |

### Configuring PPPoE on ATM Permanent Virtual Circuits

To configure PPPoE on a range of ATM PVCs, enter the following commands beginning in global configuration mode:

|               | Command                                                                                                           | Purpose                                                                           |
|---------------|-------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>interface atm</b> <i>slot/0.subinterface-number</i> <b>multipoint</b>                          | Specifies an ATM multipoint subinterface.                                         |
| <b>Step 2</b> | Router(config-subif)# <b>range</b> [ <i>range-name</i> ]<br><b>pvc</b> <i>start-vpi/start-vci end-vpi/end-vci</i> | Creates a range of PVCs.                                                          |
| <b>Step 3</b> | Router(config-if-atm-range)# <b>encapsulation aal5snap</b>                                                        | Configures VC multiplexed encapsulation on a PVC range.                           |
| <b>Step 4</b> | Router(config-if)# <b>protocol pppoe</b>                                                                          | Specifies the VPDN group to be used to establish PPPoE sessions on the PVC range. |

## Configuring PPPoE on ATM PVCs Using a Different MAC Address

To change the way PPPoE selects a MAC address when PPPoE and RBE are configured on two separate PVCs on the same DSL line, enter the following commands beginning in global configuration mode:

|               | Command                                                                                     | Purpose                                                                                                                                                                                                                                                                                                                                                 |
|---------------|---------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>vpdn-group pppoe-term</b>                                                | Specifies the VPDN group to be used to establish PPPoE sessions on a PVC.                                                                                                                                                                                                                                                                               |
| <b>Step 2</b> | Router(config-vpdn)# <b>accept-dialin</b>                                                   | Configures the L2TP access concentrator (LAC) to accept PPPoE sessions from a client and creates an accept-dialin VPDN subgroup.                                                                                                                                                                                                                        |
| <b>Step 3</b> | Router(config-vpdn-acc-in)# <b>protocol pppoe</b>                                           | Configures a static map for an ATM PVC.                                                                                                                                                                                                                                                                                                                 |
| <b>Step 4</b> | Router(config-vpdn-acc-in)# <b>exit</b>                                                     | Exits accept-dialin configuration mode and returns to VPDN configuration mode.                                                                                                                                                                                                                                                                          |
| <b>Step 5</b> | Router(config-vpdn)# <b>pppoe mac-address</b><br>{ <b>autoselect</b>   <i>mac-address</i> } | Changes the way PPPoE selects a MAC address.<br><br>The autoselect option always chooses a “MAC plus 7” address and no other address. For example, it chooses the ATM interface MAC address, interface MAC address plus 1, plus 2, plus 3, plus 4, plus 5, or plus 6).<br><br>Use the <i>mac-address</i> option to enter an explicit MAC address value. |



### Note

Use the **pppoe mac-address** command in VPDN group configuration mode. The Cisco 10000 series router applies the command to all PPPoEoA sessions brought up after you issue the command. MAC address usage does not change until you explicitly configure it using the **pppoe mac-address** command. The router limits the change to PPPoE sessions on ATM interfaces only and does not apply it to other interfaces on which PPPoE operates (such as Ethernet, Ethernet VLAN and DOCSIS interfaces).

## Configuring PPPoE over Ethernet Virtual Connections and Applying Virtual Templates

To configure PPPoE over Ethernet, perform the following configuration tasks:

- [Configuring a Virtual Template Interface, page 3-17](#)
- [Configuring PPPoE over Ethernet in a BBA Group, page 3-21](#)

## Configuring PPPoE over Ethernet in a BBA Group



### Note

Cisco IOS Release 12.2(15)BX does not support RADIUS configuration of BBA groups. You must configure BBA groups manually.

To configure a broadband aggregation (BBA) group for PPPoE and to link it to the appropriate virtual template interface, enter the following commands beginning in global configuration mode:

|               | Command                                                                    | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|---------------|----------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>bba-group pppoe</b> { <i>name</i>   <b>global</b> }     | Configures a BBA group to be used to establish PPPoE sessions.<br><br><i>name</i> identifies the BBA group. You can have multiple BBA groups.<br><br><b>global</b> is the default BBA group used for ATM connections when a BBA group name is not specified.                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Step 2</b> | Router(config-bba)# <b>virtual-template</b> <i>template-number</i>         | Specifies the virtual template interface to use to clone virtual access interfaces (VAIs).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 3</b> | Router(config-bba)# <b>pppoe limit per-mac</b> <i>per-mac-limit</i>        | (Optional) Specifies the maximum number of sessions per MAC address for each PPPoE port that uses the group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| <b>Step 4</b> | Router(config-bba)# <b>pppoe limit max-sessions</b> <i>number</i>          | (Optional) Specifies the maximum number of PPPoE sessions that can be terminated on this router from all interfaces.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Step 5</b> | Router(config-bba)# <b>pppoe limit per-vc</b> <i>per-vc-limit</i>          | (Optional) Specifies the maximum number of PPPoE sessions for each VC that uses the group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 6</b> | Router(config-bba)# <b>exit</b>                                            | Returns to global configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| <b>Step 7</b> | Router(config)# <b>interface atm</b> <i>slot/subslot/port.subinterface</i> | Specifies the interface to which you want to attach the BBA group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Step 8</b> | Router(config-if)# <b>pvc</b> [ <i>name</i> ] <i>vpi/vci</i>               | Creates an ATM permanent virtual circuit (PVC) and enters ATM PVC configuration mode.<br><br>(Optional) <i>name</i> specifies the name of the PVC or map. The name can be up to 16 characters.<br><br><i>vpi/</i> specifies the ATM network VPI for the PVC that you named. Valid values are from 0 to 255. If a value is not specified, the vpi value is set to 0.<br><br><i>vci</i> specifies the ATM network VCI for the PVC you named. Valid values are from 0 to 1 less than the maximum value set for this interface using the <b>atm vc-per-vp</b> command.<br><br><b>Note</b> You cannot set both <i>vpi</i> and <i>vci</i> to 0; if one is 0, the other cannot be 0. |
| <b>Step 9</b> | Router(config-if)# <b>protocol pppoe group</b> <i>group-name</i>           | Attaches the BBA group to the PVC.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

**Note**

You cannot simultaneously configure a BBA group for PPPoE and a VPDN group for PPPoE. If you configure a BBA group and then you configure a VPDN group, the **protocol** command in VPDN accept-dialin configuration mode does not include an option for PPPoE (for example, you cannot specify the **protocol pppoe** command). Use the **no bba-group pppoe** command to re-enable the **pppoe** option for the **protocol** command.

## Configuring RBE over ATM Virtual Connections

To configure RBE over ATM virtual connections and apply virtual templates, perform the following configuration tasks:

- [Configuring the PE Router, page 3-22](#)
- [Configuring DHCP Option 82 for RBE, page 3-25](#)
- [Configuring DHCP Relay Support for MPLS VPN Suboptions, page 3-26](#)
- [Specifying a VPN ID, page 3-27](#)

### Configuring the PE Router

To configure the PE router, perform the following required configuration tasks:

- [Defining Loopbacks, page 3-22](#)
- [Defining PVCs, page 3-23](#)
- [Configuring Label Switching, page 3-23](#)
- [Configuring the VRF for Each VPN, page 3-23](#)
- [Configuring a Dedicated PVC, page 3-24](#)
- [Configuring BGP to Advertise Networks, page 3-24](#)

**Note**

For more information, see the “DSL Access to MPLS VPN Integration” chapter in the *Cisco Remote Access to MPLS VPN Solution Overview and Provisioning Guide, Release 2.0*.

### Defining Loopbacks

To define loopbacks, enter the following commands beginning in global configuration mode:

|               | Command                                                                    | Purpose                                                                                |
|---------------|----------------------------------------------------------------------------|----------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>interface loopback</b> <i>number</i>                    | Creates a loopback interface to reach the router. Enters interface configuration mode. |
| <b>Step 2</b> | Router(config-if)# <b>ip vrf forwarding</b> <i>vrf-name</i>                | Associates a VRF with the loopback interface.                                          |
| <b>Step 3</b> | Router(config-if)# <b>ip address</b> [ <i>address</i> ] [ <i>netmask</i> ] | Assigns an IP address to the loopback interface.                                       |

## Defining PVCs

To define PVCs, enter the following commands beginning in global configuration mode:

|               | Command                                                                                               | Purpose                                                                                                                                   |
|---------------|-------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>interface atm</b><br><i>slot/port.subinterface-number</i><br><b>point-to-point</b> | Specifies an ATM point-to-point subinterface. Enters subinterface configuration mode.                                                     |
| <b>Step 2</b> | Router(config-subif)# <b>ip vrf forwarding</b><br><i>vrf-name</i>                                     | Associates a VRF with the ATM point-to-point subinterface.                                                                                |
| <b>Step 3</b> | Router(config-subif)# <b>ip unnumbered</b><br><b>Loopback</b> <i>number</i>                           | Configures the ATM subinterface as unnumbered to a loopback interface.<br><br><b>Note</b> The loopback interface must be in the same VRF. |
| <b>Step 4</b> | Router(config-subif)# <b>pvc</b> [ <i>vpi/vci</i><br><i>number</i> ]                                  | Configures the PVC on the subinterface. Enters PVC configuration mode.                                                                    |
| <b>Step 5</b> | Router(config-subif-pvc)# <b>encapsulation</b><br><b>aal5snap</b>                                     | Configures the ATM adaptation layer (AAL) and encapsulation type on the ATM PVC.                                                          |
| <b>Step 6</b> | Router(config-subif-pvc)# <b>no protocol ip</b><br><b>inarp</b>                                       | Disables Inverse ARP on the ATM PVC.                                                                                                      |

## Configuring Label Switching

To configure label switching on the interface connected to the MPLS cloud, enter the following commands beginning in global configuration mode:

|               | Command                                                                                              | Purpose                                                                                   |
|---------------|------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>interface atm</b><br><i>slot/port.subinterface-number</i><br><b>tag-switching</b> | Connects to an MPLS cloud using MPLS ATM tagging. Enters subinterface configuration mode. |
| <b>Step 2</b> | Router(config-subif)# <b>ip address</b> <i>address</i>                                               | Assigns an IP address to the ATM subinterface.                                            |
| <b>Step 3</b> | Router(config-subif)# <b>tag-switching atm</b><br><b>vp-tunnel</b> <i>vpi</i>                        | Specifies an interface or subinterface as a virtual private (VP) tunnel.                  |
| <b>Step 4</b> | Router(config-subif)# <b>tag-switching ip</b>                                                        | Enables label switching of IP packets on the interface.                                   |

## Configuring the VRF for Each VPN

To configure the VRF for each VPN, enter the following commands beginning in global configuration mode:

|               | Command                                                                                                                         | Purpose                                                                                         |
|---------------|---------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>ip vrf</b> <i>vrf-name</i>                                                                                   | Enters VRF configuration mode and defines the virtual routing instance by assigning a VRF name. |
| <b>Step 2</b> | Router(config-vrf)# <b>rd</b><br><i>route-distinguisher</i>                                                                     | Creates routing and forwarding tables.                                                          |
| <b>Step 3</b> | Router(config-vrf)# <b>route-target</b> { <b>import</b><br>  <b>export</b>   <b>both</b> }<br><i>route-target-ext-community</i> | Creates a list of import and export route target communities for the specified VRF.             |

## Configuring a Dedicated PVC

To configure a dedicated PVC for each VPN, enter the following commands beginning in global configuration mode:

|               | Command                                                                                            | Purpose                                                                            |
|---------------|----------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>interface atm</b> <i>slot/port.subinterface-number</i><br><b>point-to-point</b> | Creates a point-to-point ATM subinterface. Enters subinterface configuration mode. |
| <b>Step 2</b> | Router(config-subif)# <b>ip vrf forwarding</b> <i>vrf-name</i>                                     | Associates a VRF with the ATM point-to-point subinterface.                         |
| <b>Step 3</b> | Router(config-subif)# <b>ip address</b> <i>address</i>                                             | Assigns an IP address to the ATM subinterface.                                     |
| <b>Step 4</b> | Router(config-subif)# <b>pvc</b> [ <i>vpi/vci</i> <i>number</i> ]                                  | Configures the PVC on the subinterface. Enters PVC configuration mode.             |
| <b>Step 5</b> | Router(config-subif-pvc)# <b>encapsulation</b> <b>aal5snap</b>                                     | Configures the ATM adaptation layer (AAL) and encapsulation type on the ATM PVC.   |

## Configuring BGP to Advertise Networks

To configure BGP to advertise the networks for each VPN, enter the following commands beginning in global configuration mode:

|               | Command                                                                                                                          | Purpose                                                                                                                                                                                                                                                                                                                                   |
|---------------|----------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>router bgp</b> <i>autonomous-system</i>                                                                       | Configures the internal BGP (iBGP) routing process with the autonomous system number passed along to other iBGP routers.                                                                                                                                                                                                                  |
| <b>Step 2</b> | Router(config-router)# <b>no bgp default</b> <b>ipv4-unicast</b>                                                                 | Disables IPv4 BGP routing.                                                                                                                                                                                                                                                                                                                |
| <b>Step 3</b> | Router(config-router)# <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>remote-as</b> <i>as-number</i>          | Configures the neighboring PE router's IP address or iBGP peer group and identifies it to the local autonomous system. The MP-BGP neighbors must use the loopback addresses.                                                                                                                                                              |
| <b>Step 4</b> | Router(config-router)# <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>update-source</b> <i>interface-type</i> | Allows iBGP sessions to use any operational interface for TCP connections.                                                                                                                                                                                                                                                                |
| <b>Step 5</b> | Router(config-router)# <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>activate</b>                            | Activates route exchanges with the global BGP neighbors.                                                                                                                                                                                                                                                                                  |
| <b>Step 6</b> | Router(config-router)# <b>address-family ipv4 vrf</b> <i>vrf-name</i>                                                            | Enters address family configuration mode and configures the VRF routing table for BGP routing sessions that use standard IPv4 address prefixes.<br><br>The <i>vrf-name</i> argument specifies the name of the virtual routing and forwarding (VRF) instance to associate with subsequent IPv4 address family configuration mode commands. |

|                | Command                                                                                                                        | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|----------------|--------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 7</b>  | Router(config-router-af)# <b>redistribute</b> <i>protocol</i>                                                                  | Redistributes routes from one routing domain into another routing domain.<br><br>The <i>protocol</i> argument is the source protocol from which routes are being redistributed. It can be one of the following keywords: <b>bgp</b> , <b>connected</b> , <b>egp</b> , <b>igrp</b> , <b>isis</b> , <b>ospf</b> , <b>static</b> [ip], or <b>rip</b> .<br><br>The <b>connected</b> keyword refers to routes that are established automatically by virtue of having enabled IP on an interface. |
| <b>Step 8</b>  | Router(config-router-af)# <b>exit-address-family</b>                                                                           | Exits address family configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 9</b>  | Router(config-router)# <b>address-family</b> <b>vpnv4</b> [ <b>unicast</b> ]                                                   | Enters address family configuration mode for configuring BGP routing sessions that use standard Virtual Private Network (VPN) Version 4 address prefixes.<br><br>(Optional) The <b>unicast</b> keyword specifies VPN Version 4 unicast address prefixes.                                                                                                                                                                                                                                    |
| <b>Step 10</b> | Router(config-router-af)# <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>activate</b>                       | Activates route exchanges with the global BGP neighbors.                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 11</b> | Router(config-router-af)# <b>neighbor</b> { <i>ip-address</i>   <i>peer-group-name</i> } <b>send-community</b> [ <b>both</b> ] | Specifies that a community attribute should be sent to a BGP neighbor.<br><br>The <b>both</b> keyword specifies that both community attributes should be sent.                                                                                                                                                                                                                                                                                                                              |
| <b>Step 12</b> | Router(config-router-af)# <b>exit-address-family</b>                                                                           | Exits address family configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Step 13</b> | Router(config-router)# <b>exit</b>                                                                                             | Exits router configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Step 14</b> | Router(config)# <b>interface</b> <b>atm</b> <i>slot/port.subinterface-number</i> <b>point-to-point</b>                         | Creates a point-to-point ATM subinterface. Enters subinterface configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Step 15</b> | Router(config-subif)# <b>atm route-bridged ip</b>                                                                              | Enables RBE on the subinterface.                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

### Configuring DHCP Option 82 for RBE

To configure DHCP Option 82 support for RBE connections, enter the following commands beginning in global configuration mode:

|               | Command                                                  | Purpose                                                                                                                                                           |
|---------------|----------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>ip dhcp relay information option</b>  | Enables the system to insert the DHCP relay agent information option in VPN suboptions.                                                                           |
| <b>Step 2</b> | Router(config)# <b>rbe nasip</b> <i>source_interface</i> | Specifies the IP address of an interface on the DHCP relay agent. This is the interface address that is sent to the DHCP server in the agent remote ID suboption. |

[Example 3-7](#) enables DHCP option 82 support on the DHCP relay agent by using the **ip dhcp relay information option** command. The **rbe nasip** command configures the router to forward the IP address for Loopback0 to the DHCP server. The value (in hexadecimal) of the agent remote ID suboption is 010100000B0101814058320 and the value of each field is the following:

- Port Type: 0x01
- Version: 0x01

- Reserved: undefined
- NAS IP address: 0x0B010181 (hexadecimal value of 11.1.1.129)
- NAS Port
  - Interface (slot/module/port): 0x40 (The slot/module/port values are 01 00/0/000.)
  - VPI: 0x58 (hexadecimal value of 88)
  - VCI: 0x320 (hexadecimal value of 800)

### Example 3-7 Configuring Option 82 for RBE

```

ip dhcp-server 172.16.1.2
!
ip dhcp relay information option
!
interface Loopback0
 ip address 11.1.1.129 255.255.255.192
!
interface ATM4/0
 no ip address
!
interface ATM4/0.1 point-to-point
 ip unnumbered Loopback0
 ip helper-address 172.16.1.2
 atm route-bridged ip
 pvc 88/800
 encapsulation aal5snap
!
interface Ethernet 5/1
 ip address 172.16.1.1 255.255.0.0
!
router eigrp 100
 network 10.0.0.0
 network 172.16.0.0
!
rbe nasip Loopback0

```

### Configuring DHCP Relay Support for MPLS VPN Suboptions

To configure DHCP relay support for MPLS VPN suboptions, enter the following commands beginning in global configuration mode:

|        | Command                                                     | Purpose                                                                                                                                                                                                                                                                                                                  |
|--------|-------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Step 1 | Router(config)# <b>ip dhcp relay information option vpn</b> | Enables the system to insert VPN suboptions into the DHCP relay agent information option in forwarded BOOTREQUEST messages to a DHCP server. Sets the gateway address to the outgoing interface toward the DHCP server. The VPN suboptions are also added to the BOOTP broadcast packets when the command is configured. |

|               | Command                                                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|---------------|------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 2</b> | Router(config)# <b>interface</b> <i>type number</i>                          | Specifies an interface and enters interface configuration mode.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>Step 3</b> | Router(config-if)# <b>ip helper-address</b> <i>vrf name [global] address</i> | <p>Forwards UDP broadcasts, including BOOTP, received on an interface.</p> <p>If the DHCP server resides in a VPN or global space that is different from the VPN, the <b>vrf name</b> or <b>global</b> options allow you to specify the name of the VRF or global space where the DHCP server resides.</p> <p>The <b>vrf name</b> argument is the virtual routing and forwarding (VRF) instance for the VPN.</p> <p>The <b>global</b> argument is the global routing table.</p> <p>The <i>address</i> argument is the destination broadcast or host address to be used when forwarding UDP broadcasts. You can configure more than one helper address per interface.</p> |

In [Example 3-8](#), the DHCP relay receives a DHCP request on Ethernet interface 0/1 and sends the request to the DHCP server located at IP helper address 10.44.23.7, which is associated with the VRF named *red*.

#### Example 3-8 Configuring DHCP Relay Support for MPLS VPN Suboptions

```
ip dhcp relay information option vpn
!
interface ethernet 0/1
 ip helper-address vrf red 10.44.23.7
!
```

### Specifying a VPN ID

To specify a VPN ID, enter the following commands beginning in global configuration mode:

|               | Command                                                | Purpose                                                                                                                                                                                                                                                                                                                                   |
|---------------|--------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>ip vrf</b> <i>vrf-name</i>          | <p>Creates a VRF routing table and a CEF forwarding table and enters VRF configuration mode.</p> <p>The <i>vrf-name</i> argument is the name you assign to the VRF.</p>                                                                                                                                                                   |
| <b>Step 2</b> | Router(config-vrf)# <b>vpn id</b> <i>oui:vpn-index</i> | <p>Assigns a VPN ID to the VRF.</p> <p>The <i>oui:</i> argument is an organizationally unique identifier. The IEEE organization assigns this identifier to companies. The OUI is restricted to three octets.</p> <p>The <i>vpn-index</i> argument identifies the VPN within the company. This VPN index is restricted to four octets.</p> |

[Example 3-9](#) assigns a VPN ID to the VRF named *vpn1*.

**Example 3-9 Configuring a VPN ID**

```
Router(config)# ip vrf vpn1
Router(config-vrf)# vpn id al:3f6c
Router(config-vrf)# end
```

## Configuring and Associating Virtual Private Networks

To add a virtual private network (VPN) service to your MPLS configuration, you perform the following tasks:

- Configure VPNs
- Associate VPNs with a virtual template interface

### Configuring Virtual Private Networks

To configure dial-in and dial-out virtual private networks (VPNs), perform the following tasks:

- Enable a VPN tunnel
- Configure VPN tunnel authentication

For more information about configuring virtual private networks, see the “Configuring Virtual Private Networks” chapter in the *Cisco IOS Dial Technologies Configuration Guide, Release 12.2*. This chapter describes the procedures used to configure, verify, monitor, and troubleshoot VPNs and also provides configuration examples.

### Associating VPNs with a Virtual Template Interface

After you configure the VPNs, associate each one with a virtual template interface. To do this association, perform the following tasks:

- [Creating a VRF Configuration for a VPN, page 3-28](#)
- [Associating a VRF Configuration for a VPN with a Virtual Template Interface, page 3-29](#)



**Note** Do not enable VPN service on the fa0/0/0 management interface. The configuration for this interface is included in the configuration file.

### Creating a VRF Configuration for a VPN

To create a VRF configuration for a VPN, enter the following commands beginning in global configuration mode:

|               | Command                                                  | Purpose                                                                                     |
|---------------|----------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>ip vrf</b> <i>vrf-name</i>            | Enters VRF configuration mode and defines the VPN routing instance by assigning a VRF name. |
| <b>Step 2</b> | Router(config-vrf)# <b>rd</b> <i>route-distinguisher</i> | Creates routing and forwarding tables.                                                      |

|               | Command                                                                                            | Purpose                                                                             |
|---------------|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------|
| <b>Step 3</b> | Router(config-vrf)# <b>vpn id</b><br><i>route-distinguisher</i>                                    | Associates the VPN with the VRF.                                                    |
| <b>Step 4</b> | Router(config-vrf)# <b>route-target {import   export   both}</b> <i>route-target-ext-community</i> | Creates a list of import and export route target communities for the specified VRF. |

#### Example 3-10 Creating a VRF Configuration for a VPN

```
ip vrf common
 rd 100:1000
 vpn id 100:1000
 route-target export 100:1000
 route-target import 100:1000
```



#### Note

For more information about creating VRFs, see the [“Configuring Virtual Routing and Forwarding Instances”](#) section on page 3-13.

### Associating a VRF Configuration for a VPN with a Virtual Template Interface

After you create a VRF configuration for a VPN, associate the VRF with a virtual template interface. The virtual template interface is used to create and configure a virtual access interface (VAI).

To associate a VRF, enter the following commands beginning in global configuration mode:

|               | Command                                                            | Purpose                                                                                                                                                                                                                                                                    |
|---------------|--------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Step 1</b> | Router(config)# <b>interface virtual-template</b><br><i>number</i> | Creates a virtual template interface and enters interface configuration mode.                                                                                                                                                                                              |
| <b>Step 2</b> | Router(config-if)# <b>ip vrf forwarding</b><br><i>vrf-name</i>     | Associates the VRF with the virtual template interface.                                                                                                                                                                                                                    |
| <b>Step 3</b> | Router(config-if)# <b>ip unnumbered</b> <i>type number</i>         | Enables IP without assigning a specific IP address to the interface.<br><br>The <i>type</i> and <i>number</i> arguments are the type and number of another interface on which the router has an assigned IP address. The interface cannot be another unnumbered interface. |

#### Example 3-11 Associating a VRF Configuration for a VPN with a Virtual Template Interface

```
interface Virtual-Template1
 ip vrf forwarding common
 ip unnumbered Loopback1
```



#### Note

- For more information about configuring a virtual template interface, see the [“Configuring a Virtual Template Interface”](#) section on page 3-17.
- For more information about creating and associating VRFs, see the [“Configuring Virtual Routing and Forwarding Instances”](#) section on page 3-13 and the [“Associating VRFs”](#) section on page 3-13.

## Configuring RADIUS User Profiles for RADIUS-Based AAA

Use the per VRF AAA feature to partition authentication, authorization, and accounting (AAA) services based on a virtual routing and forwarding (VRF) instance. This feature allows the Cisco 10000 router to communicate directly with the customer RADIUS server without having to go through a RADIUS proxy.

For more information about configuring the per VRF AAA feature on the Cisco 10000 series router, see the [“Optional Configuration Tasks for LAC” section on page 5-7](#).

For more information about configuring your RADIUS server, see your RADIUS documentation.

## Verifying VPN Operation

To verify VPN operation, enter any of the following commands in privileged EXEC mode:

| Command                                                                                                          | Purpose                                                                                    |
|------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------|
| Router# <b>show ip vrf</b>                                                                                       | Displays the defined VRFs and interfaces.                                                  |
| Router# <b>show ip vrf</b> [{ <b>brief</b>   <b>detail</b>   <b>interfaces</b> }] <i>vrf-name</i>                | Displays information about defined VRFs and associated interfaces.                         |
| Router# <b>show ip route vrf</b> <i>vrf-name</i>                                                                 | Displays the IP routing table for a VRF.                                                   |
| Router# <b>show ip protocols vrf</b> <i>vrf-name</i>                                                             | Displays the routing protocol information for a VRF.                                       |
| Router# <b>show ip interface</b> <i>interface-number</i>                                                         | Displays the VRF table associated with an interface.                                       |
| Router# <b>show ip bgp vpnv4 all</b> [ <b>tags</b> ]                                                             | Displays information about all BGPs.                                                       |
| Router# <b>show tag-switching forwarding vrf</b> <i>vrf-name</i> [ <i>prefix mask/length</i> ] [ <b>detail</b> ] | Displays label forwarding entries that correspond to VRF routes advertised by this router. |

## Configuration Examples for RA to MPLS VPN

This section provides configuration examples for the following configurations:

- [PPPoA to MPLS VPN Configuration Example, page 3-31](#)
- [PPPoE to MPLS VPN Configuration Example, page 3-34](#)
- [RBE to MPLS VPN Configuration Example, page 3-38](#)

## PPPoA to MPLS VPN Configuration Example

[Example 3-12](#) shows how to configure the RA to MPLS VPN feature on the Cisco 10000 series router. In this example, one VRF is configured with 300 PPPoA sessions.

### **Example 3-12 Configuring PPPoA to MPLS VPN**

```
!Enables the AAA access control model.
aaa new-model
!
!Configures AAA accounting.
aaa authentication login default none
aaa authentication ppp default local
aaa authorization network default local
aaa session-id common
enable password vermont
!
username vpn1 password 0 vpn1
!
!Configures the vpn1 VRF.
ip vrf vpn1
    rd 10:1
    route-target export 10:1
    route-target import 10:1
!
!Configures the policy map for the default class.
policy-map mypolicy
    class class-default
        police 200000 400000 800000 conform-action transmit exceed-action drop
!
no virtual-template snmp
!
!Sets the size of the small and middle buffers.
buffers small permanent 20000
buffers middle permanent 7000
!
!Defines the general loopback interface used for reachability to the router and as a
!source IP address for sessions (IBGP, TDP, and so on).
interface Loopback0
    ip address 10.1.1.1 255.255.255.255
!
!Creates a loopback interface in the vpn1 VRF. You do this for each customer VRF you IP
!unnumber interfaces to.
interface Loopback1
    ip vrf forwarding vpn1
    ip address 10.16.1.1 255.255.255.255
!
!Configures the management interface. You should not configure VPN over the FastEthernet
!interface.
interface FastEthernet0/0/0
    ip address 192.168.16.1 255.255.255.0
    no ip proxy-arp
!
!Enables label switching of IP packets on the interface.
interface GigabitEthernet1/0/0
    ip address 172.16.4.1 255.255.0.0
    negotiation auto
    tag-switching ip
!
```

```

interface GigabitEthernet2/0/0
  ip address 172.16.3.1 255.255.0.0
  negotiation auto
  tag-switching ip
!
interface ATM3/0/0
  no ip address
  atm flag sls0 0
  atm sonet stm-4
  no atm ilmi-keepalive
!
interface ATM4/0/0
  no ip address
  load-interval 30
  no atm pxf queuing
  atm sonet stm-4
  no atm ilmi-keepalive
!
interface ATM4/0/0.1 multipoint
  range pvc 3/32 3/354
    encapsulation aa5mux ppp Virtual-Template1
!
interface ATM6/0/0
  no ip address
  no atm pxf queuing
  no atm ilmi-keepalive
!
interface atm6/0/1
  no ip address
  no atm ilmi-keepalive
!
interface ATM6/0/2
  no ip address
  no atm ilmi-keepalive
!
interface ATM6/0/3
  no ip address
  no atm ilmi-keepalive
!
!Enables label switching of IP packets on the interface.
interface POS7/0/0
  ip address 172.16.1.1 255.255.0.0
  keepalive 30
  tag-switching ip
  crc32
!
interface POS8/0/0
  ip address 172.16.2.1 255.255.0.0
  keepalive 30
  tag-switching ip
  crc32
!
!Configures the virtual template and associates the vpn1 VRF with it.
interface Virtual-Template1
  ip vrf forwarding vpn1
  ip unnumbered Loopback1
  peer default ip address pool vpn1
  ppp max-configure 255
  ppp max-failure 255
  ppp authentication chap
  ppp timeout retry 25
  ppp timeout authentication 20
!
!Configures OSPF to advertise networks.

```

```
router ospf 200
  log-adjacency-changes
  auto-cost reference-bandwidth 10000
  network 10.1.1.1 0.0.0.0 area 40
  network 172.16.0.0 0.255.255.255 area 40
!
!Configures BGP to advertise the networks for each VPN.
router bgp 100
  bgp router-id 10.1.1.1
  no bgp default ipv4-unicast
  bgp cluster-id 671154433
  bgp log-neighbor-changes
  bgp bestpath scan-time 30
  bgp scan-time 30
  neighbor 10.1.1.4 remote-as 100
  neighbor 10.1.1.4 update-source Loopback0
  neighbor 10.1.1.4 activate
!
!Enters address family configuration mode to configure the VRF routing table on BGP.
address-family ipv4 vrf vpn1
  redistribute connected
  no auto-summary
  no synchronization
  exit-address-family
!
!Configures MP-IBGP.
address-family vpnv4
  neighbor 10.1.1.4 activate
  neighbor 10.1.1.4 send-community both
  exit-address-family
!
!Specifies the IP local pool to use for the vpn1 VRF address assignment.
ip local pool vpn1 192.168.1.1 192.168.2.67
!
!Enters routing information in the routing table.
ip classless
ip route 192.168.16.0 255.255.255.0 198.168.76.1
no ip http server
ip pim bidir-enable
!
!
no cdp run
!Configures RADIUS accounting. radius-server retransmit is on by default and cannot be
removed.
radius-server retransmit 3
radius-server authorization permit missing Service-Type
call admission limit 90
!
```

## PPPoE to MPLS VPN Configuration Example

[Example 3-13](#) shows how to configure the RA to MPLS VPN feature with one VRF for PPPoE sessions.

### Example 3-13 Configuring PPPoE to MPLS VPN

```

!
!Enables the AAA access control model.
aaa new-model
!
!Configures AAA accounting.
aaa authentication login default none
aaa authentication enable default none
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization network default local
aaa session-id common
enable password cisco
!
username pppoe password 0 pppoe
username pppoa password 0 pppoa
username common password 0 common
!
!Preprovisions slots in the Cisco 10000 series router for line cards.
card 1/0 1gigetheretnet-1
card 2/0 1gigetheretnet-1
card 3/0 loc12pos-1
card 4/0 loc12pos-1
card 5/0 loc12atm-1
card 6/0 loc12atm-1
card 7/0 4oc3atm-1
card 8/0 4oc3atm-1
!
!Creates the common VRF.
ip vrf common
 rd 100:1000
  route-target export 100:1000
  route-target import 100:1000
!
!Specifies the VPDN group to be used to establish PPPoE sessions and specifies the maximum
!number of PPPoE sessions to be established over a virtual circuit.
vpdn-group pppoe
 accept-dialin
  protocol pppoe
  virtual-template 1
 pppoe limit per-mac 32000
 pppoe limit per-vc 1
!
no virtual-template snmp
!
!Configures the small buffer.
buffers small permanent 15000
!
vc-class atm vpn
 protocol pppoe
 encapsulation aal5snap
!
!Defines the general loopback interface used for reachability to the router and as a
!source IP address for sessions (IBGP, TDP, and so on).
interface Loopback0
 ip address 10.16.3.1 255.255.255.255
 ip ospf network point-to-point

```

```
!  
!Creates a loopback interface in the vpn1 VRF. You do this for each customer VRF you IP  
!unnumber interfaces to.  
interface Loopback1  
  ip vrf forwarding vpn1  
  ip address 10.24.1.1 255.255.255.255  
!  
interface Loopback2  
  ip vrf forwarding vpn2  
  ip address 10.8.1.2 255.255.255.255  
!  
!Configures the management interface. You should not configure VPN over the FastEthernet  
!interface.  
interface FastEthernet0/0/0  
  ip address 10.9.100.32 255.0.0.0  
  no ip proxy-arp  
  full-duplex  
!  
!Enables label switching of IP packets on the interface.  
interface GigabitEthernet1/0/0  
  ip address 10.1.10.1 255.255.0.0  
  no ip redirects  
  load-interval 30  
  negotiation auto  
  tag-switching ip  
!  
interface GigabitEthernet2/0/0  
  ip address 10.2.10.1 255.255.0.0  
  no ip redirects  
  load-interval 30  
  negotiation auto  
  tag-switching ip  
!  
interface POS3/0/0  
  ip address 10.3.10.1 255.255.0.0  
  no ip redirects  
  ip ospf cost 2  
  keepalive 30  
  tag-switching ip  
  crc 32  
  clock source internal  
  pos scramble-atm  
!  
interface POS4/0/0  
  ip address 10.4.10.1 255.255.0.0  
  no ip redirects  
  ip ospf cost 2  
  keepalive 30  
  tag-switching ip  
  crc 32  
  clock source internal  
  pos scramble-atm  
!  
interface ATM5/0/0  
  no ip address  
  load-interval 30  
  no atm pxf queuing  
  atm clock INTERNAL  
  atm sonet stm-4  
  no atm ilmi-keepalive  
!  
interface ATM5/0/0.1000 multipoint  
  range pvc 2/32 2/63  
!
```

```

class-int vpn
!
interface ATM6/0/0
no ip address
load-interval 30
no atm pxf queuing
atm clock INTERNAL
atm sonet stm-4
no atm ilmi-keepalive
!
interface ATM6/0/0.1000 multipoint
range pvc 2/32 2/63
encapsulation aal5snap
protocol pppoe
!
class-int vpn
!
interface ATM7/0/0
no ip address
no atm ilmi-keepalive
!
interface ATM7/0/1
no ip address
no atm ilmi-keepalive
!
interface ATM7/0/2
no ip address
no atm ilmi-keepalive
!
interface ATM7/0/3
no ip address
no atm ilmi-keepalive
!
interface ATM8/0/0
no ip address
no atm ilmi-keepalive
!
interface ATM8/0/1
no ip address
no atm ilmi-keepalive
!
interface ATM8/0/2
no ip address
no atm ilmi-keepalive
!
interface ATM8/0/3
no ip address
no atm ilmi-keepalive
!
interface ATM8/0/3.100 multipoint
range pvc 2/32 2/42
encapsulation aal5snap
protocol pppoe
!
!Associates the common VRF with the interface.
interface ATM8/0/3.101 point-to-point
ip vrf forwarding common
ip address 10.22.10.1 255.255.255.0
pvc 3/32
encapsulation aal5snap
!

```

```
!Defines the virtual template and associates the common VRF with it.
interface Virtual-Template1
 ip vrf forwarding common
 ip unnumbered Loopback1
 peer default ip address pool common
 ppp authentication chap
!
!Configures OSPF to advertise the networks.
router ospf 100
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 network 10.16.3.1 0.0.0.0 area 0
 network 10.1.0.0 0.0.255.255 area 0
 network 10.2.0.0 0.0.255.255 area 0
 network 10.3.0.0 0.0.255.255 area 0
 network 10.4.0.0 0.0.255.255 area 0
!
router rip
 version 2
!
!Enters address family configuration mode to configure the VRF for PE to CE routing
!sessions.
 address-family ipv4 vrf common
 version 2
 network 10.0.0.0
 no auto-summary
 exit-address-family
!
!Configures BGP to advertise the networks for the VPN.
router bgp 100
 no synchronization
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 172.16.1.4 remote-as 100
 neighbor 172.16.1.4 activate
!
!Enters address family configuration mode to configure the common VRF for PE to CE routing
!sessions.
 address-family ipv4 vrf common
 no auto-summary
 no synchronization
 aggregate-address 2.10.0.0 255.255.0.0 summary-only
 exit-address-family
!
 address-family vpnv4
 neighbor 172.16.1.4 activate
 neighbor 172.16.1.4 send-community both
 exit-address-family
!
!Specifies the IP local pool to use for the VRF address assignment.
ip local pool common 2.10.1.1 2.10.126.0
ip classless
!Enters routing information in the routing table for the VRF.
ip route 20.0.0.0 255.0.0.0 FastEthernet0/0/0 20.9.0.1
ip route vrf common 10.22.0.0 255.255.0.0 Null0
ip route vrf common 10.30.0.0 255.255.0.0 2.1.1.1 3
ip route vrf common 10.32.0.0 255.255.0.0 2.2.151.1 2
ip route vrf common 10.33.0.0 255.255.0.0 2.3.101.1 2
no ip http server
ip pim bidir-enable
!
no cdp run
!
```

```

!Specifies the RADIUS host and configures RADIUS accounting. radius-server retransmit is
!on by default and cannot be removed.
radius-server host 10.19.100.150 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key test
radius-server authorization permit missing Service-Type
radius-server vsa send authentication
call admission limit 90
!

```

## RBE to MPLS VPN Configuration Example

[Example 3-14](#) shows how to configure RBE on ATM interfaces, creates and associates two VRFs named *CustomerA* and *CustomerB*, and configures DHCP Option 82 support for RBE connections.

### Example 3-14 Configuring RBE to MPLS VPN

```

ip vrf CustomerA
rd 100:100
route-target export 100:100
route-target import 100:100
!
ip vrf CustomerB
rd 101:101
route-target export 101:101
route-target import 101:101
!
interface int g1/0/0
ip address 192.168.1.1 255.255.255.0
tag-switching ip
!
interface loopback0
! BGP update source
ip address 10.100.10.1 255.255.255.255
!
router ospf 1
network 192.168.1.0 0.0.0.255 area 0
redistribute connected
!
interface loopback 1
! description for VRF CustomerA
ip address 10.101.10.1 255.255.255.255
ip vrf forwarding CustomerA
!
interface loopback 2
! description for VRF CustomerB
ip address 10.102.20.1 255.255.255.255
ip vrf forwarding CustomerB
!
ip dhcp relay information option
ip dhcp relay information option vpn
!
interface atm7/0/0
no atm pxf queuing
!
interface atm7/0/0.1 point-to-point
ip vrf forwarding CustomerA
ip unnumbered loopback1
ip helper-address vrf CustomerA 192.168.2.1
atm route ip
range pvc 101/32 101/2031

```

```
encapsulation aal5snap
!
interface atm8/0/0
no atm pxf queuing
!
interface atm8/0/0.1 point-to-point
ip vrf forwarding CustomerB
ip unnumbered loopback2
 ip helper-address vrf CustomerB 192.168.3.1
atm route ip
range pvc 102/32 102/2031
encapsulation aal5snap
!
router bgp 1
no synchronization
redistribute connected
neighbor 192.168.1.2 remote-as 1
neighbor 192.168.1.2 update source loopback0
neighbor 192.168.1.2 activate
no auto-summary
!
address-family ipv4 vrf CustomerA
redistribute connected
redistribute static
no auto-summary
no synchronization
exit-address-family
!
address-family ipv4 vrf CustomerB
redistribute connected
redistribute static
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor 192.168.1.2 activate
neighbor 192.168.1.2 send-community extended
no auto-summary
exit-address-family
```

## Monitoring and Maintaining an MPLS Configuration

To monitor and maintain an MPLS configuration, perform the following verification tasks:

- [Verifying the Routing Protocol Is Running, page 3-40](#)
- [Verifying MPLS, page 3-40](#)
- [Verifying Connections Between Neighbors, page 3-40](#)
- [Verifying Label Distribution, page 3-41](#)
- [Verifying Label Bindings, page 3-42](#)
- [Verifying Labels Are Set, page 3-43](#)

For more information, see the “Troubleshooting Tag and MPLS Switching Connections” chapter in the *ATM and Layer 3 Switch Router Troubleshooting Guide, Cisco IOS Release 12.1(13)E1*.

## Verifying the Routing Protocol Is Running

To verify that the routing protocol is running, enter any of the following commands in privileged EXEC mode:

| Command                          | Purpose                                                                                                                                                               |
|----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router# <b>show ip protocols</b> | Displays the parameters and current state of the active routing protocol process. Ensure that the protocol routes for the MPLS network and all neighbors are present. |
| Router# <b>show ip route</b>     | Displays the current state of the routing table. Ensure that all routers and routes are present.                                                                      |

## Verifying MPLS

To verify MPLS, enter the following command in privileged EXEC mode:

| Command                             | Purpose                                                                                                                                                                                                                          |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router# <b>show mpls interfaces</b> | Displays information about the interfaces that have been configured for label switching. Use this command to verify that MPLS is globally enabled and that a label distribution protocol is running on the requested interfaces. |

### Example 3-15 show mpls interfaces

```
Router# show mpls interfaces

InterfaceIPTunnelOperational
(...)
Serial0/1.1Yes (tdp)YesYes
Serial0/1.2YesYesNo
Serial0/1.3Yes (tdp)YesYes
(...)
```

The fields in this example indicate the following:

- IP field—Indicates that MPLS IP is configured for an interface. The label distribution protocol (LDP) appears in parentheses to the right of the IP status. The LDP is either Tag Distribution Protocol (TDP) as defined in the Cisco Tag Switching architecture, or LDP as defined by IETF in RFC 3036.
- Tunnel field—Indicates the capacity of traffic engineering on the interface.
- Operational field—Indicates the status of the LDP. In the above example, the Operational field indicates down on Serial 0/1.2 because the interface is down.

## Verifying Connections Between Neighbors

An unlabeled connection must exist between each pair of neighboring routers. The routing protocol and the label distribution protocol use the unlabeled connection to build the routing table and the Label Forwarding Information Base (LFIB).

To verify the connections between neighbors, enter any of the following commands in privileged EXEC mode:

| Command                                                           | Purpose                                                |
|-------------------------------------------------------------------|--------------------------------------------------------|
| Router# <b>ping</b> [protocol   tag] {host-name   system-address} | Verifies basic network connectivity between neighbors. |
| Router# <b>ping vrf</b> vrf-name system-address                   | Verifies connectivity to the VRF specified.            |
| Router# <b>debug mpls packet</b>                                  | Verifies that MPLS labels are set.                     |



#### Caution

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco Systems technical support personnel. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

#### Example 3-16 ping

```
Router# ping 10.10.10.6
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 10.10.10.6, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 56/56/60 ms

#### Example 3-17 ping vrf

```
Router# ping vrf vrf-1 192.168.1.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4/ ms

## Verifying Label Distribution

To verify label distribution, enter any of the following commands in privileged EXEC mode:

| Command                                         | Purpose                                                                                           |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Router# <b>show mpls forwarding-table</b>       | Displays the discovered neighbors. The Local Tag field displays the label assigned by the router. |
| Router# <b>show tag-switching tdp discovery</b> | Displays the status of the LDP discovery process.                                                 |

**Example 3-18 show mpls forwarding-table Command**

```
Router# show mpls forwarding-table

LocalOutgoingPrefixBytes tagOutgoingNext Hop
tag tag or VCor Tunnel Idswitchedinterface
16 Untagged10.1.0.0/160AT9/0/010.4.4.2
17 Untagged10.0.0.0/80AT9/0/010.4.4.2
18 Untagged192.168.0.0/160AT9/0/110.6.6.2
19 Pop tag192.168.2.1/32624Fa11/0/0172.16.0.1
20 Pop tag192.168.2.2/320Fa11/0/1172.16.0.18
```

In [Example 3-19](#), TDP is used to bind labels with routes. If label distribution protocol is running correctly, it assigns one label per forwarding equivalent class. If any of the presumed neighbors is missing and cannot be pinged, a connectivity problem exists and the label distribution protocol cannot run.

**Example 3-19 show tag-switching tdp discovery Command**

```
Router# show tag-switching tdp discovery

Local TDP Identifier:
  10.10.10.3:0
Discovery Sources:
  Interfaces:
    Serial0/1.1 (tdp): xmit/recv
      TDP Id: 10.10.10.1:0
    Serial0/1.2 (tdp): xmit/recv
      TDP Id: 10.10.10.2:0
    Serial0/1.3 (tdp): xmit/recv
      TDP Id: 10.10.10.6:0
```



**Note**

The neighbor relationship is not established when the router ID for the label distribution protocol cannot be reached from the global routing table.

# Verifying Label Bindings

To verify label bindings, enter any of the following commands in privileged EXEC mode:

| Command                                                                                        | Purpose                                                            |
|------------------------------------------------------------------------------------------------|--------------------------------------------------------------------|
| Router# <b>show mpls ip bindings</b>                                                           | Displays the labels assigned to each destination.                  |
| Router# <b>show mpls tag-switching forwarding-table</b><br>{ip-address   prefix} <b>detail</b> | Displays the different routes and the labels associated with them. |

**Example 3-20 show mpls ip bindings Command**

```
Router# show mpls ip binding

10.4.4.0/24
  in label:imp-null
  out label:imp-nullsr: 172.16.1.18:0
10.6.6.0/24
  in label:imp-null
  out label:imp-nullsr: 172.16.1.18:0
```

```

10.0.0.0/8
    in label:17
10.18.0.0/8
    out label:16
172.16.1.0/30
    in label:imp-null
    out label:imp-null1sr: 192.168.1.1:0
    out label:201sr: 172.16.1.18:0
172.16.1.16/30
    in label:imp-null
    out label:161sr: 192.168.1.1:0
    out label:imp-null1sr: 172.16.1.18:0

```

## Verifying Labels Are Set

To verify that the labels are set, enter the following command in privileged EXEC mode:

| Command                                  | Purpose                                                                            |
|------------------------------------------|------------------------------------------------------------------------------------|
| Router# <b>traceroute</b> <i>address</i> | Displays the route to the specified address and the labels set for the interfaces. |

### Example 3-21 traceroute Command

```

Router# traceroute 10.10.10.4

Type escape sequence to abort.
Tracing the route to 10.10.10.4
  1 10.1.1.21 [MPLS: Label 25 Exp 0] 296 msec 256 msec 244 msec
  2 10.1.1.5 [MPLS: Label 22 Exp 0] 212 msec 392 msec 352 msec
  3 10.1.1.14 436 msec * 268 msec

```

## Monitoring and Maintaining the MPLS VPN

To monitor and maintain an MPLS VPN configuration, perform the following verification tasks:

- [Verifying VRF Configurations, page 3-44](#)
- [Verifying the Routing Table, page 3-44](#)
- [Verifying the PE to PE Routing Protocols, page 3-45](#)
- [Verifying the PE to CE Routing Protocol, page 3-46](#)
- [Verifying the MPLS VPN Labels, page 3-46](#)
- [Testing the VRF, page 3-46](#)



**Note** Before you establish an MPLS VPN, verify the connections between PE routers by using the **ping** command.

## Verifying VRF Configurations

To verify VRF configurations, enter any of the following commands in privileged EXEC mode:

| Command                                    | Purpose                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router# <b>show ip vrf</b>                 | Displays a summary of all VRFs present on the current router and their associated route distinguishers and interfaces. Use this command to verify the names and configuration of each VRF and the route distinguisher configuration at each PE router.                                                                                           |
| Router# <b>show ip vrf interfaces</b>      | Displays the VRFs present on the router and the associated interfaces.                                                                                                                                                                                                                                                                           |
| Router# <b>show ip vrf detail vrf-name</b> | Displays detailed information about the VRF you specify. Use this command to determine if the global routing table contains all connected addresses, if the exported routing attributes of a VRF on a PE router are the imported routing attributes of the VRF on another PE router, and to determine the status and IP addresses of interfaces. |

### Example 3-22 show ip vrf interfaces Command

```
Router# show ip vrf interfaces

InterfaceIP-AddressVRFProtocol
Loopback101100.0.6.1vrf-1up
Loopback111200.1.6.1vrf-2up
```

### Example 3-23 show ip vrf detail vrf-name

```
Router# show ip vrf detail vrf-1

VRF vrf-1; default RD 100:101
  Interfaces:
    Loopback101Loopback111
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:1001
  Import VPN route-target communities
    RT:100:1001
  No import route-map
  No export route-map
```

## Verifying the Routing Table

To verify the routing table for VRFs, enter any of the following commands in privileged EXEC mode:

| Command                                                  | Purpose                                                       |
|----------------------------------------------------------|---------------------------------------------------------------|
| Router# <b>show ip route vrf vrf-name</b>                | Displays MPLS VPN connections in the routing table.           |
| Router# <b>show ip route vrf vrf-name system-address</b> | Displays routing table information for the specified address. |

## Verifying the PE to PE Routing Protocols

Border Gateway Protocol (BGP) is used for routing sessions between PE routers. To verify PE to PE routing sessions, enter any of the following commands in privileged EXEC mode:

| Command                                                  | Purpose                                                                                                      |
|----------------------------------------------------------|--------------------------------------------------------------------------------------------------------------|
| Router# <b>show ip bgp neighbors</b>                     | Displays detailed information on the BGP and TCP connections to individual neighbors.                        |
| Router# <b>show ip bgp vpnv4 all</b>                     | Shows the VPN address information from the BGP table.                                                        |
| Router# <b>show ip bgp vpnv4 vrf vrf-name</b>            | Displays network layer reachability information associated with the specified VRF.                           |
| Router# <b>show ip bgp vpnv4 vrf vrf-name ip-address</b> | Displays network layer reachability information associated with the specified VRF and a specific connection. |

### Example 3-24 show ip bgp vpnv4 all Command

```
Router# show ip bgp vpnv4 all

BGP table version is 17, local router ID is 192.168.1.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Route Distinguisher: 100:1 (default for vrf vrf-1)
*>i10.1.1.0/24192.168.1.101000101?
*>i172.16.1.100/30192.168.1.101000?
*> 172.16.1.116/300.0.0.0032768?
*>i172.16.42.0/24192.168.1.101000101?
*>i192.168.2.1/32192.168.1.101000101i
*> 192.168.5.1/32172.16.1.11800202i
Route Distinguisher: 200:1 (default for vrf vrf-2)
*>i172.16.2.100/30192.168.1.101000?
*> 172.16.2.116/300.0.0.0032768?
```

### Example 3-25 show ip bgp vpnv4 vrf vrf-name ip-address Command

```
Router# show ip bgp vpnv4 vrf vrf-1 172.16.2.116

BGP routing table entry for 200:1:172.16.2.116/30, version 7
Paths: (1 available, best #1, table vrf-1)
  Advertised to non peer-group peers:
    192.168.1.1
  Local
    0.0.0.0 from 0.0.0.0 (102.168.1.2)
      Origin incomplete, metric 0, localpref 100, weight 32768, valid, sourced
      Extended Community: RT:200:1
```

## Verifying the PE to CE Routing Protocol

If the CE router uses a routing protocol other than BGP (for example, RIP or OSPF), enter any of the following commands in privileged EXEC mode to verify the PE to CE routing sessions:

| Command                                                                                | Purpose                                                                                                            |
|----------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------|
| Router# <b>show ip rip database vrf</b> <i>vrf-name</i>                                | Displays summary address entries in the Routing Information Protocol (RIP) routing database for the specified VRF. |
| Router# <b>show ip ospf</b> [ <i>process-id</i> [ <i>area-id</i> ]]<br><b>database</b> | Displays lists of information related to the OSPF database for a specific router.                                  |



### Note

The **show ip rip database vrf** and **show ip ospf** commands are useful for verifying the routing table from the CE router side of the connection and for determining if neighbors are missing from the routing table.

## Verifying the MPLS VPN Labels

An MPLS VPN uses a transport label to identify the VRF and another label to identify the backbone. To verify the MPLS VPN labels, enter any of the following commands in privileged EXEC mode:

| Command                                                  | Purpose                                                                                                                               |
|----------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|
| Router# <b>traceroute vrf</b> <i>vrf-name ip-address</i> | Displays the transport addresses for the specified VRF. Ensure that the interfaces displayed are the correct cross-connect addresses. |
| Router# <b>show ip bgp vpnv4 all tags</b>                | Displays the labels for a particular VRF.                                                                                             |



### Note

The **traceroute vrf** command works with an MPLS-aware traceroute, and only if the backbone ATM switch routers are configured to propagate and generate IP Time to Live (TTL) information.

### Example 3-26 *traceroute vrf* Command

```
Router# traceroute vrf vrf-1 192.168.1.1
```

```
Type escape sequence to abort.
```

```
Tracing the route to 192.168.1.1
```

```
 1 10.0.1.17 4 msec 0 msec 4 msec
 2 10.0.1.101 0 msec 0 msec 0 msec
 3 10.0.1.102 4 msec * 0 msec
```

## Testing the VRF

To test the VRF to ensure that it is working properly, enter any of the following commands in privileged EXEC mode:

| Command                                                           | Purpose                                                             |
|-------------------------------------------------------------------|---------------------------------------------------------------------|
| Router# <b>ping</b> [protocol   tag] {host-name   system-address} | Verifies basic network connectivity between neighbors.              |
| Router# <b>ping vrf</b> vrf-name system-address                   | Tests network connectivity of the specified VRF from the PE router. |

### Example 3-27 ping vrf vrf-name system-address Command

```
Router# ping vrf vrf-1 192.168.6.1
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.6.1, timeout is 2 seconds:

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 176/264/576 ms

## Monitoring and Maintaining PPPoX to MPLS VPN

To monitor and maintain PPPoX to MPLS VPN environments, enter any of the following commands in privileged EXEC mode:

| Command                                                           | Purpose                                                                                                                                                                  |
|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router# <b>show atm pvc ppp</b>                                   | Displays all ATM PVCs and PPPoA traffic information.<br><b>Note</b> This command applies only to PPPoA sessions.                                                         |
| Router# <b>show int virtual-access</b> virtual access interface # | Displays status, traffic data, and configuration information about a specified virtual access interface.                                                                 |
| Router# <b>show ip route vrf</b> vrf-name                         | Displays the IP routing table associated with a VRF.                                                                                                                     |
| Router# <b>show ip local pool</b>                                 | Displays statistics for any defined IP address pools.                                                                                                                    |
| Router# <b>show vpdn session</b> [all]                            | Displays information about active L2TP tunnel and message identifiers in a virtual private dialup network (VPDN).<br><b>Note</b> This command applies to PPPoE sessions. |
| Router# <b>show vpdn tunnel</b>                                   | Displays information about active L2TP tunnel and message identifiers in a VPDN.<br><b>Note</b> This command applies to PPPoE sessions.                                  |
| Router# <b>debug aaa authentication</b>                           | Displays information about AAA authentication.                                                                                                                           |
| Router# <b>debug aaa authorization</b>                            | Displays information about AAA authorization.                                                                                                                            |
| Router# <b>debug ip peer</b>                                      | Displays address activity and contains additional output when pool groups are defined.                                                                                   |
| Router# <b>debug ppp negotiation</b>                              | Displays PPP packets transmitted during PPP startup where PPP options are negotiated.                                                                                    |
| Router# <b>debug ppp authentication</b>                           | Displays authentication protocol messages, including Challenge Authentication Protocol (CHAP) packet exchanges and Password Authentication Protocol (PAP) exchanges.     |

| Command                                | Purpose                                                                                                                                                                                |
|----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router# <b>debug radius</b>            | Displays information associated with the Remote Authentication Dial-In User (RADIUS) server.                                                                                           |
| Router# <b>debug vpdn pppoe-events</b> | Displays PPPoE protocol errors that prevent a session from being established or errors that cause an established session to be closed.                                                 |
| Router# <b>debug vtemplate</b>         | Displays cloning information for a virtual access interface from the time it is cloned from a virtual template to the time the virtual access interface comes down when the call ends. |

**Caution**

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco Systems technical support personnel. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

**Note**

For more information, see the “Troubleshooting DSL Access to MPLS VPN Integration” chapter in the *Troubleshooting Cisco Remote Access to MPLS VPN Integration, Release 2.0*.

## Monitoring and Maintaining RBE to MPLS VPN

To monitor and maintain RBE to MPLS VPN environments, enter any of the following commands in privileged EXEC mode:

| Command                                      | Purpose                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router# <b>show atm map</b>                  | Displays the list of all configured ATM static maps to remote hosts on an ATM network and on ATM bundle maps.<br><br><b>Note</b> This command enables you to confirm the configuration of the map statements in a static map. This command is useful when an encapsulation failure occurs on a packet because a Layer 3 address could not be mapped to a corresponding Layer 2 address. |
| Router# <b>show atm vc</b>                   | Displays all ATM PVCs, SVCs, and traffic information.                                                                                                                                                                                                                                                                                                                                   |
| Router# <b>show interfaces atm interface</b> | Displays information about the ATM interface.                                                                                                                                                                                                                                                                                                                                           |
| Router# <b>show ip arp vrf name</b>          | Displays the Address Resolution Protocol (ARP) cache associated with a VRF.                                                                                                                                                                                                                                                                                                             |
| Router# <b>show ip route vrf name</b>        | Displays the IP routing table associated with a VRF.                                                                                                                                                                                                                                                                                                                                    |

| Command                                    | Purpose                                                                                                                                                                        |
|--------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Router# <b>debug ip packet</b>             | Displays general IP debugging information and IP security option (IPSO) security transactions.<br><br><b>Note</b> This command is useful if the RFC 1483 PVC does not connect. |
| Router# <b>debug ip dhcp</b>               | Displays information about DHCP client activities and the status of DHCP packets.                                                                                              |
| Router# <b>debug ip dhcp server events</b> | Reports server events, such as address assignments and database updates.                                                                                                       |
| Router# <b>debug ip dhcp server packet</b> | Decodes DHCP receptions and transmissions.                                                                                                                                     |

**Caution**

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use debug commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco Systems technical support personnel. Moreover, it is best to use debug commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased debug command processing overhead will affect system use.

**Note**

For more information, see the “Troubleshooting DSL Access to MPLS VPN Integration” chapter in the *Troubleshooting Cisco Remote Access to MPLS VPN Integration, Release 2.0*.

