MPLS VPN Half-Duplex VRF

This module explains how to ensure that virtual private network (VPN) clients that connect to the same provider edge (PE) router at the edge of the Multiprotocol (MPLS) Virtual Private Network (VPN) use the hub site. This feature prevents the VPN clients from communicating directly with each other by bypassing the hub site. This feature also provides scalable hub-and-spoke connectivity for subscribers of an MPLS VPN service by removing the requirement of one VRF per spoke.

Feature Module History

This module was first published on May 2, 2005, and was most recently updated on May 23, 2006.

Feature Name	Releases	Feature Configuration Information
MPLS VPN: Half Duplex VRF Support	12.3(6) 12.3(11)T	This feature ensures that VPN clients that connect to the same PE router at the edge of the MPLS VPN use the hub site to communicate.
Configuring Scalable Hub-and-Spoke MPLS VPNs	12.2(28)SB	The feature was integrated into the SB train.
MPLS VPN Half-Duplex VRF	12.2(28)SB2	Support for dynamic routing protocols was added. For the Cisco 10000 series routers, see the "Half-Duplex VRF" section of the "Configuring Multiprotocol Label Switching" chapter in the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide* at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/cfggdes/bba/dffsrv.htm#wp1065648

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

CISCO SYSTEMS

Corporate Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Contents

Prerequisites for Configuring MPLS VPN Half-Duplex VRF

You must have a working MPLS core network.

Restrictions for MPLS VPN Half-Duplex VRF

The following are not supported on interfaces configured with MPLS VPN Half-Duplex VRF:

- Multicast
- Carrier-Supporting-Carrier
- Inter-Autonomous System

Information about Configuring MPLS VPN Half-Duplex VRF

To configure this feature, you need to understand the following concepts:

- Overview, page 2
- Upstream and Downstream VRFs, page 3
- Reverse Path Forwarding Check, page 4

For information about this feature on the Cisco 10000 series routers, see the "Half-Duplex VRF" section of the "Configuring Multiprotocol Label Switching" chapter in the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/cfggdes/bba/dffsrv.htm#wp1065648

Overview

This feature prevents local connectivity between subscribers at the spoke provider edge (PE) router and ensures that a hub site instead provides the subscriber connectivity. Any sites that connect to the same PE router must forward intersite traffic using the hub site. This ensures that the routing done at the spoke site moves from the access-side interface to the network-side interface or from the network-side interface to the access-side interface, but never directly from one access-side interface to another access-side interface.

Therefore, this feature prevents situations where the spoke PE router would locally switch the spokes without passing the traffic through the hub site. Thus, subscribers are prevented from directly connecting to each other.

This feature eases configuration by removing an earlier requirement of one VRF per spoke. In earlier releases, when spokes connected to the same PE router, each spoke was configured in a separate VRF to ensure that the traffic between the spokes traversed the central link between the wholesale service provider and the ISP. However, this solution was not scalable. When many spokes connected to the same PE router, configuration of VRFs for each spoke became quite complex and greatly increased memory usage. This was especially true in large-scale environments that supported high-density remote access to Layer 3 VPNs.

Initially, these improvements were implemented in broadband and remote access situations using only static routing among the spokes. Now this feature is also available for standard VPN contexts (including PPPoX and 802.1q VLANs)—employing dynamic routing, numbered IP addresses, and Layer 2 encapsulations.

Figure 1 shows a sample hub-and-spoke topology.

Figure 1   Hub-and-Spoke Topology
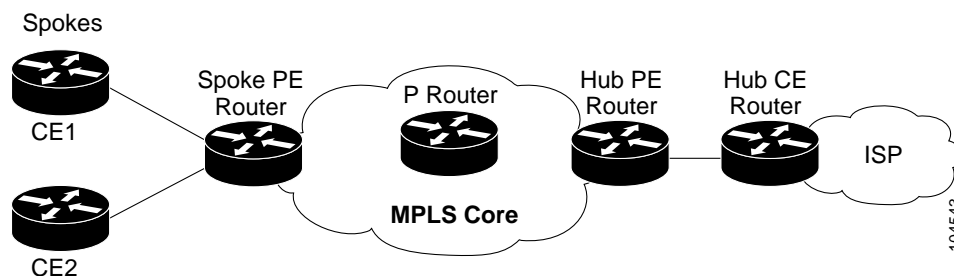
Upstream and Downstream VRFs

This feature uses two unidirectional VRFs to forward IP traffic between the spokes and the hub PE router:

- The upstream VRF forwards IP traffic from the spokes toward the hub PE router. This VRF typically contains only a default route but might also contain summary routes and several default routes. The default route points to the interface on the hub PE router that connects to the upstream ISP. The router dynamically learns about the default route from the routing updates that the hub PE router or home gateway sends.

  Note   Although the upstream VRF is typically populated from the hub, it is possible also to have a separate local upstream interface on the spoke PE for a different local service that would not be required to go through the hub: for example, a local DNS or game server service.

- The downstream VRF forwards traffic from the hub PE router back to the spokes. This VRF can contain:
  - Point-to-Point Protocol (PPP) peer routes for the spokes and per-user static routes received from the Authentication, Authorization, and Accounting (AAA) server or from the DHCP server
  - Routes imported from the hub PE router

> – BGP, OSPF, RIP, or EiGRP dynamic routes for the spokes.

The spoke PE router redistributes routes from the downstream VRF into Multiprotocol Border Gateway Protocol (MP-BGP). That router typically advertises a summary route across the MPLS core for the connected spokes. The VRF configured on the hub PE router imports the advertised summary route.

Reverse Path Forwarding Check

The unicast Reverse Path Forwarding (RPF) check ensures that an IP packet which enters a router uses the correct inbound interface. This feature supports unicast RPF check on the spoke-side interfaces. Because different VRFs are used for downstream and upstream forwarding, the RPF mechanism ensures that source address checks occur in the downstream VRF.

Unicast RPF is not on by default. You need to enable it, an described in *Configuring Unicast Reverse Path Forwarding*.

How to Configure MPLS VPN Half-Duplex VRF

This section contains the following procedures:

- Configuring the Upstream and Downstream VRFs on the Spoke PE Router, page 4 (required)
- Associating VRFs, page 5 (required)
- Configuring the Downstream VRF for an AAA Server, page 7 (optional)
- Verifying the Configuration, page 8 (optional)

To configure this feature on the Cisco 10000 series routers, see the "Half-Duplex VRF" section of the "Configuring Multiprotocol Label Switching" chapter in the *Cisco 10000 Series Router Broadband Aggregation, Leased-Line, and MPLS Configuration Guide* at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/aggr/10000/swconfig/cfggdes/bba/dffsrv.htm#wp1065648

Configuring the Upstream and Downstream VRFs on the Spoke PE Router

To configure the upstream and downstream VRFs on the PE router or on the spoke PE router, use the following procedure.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target** {**import** | **export** | **both**} *route-target-ext-community*
6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip vrf** *vrf-name* **Example:** `Router(config)# ip vrf U`	Enters VRF configuration mode and defines the VRF instance by assigning a VRF name.
Step 4	**rd** *route-distinguisher* **Example:** `Router(config-vrf)# rd 1:0`	Creates routing and forwarding tables.
Step 5	**route-target** {**import** | **export** | **both**} *route-target-ext-community* **Example:** `Router(config-vrf)# route-target import 1:0`	Creates a list of import and export route target communities for the specified VRF. • The **import** keyword is required to create an upstream VRF. The upstream VRF is used to import the default route from the hub PE router. • The **export** keyword is required to create a downstream VRF. The downstream VRF is used to export the routes of all subscribers of a given service that the VRF serves.
Step 6	**exit** **Example:** `Router(config-vrf)# exit`	Returns to global configuration mode.

Associating VRFs

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

• Interface or subinterface

• In the case of broadband or remote-access, 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 on the PE router.

SUMMARY STEPS

1. **enable**

2. **configure terminal**

3. **interface** *type number*

   or

   interface virtual-template *number*

4. **ip vrf forwarding** *vrf-name1* [**downstream** *vrf-name2*]

5. **ip address** *ip-address mask*

   or

   ip unnumbered *type number*

6. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# configure terminal	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** Router(config)# interface POS3/0/1 OR **interface virtual-template** *number* **Example:** Router(config)# interface virtual-template 1	[*For standard VPN situations*]: Moves configuration to a spoke-CE-facing interface or subinterface, and enters interface configuration mode. [*For broadband or remote access situations*]: Creates a virtual template interface that can be configured and applied dynamically in creating spoke-CE-facing virtual access interfaces, and enters interface configuration mode.
Step 4	**ip vrf forwarding** *vrf-name1* [**downstream** *vrf-name2*] **Example:** Router(config-if)# ip vrf forwarding vpn1 downstream D	Associates the interface, subinterface, or virtual template interface with the VRF you specify. • The *vrf-name1* argument is the name of the VRF associated with the interface, subinterface, or virtual template interface. • The *vrf-name2* argument is the name of the downstream VRF into which the peer and per-user routes are installed. [If an AAA server is used, it provides the VRF membership; you do not need to configure the VRF members on virtual templates.]

	Command or Action	Purpose

Step 5	`ip address` *number mask*
	
	Example:
	`Router(config-if)# ip address 10.0.0.1`
	`255.0.0.0`
	
	OR
		[*For standard VPN situations*]: Enables IP processing on the specified interface.

	`ip unnumbered` *type number* **Example:** `Router(config-if)# ip unnumbered Loopback1`	[*For broadband or remote access situations*]: Enables IP processing on an interface without assigning it an explicit IP address. The *type* and *number* arguments are the type and number of another interface on which this router has an assigned IP address. That other interface cannot be unnumbered.

Step 6	`exit`
	
	Example:
	`Router(config-if)# exit`
		Returns to global configuration mode.

Configuring the Downstream VRF for an AAA Server

To configure the downstream VRF for an AAA (RADIUS) server in broadband or remote access situations, enter the following Cisco attribute value:

lcp:interface-config=ip vrf forwarding U downstream D

In standard VPN situations, enter instead the following Cisco attribute value:

ip:vrf-id=U downstream D

Verifying the Configuration

To verify the configuration, perform the following steps.

SUMMARY STEPS

1. **show ip vrf** [**brief** | **detail** | **interfaces** | **id**] [*vrf-name*] [*output-modifiers*]
2. **show ip route vrf** *vrf-name*
3. **show running-config** [**interface** *type number*]

DETAILED STEPS

Step 1   **show ip vrf** [**brief** | **detail** | **interfaces** | **id**] [*vrf-name*] [*output-modifiers*]

Use this command to display information about all of the VRFs configured on the router, including the downstream VRF for each associated interface or VAI.

```
Router# show ip vrf
  Name      Default RD      Interfaces
  Down      100:1           POS3/0/3 [D]
                            POS3/0/1  [D]
            100:3           Loopback2
                            Virtual-Access3 [D]
                            Virtual-Access4 [D]

   Up       100:2           POS3/0/3
                            POS3/0/1
            100:4           Virtual-Access3
                            Virtual-Access4
```

show ip vrf detail *vrf-name*

Use this command to display detailed information about the VRF you specify, including all interfaces, subinterfaces and VAIs associated with the VRF.

If you do not specify a value for *vrf-name*, detailed information about all of the VRFs configured on the router appears.

The following example shows how to display detailed information for the VRF called vrf1, in a broadband or remote access case.

```
Router# show ip vrf detail vrf1

VRF D; default RD 2:0; default VPNID <not set>
  Interfaces:
        Loopback2          Virtual-Access3 [D]  Virtual-Access4 [D]
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:2:0
  Import VPN route-target communities
    RT:2:1
  No import route-map
  No export route-map
VRF U; default RD 2:1; default VPNID <not set>
  Interfaces:
    Virtual-Access3          Virtual-Access4
  Connected addresses are not in global routing table
  No Export VPN route-target communities
  Import VPN route-target communities
    RT:2:1
```

```
  No import route-map
  No export route-map
```

The following example shows the vrf detail in a standard VPN situation.

```
Router# show ip vrf detail
VRF Down; default RD 100:1; default VPNID <not set> VRF Table ID = 1
  Description: import only from hub-pe
  Interfaces:
    Pos3/0/3 [D]        Pos3/0/1:0.1 [D]
  Connected addresses are not in global routing table
  Export VPN route-target communities
    RT:100:0
  Import VPN route-target communities
    RT:100:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF Up; default RD 100:2; default VPNID <not set> VRF Table ID = 2
  Interfaces:
    Pos3/0/1          Pos3/0/3
  Connected addresses are not in global routing table
  No Export VPN route-target communities
  Import VPN route-target communities
    RT:100:1
  No import route-map
  No export route-map
  VRF label distribution protocol: not configured
```

Step 2   **show ip route vrf** *vrf-name*

Use this command to display the IP routing table for the VRF you specify, and information about the per-user routes installed in the downstream VRF.

The following example shows how to display the routing table for the downstream VRF named D, in a broadband or remote access situation.

```
Router# show ip route vrf D

Routing Table: D
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS interarea
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
U       10.0.0.2/32 [1/0] via 2.8.1.1
S       10.0.0.0/8 is directly connected, Null0
U       10.0.0.5/32 [1/0] via 2.8.1.2
C       10.8.1.2/32 is directly connected, Virtual-Access4
C       10.8.1.1/32 is directly connected, Virtual-Access3
```

The following example shows how to display the routing table for the downstream VRF named Down, in a standard VPN situation.

```
Router# show ip route vrf Down
Routing Table: Down
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
```

```
                    E1 - OSPF external type 1, E2 - OSPF external type 2
                    i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
                    ia - IS-IS inter area, * - candidate default, U - per-user static route
                    o - ODR, P - periodic downloaded static route

        Gateway of last resort is 10.13.13.13 to network 0.0.0.0

        C    10.2.0.0/8 is directly connected, Pos3/0/3
             10.3.0.0/32 is subnetted, 1 subnets
        B       10.4.16.16 [200/0] via 10.13.13.13, 1w3d
        B    10.6.0.0/8 [200/0] via 10.13.13.13, 1w3d
        C    10.0.0.0/8 is directly connected, Pos3/0/1
             10.7.0.0/16 is subnetted, 1 subnets
        B       10.7.0.0 [20/0] via 10.0.0.2, 1w3d
             10.0.6.0/32 is subnetted, 1 subnets
        B       10.0.6.14 [20/0] via 10.0.0.2, 1w3d
             10.8.0.0/32 is subnetted, 1 subnets
        B       10.8.15.15 [20/0] via 34.0.0.2, 1w3d
        B*   0.0.0.0/0 [200/0] via 13.13.13.13, 1w3d
```

The following example shows how to display the routing table for the upstream VRF named U in a broadband or remote access situation.

```
Router# show ip route vrf U

Routing Table: U
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS interarea
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.0.20 to network 0.0.0.0

    10.0.0.0/32 is subnetted, 1 subnets
C       10.0.0.8 is directly connected, Loopback2
B*   0.0.0.0/0 [200/0] via 192.168.0.20, 1w5d
```

The following example shows how to display the routing table for the upstream VRF named Up in a standard VPN situation.

```
Router# show ip route vrf Up
Routing Table: Up
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 10.13.13.13 to network 0.0.0.0

    10.2.0.0/32 is subnetted, 1 subnets
C       10.2.0.1 is directly connected, Pos3/0/3
    10.3.0.0/32 is subnetted, 1 subnets
B       10.3.16.16 [200/0] via 10.13.13.13, 1w3d
B    10.6.0.0/8 [200/0] via 10.13.13.13, 1w3d
    10.0.0.0/32 is subnetted, 1 subnets
C       10.0.0.1 is directly connected, Pos3/0/1
B*   0.0.0.0/0 [200/0] via 10.13.13.13, 1w3d
```

Step 3   **show running-config** [**interface** *type number*]

Use this command to display information about the interface, subinterface or VAI you specify, including information about the associated upstream and downstream VRFs.

The following example shows how to display information about the subinterface named POS3/0/1.

```
Router# show running-config interface POS3/0/1

Building configuration...

Current configuration : 4261 bytes
!
interface POS3/0/1
    ip vrf forwarding Up downstream Down
    ip address 10.0.0.1 255.0.0.0
end
```

The following example shows how to display information about the interface named virtual-access 4.

```
Router# show running-config interface virtual-access 4

Building configuration...

Current configuration : 92 bytes
!
interface Virtual-Access4
 ip vrf forwarding U downstream D
 ip unnumbered Loopback2
end
```

Configuration Examples for MPLS VPN Half-Duplex VRF

This section provides the following configuration examples:

- Configuring the Upstream and Downstream VRFs on the Spoke PE Router: Example, page 12
- Associating VRFs: Examples, page 12
- Configuring MPLS VPN Half-Duplex VRF: Example using Static CE-PE Routing, page 12
- Configuring MPLS VPN Half-Duplex VRF: Example using RADIUS Server and Static CE-PE Routing, page 14
- Configuring MPLS VPN Half-Duplex VRF: Example using Dynamic CE-PE Routing, page 15

Configuring the Upstream and Downstream VRFs on the Spoke PE Router: Example

The following example configures an upstream VRF named U:

```
Router> enable
Router# configure terminal
Router(config)# ip vrf U
Router(config-vrf)# rd 1:0
Router(config-vrf)# route-target import 1:0
```

The following example configures a downstream VRF named D:

```
Router> enable
Router# configure terminal
Router(config)# ip vrf D
Router(config-vrf)# rd 1:8
Router(config-vrf)# route-target export 1:100
```

Associating VRFs: Examples

The following example associates the VRF named Up with the POS3/0/1 subinterface and specifies the downstream VRF named Down:

```
Router> enable
Router# configure terminal
Router(config)# interface POS3/0/1
Router(config-if)# ip vrf forwarding Up downstream Down
Router(config-if)# ip address 10.0.0.1 255.0.0.0
```

The following example associates the VRF named U with the virtual-template 1 interface and specifies the downstream VRF named D:

```
Router> enable
Router# configure terminal
Router(config)# interface virtual-template 1
Router(config-if)# ip vrf forwarding U downstream D
Router(config-if)# ip unnumbered Loopback1
```

Configuring MPLS VPN Half-Duplex VRF: Example using Static CE-PE Routing

This example uses the hub-and-spoke topology shown in Figure 2 with local authentication (that is, the RADIUS server is not used).

Figure 2 **Sample Topology**
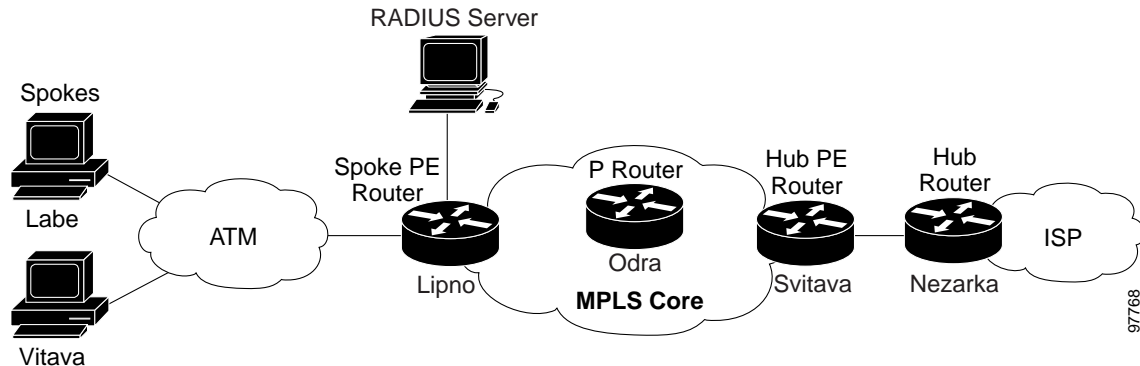

```
ip vrf D
 rd 1:8
 route-target export 1:100
!
ip vrf U
 rd 1:0
 route-target import 1:0
!
ip cef
vpdn enable
!
vpdn-group U
 accept-dialin
  protocol pppoe
  virtual-template 1
!
interface Loopback2
 ip vrf forwarding U
 ip address 10.0.0.8 255.255.255.255
!
interface ATM2/0
 description Mze ATM3/1/2
 no ip address
 no atm ilmi-keepalive
 pvc 0/16 ilmi
!
 pvc 3/100
  protocol pppoe
!
pvc 3/101
  protocol pppoe
!
interface Virtual-Template1
 ip vrf forwarding U downstream D
 ip unnumbered Loopback2
 peer default ip address pool U-pool
 ppp authentication chap
```

Configuring MPLS VPN Half-Duplex VRF: Example using RADIUS Server and Static CE-PE Routing

The following example shows how to connect two Point-to-Point Protocol over Ethernet (PPPoE) clients to a single VRF pair on the spoke PE router named Lipno. Although both PPPoE clients are configured in the same VRF, all communication occurs using the hub PE router. Half-duplex VRFs are configured on the spoke PE. The client configuration is downloaded to the spoke PE from the RADIUS server.

This example uses the hub-and-spoke topology shown in Figure 2.

Note The wholesale provider can forward the user authentication request to the corresponding ISP. If the ISP authenticates the user, the wholesale provider appends the VRF information to the request that goes back to the PE router.

```
aaa new-model
!
aaa group server radius R
 server 10.0.20.26 auth-port 1812 acct-port 1813
!
aaa authentication ppp default group radius
aaa authorization network default group radius
!
ip vrf D
 description Downstream VRF - to spokes
 rd 1:8
 route-target export 1:100
!
ip vrf U
 description Upstream VRF - to hub
 rd 1:0
 route-target import 1:0
!
ip cef
vpdn enable
!
vpdn-group U
 accept-dialin
  protocol pppoe
  virtual-template 1
!
interface Loopback2
 ip vrf forwarding U
 ip address 10.0.0.8 255.255.255.255
!
interface ATM2/0
  pvc 3/100
  protocol pppoe
  !
pvc 3/101
  protocol pppoe
  !
interface virtual-template 1
 no ip address
 ppp authentication chap
!
router bgp 1
 no synchronization
 neighbor 172.16.0.34 remote-as 1
 neighbor 172.16.0.34 update-source Loopback0
```

```
 no auto-summary
 !
address-family vpnv4
  neighbor 172.16.0.34 activate
  neighbor 172.16.0.34 send-community extended
  auto-summary
  exit-address-family
 !
address-family ipv4 vrf U
  no auto-summary
  no synchronization
  exit-address-family
!
address-family ipv4 vrf D
  redistribute static
  no auto-summary
  no synchronization
  exit-address-family
!
ip local pool U-pool 10.8.1.1 2.8.1.100
ip route vrf D 10.0.0.0 255.0.0.0 Null0
!
radius-server host 10.0.20.26 auth-port 1812 acct-port 1813
radius-server key cisco
```

Configuring MPLS VPN Half-Duplex VRF: Example using Dynamic CE-PE Routing

The following example shows how to use OSPF to dynamically advertise the routes on the Spoke sites.

This example uses the hub-and-spoke topology shown in Figure 2.

Creating the VRFs

```
ip vrf Down
    rd 100:1
    route-target export 100:0
!
ip vrf Up
    rd 100:2
    route-target import 100:1
!
```

Enabling MPLS

```
mpls ldp graceful-restart
mpls ldp router-id Loopback0 force
mpls label protocol ldp
!
```

Configuring BGP: towards Core

```
router bgp 100
    no bgp default ipv4-unicast
    bgp log-neighbor-changes
    bgp graceful-restart restart-time 120
    bgp graceful-restart stalepath-time 360
    bgp graceful-restart
    neighbor 10.13.13.13 remote-as 100
    neighbor 10.13.13.13 update-source Loopback0
```

```
    !
    address-family vpnv4
    neighbor 10.13.13.13 activate
    neighbor 10.13.13.13 send-community extended
    bgp scan-time import 5
    exit-address-family
```

Configuring BGP: towards Edge

```
    address-family ipv4 vrf Up
    no auto-summary
    no synchronization
    exit-address-family
    !
    address-family ipv4 vrf Down
    redistribute ospf 1000 vrf Down
    no auto-summary
    no synchronization
    exit-address-family
!
```

Spoke PE's Core-facing Interfaces and Processes

```
interface Loopback0
    ip address 10.11.11.11 255.255.255.255
!
interface POS3/0/2
    ip address 10.0.1.1 255.0.0.0
    mpls label protocol ldp
    mpls ip
!
router ospf 100
    log-adjacency-changes
    auto-cost reference-bandwidth 1000
    nsf enforce global
    redistribute connected subnets
    network 10.11.11.11 0.0.0.0 area 100
    network 10.0.1.0 0.255.255.255 area 100
!
```

Spoke PE's Edge-facing Interfaces and Processes

```
interface Loopback100
    ip vrf forwarding Down
    ip address 10.22.22.22 255.255.255.255
!
interface POS3/0/1
    ip vrf forwarding Up downstream Down
    ip address 10.0.0.1 255.0.0.0
!
interface POS3/0/3
    ip vrf forwarding Up downstream Down
    ip address 10.2.0.1 255.0.0.0
!
router ospf 1000 vrf Down
    router-id 10.22.22.22
    log-adjacency-changes
    auto-cost reference-bandwidth 1000
    nsf enforce global
    redistribute connected subnets
    redistribute bgp 100 metric-type 1 subnets
    network 10.22.22.22 0.0.0.0 area 300
    network 10.0.0.0 0.255.255.255 area 300
```

```
        network 10.2.0.0 0.255.255.255 area 300
        default-information originate
    !
```

Additional References

The following sections provide references related to MPLS VPNs.

Related Documents

Related Topic	Document Title
Basic MPLS VPNs	*Configuring MPLS Layer 3 VPNs*
	Configuring Scalable Hub-and-Spoke MPLS VPNs
MPLS VPN route maps	*Configuring Route Maps to Control the Distribution of MPLS Labels Between Routers in an MPLS VPN*
MPLS VPN load sharing	*Load Sharing MPLS VPN Traffic*
MPLS VPN MIBs	*Monitoring MPLS VPNs with MIBs*
Directing MPLS VPN traffic	• *Directing MPLS VPN Traffic Using Policy-Based Routing*
	• *Directing MPLS VPN Traffic Using a Source IP Address*
VPN ID	*Assigning an ID Number to a VPN*
Dialer applications with MPLS VPNs	• *Dialing to Destinations with the Same IP Address for MPLS VPNs*
MPLS VPNs and OSPF	*Ensuring That MPLS VPN Clients Using OSPF Communicate over the MPLS VPN Backbone Instead of Through Backdoor Links*

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 2547	*BGP/MPLS VPNs*

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport