CHAPTER 1

Configuring VRF-lite

Virtual Private Networks (VPNs) provide a secure way for customers to share bandwidth over an ISP backbone network. A VPN is a collection of sites sharing a common routing table. A customer site is connected to the service provider network by one or more interfaces, and the service provider associates each interface with a VPN routing table. A VPN routing table is called a VPN routing/forwarding (VRF) table.

With the VRF-lite feature, the Catalyst 4500 series switch supports multiple VPN routing/forwarding instances in customer edge devices. (VRF-lite is also termed multi-VRF CE, or multi-VRF Customer Edge Device). VRF-lite allows a service provider to support two or more VPNs with overlapping IP addresses using one interface.

Note
Starting with Cisco IOS Release 12.2(52)SG, the Catalyst 4500 switch supports VRF lite NSF support with routing protocols OSPF/EIGRP/BGP.

Note
The switch does not use Multiprotocol Label Switching (MPLS) to support VPNs. For information about MPLS VRF, refer to the Cisco IOS Switching Services Configuration Guide at:


Note
For complete syntax and usage information for the switch commands used in this chapter, see the Cisco Catalyst 4500 Series Switch Command Reference and related publications at this location:


If the command is not found in the Cisco Catalyst 4500 Command Reference, you can locate it in the larger Cisco IOS library. Refer to the Cisco IOS Command Reference and related publications at this location:


This chapter includes these topics:

- About VRF-lite, page 1-2
- Default VRF-lite Configuration, page 1-3
About VRF-lite

VRF-lite is a feature that enables a service provider to support two or more VPNs, where IP addresses can be overlapped among the VPNs. VRF-lite uses input interfaces to distinguish routes for different VPNs and forms virtual packet-forwarding tables by associating one or more Layer 3 interfaces with each VRF. Interfaces in a VRF can be either physical, such as Ethernet ports, or logical, such as VLAN SVIs, but a Layer 3 interface cannot belong to more than one VRF at any time.

Note

VRF-lite interfaces must be Layer 3 interfaces.

VRF-lite includes these devices:

- **Customer edge (CE) devices** provide customer access to the service provider network over a data link to one or more provider edge routers. The CE device advertises the site’s local routes to the provider edge router and learns the remote VPN routes from it. A Catalyst 4500 series switch can be a CE.

- **Provider edge (PE) routers** exchange routing information with CE devices by using static routing or a routing protocol such as BGP, RIPv1, or RIPv2.

  The PE is only required to maintain VPN routes for those VPNs to which it is directly attached, eliminating the need for the PE to maintain all of the service provider VPN routes. Each PE router maintains a VRF for each of its directly connected sites. Multiple interfaces on a PE router can be associated with a single VRF if all of these sites participate in the same VPN. Each VPN is mapped to a specified VRF. After learning local VPN routes from CEs, a PE router exchanges VPN routing information with other PE routers by using internal BGP (iBGP).

- **Provider routers (or core routers)** are any routers in the service provider network that do not attach to CE devices.

With VRF-lite, multiple customers can share one CE, and only one physical link is used between the CE and the PE. The shared CE maintains separate VRF tables for each customer and switches or routes packets for each customer based on its own routing table. VRF-lite extends limited PE functionality to a CE device, giving it the ability to maintain separate VRF tables to extend the privacy and security of a VPN to the branch office.

**Figure 1-1** shows a configuration where each Catalyst 4500 series switch acts as multiple virtual CEs. Because VRF-lite is a Layer 3 feature, each interface in a VRF must be a Layer 3 interface.
Figure 1-1 illustrates the packet-forwarding process in a VRF-lite CE-enabled network.

- When the CE receives a packet from a VPN, it looks up the routing table based on the input interface. When a route is found, the CE forwards the packet to the PE.

- When the ingress PE receives a packet from the CE, it performs a VRF lookup. When a route is found, the router adds a corresponding MPLS label to the packet and sends it to the MPLS network.

- When an egress PE receives a packet from the network, it strips the label and uses the label to identify the correct VPN routing table. The egress PE then performs the normal route lookup. When a route is found, it forwards the packet to the correct adjacency.

- When a CE receives a packet from an egress PE, it uses the input interface to look up the correct VPN routing table. If a route is found, the CE forwards the packet within the VPN.

To configure VRF, create a VRF table and specify the Layer 3 interface associated with the VRF. You then configure the routing protocols in the VPN and between the CE and the PE. BGP is the preferred routing protocol used to distribute VPN routing information across the providers’ backbone. The VRF-lite network has three major components:

- VPN route target communities—Lists all other members of a VPN community. You need to configure VPN route targets for each VPN community member.

- Multiprotocol BGP peering of VPN community PE routers—Propagates VRF reachability information to all members of a VPN community. You need to configure BGP peering in all PE routers within a VPN community.

- VPN forwarding—Transports all traffic between all VPN community members across a VPN service-provider network.

### Default VRF-lite Configuration

Table 1-1 shows the default VRF configuration.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>VRF</td>
<td>Disabled. No VRFs are defined.</td>
</tr>
<tr>
<td>Maps</td>
<td>No import maps, export maps, or route maps are defined.</td>
</tr>
</tbody>
</table>
Consider these points when configuring VRF in your network:

- A switch with VRF-lite is shared by multiple customers, and all customers have their own routing tables.
- Because customers use different VRF tables, you can reuse the same IP addresses. Overlapped IP addresses are allowed in different VPNs.
- VRF-lite lets multiple customers share the same physical link between the PE and the CE. Trunk ports with multiple VLANs separate packets among customers. All customers have their own VLANs.
- VRF-lite does not support all MPLS-VRF functionality: label exchange, LDP adjacency, or labeled packets.
- For the PE router, there is no difference between using VRF-lite or using multiple CEs. In Figure 1-1, multiple virtual Layer 3 interfaces are connected to the VRF-lite device.
- The Catalyst 4500 series switch supports configuring VRF by using physical ports, VLAN SVIs, or a combination of both. You can connect SVIs through an access port or a trunk port.
- A customer can use multiple VLANs as long because they do not overlap with those of other customers. A customer’s VLANs are mapped to a specific routing table ID that is used to identify the appropriate routing tables stored on the switch.
- The Layer 3 TCAM resource is shared between all VRFs. To ensure that any one VRF has sufficient CAM space, use the `maximum routes` command.
- A Catalyst 4500 series switch using VRF can support one global network and up to 64 VRFs. The total number of routes supported is limited by the size of the TCAM.
- You can use most routing protocols (BGP, OSPF, EIGRP, RIP and static routing) between the CE and the PE. However, we recommend using external BGP (EBGP) for these reasons:
  - BGP does not require multiple algorithms to communicate with multiple CEs.
  - BGP is designed for passing routing information between systems run by different administrations.
  - BGP makes it easy to pass attributes of the routes to the CE.
- VRF-lite does not support IGRP and ISIS.
- VRF-lite does not affect the packet switching rate.
- Starting with Cisco IOS Release 12.2(50)SG, Multicast and VRF can be configured together on a Layer 3 interface.
- The Catalyst 4500 series switch supports all the PIM protocols (PIM-SM, PIM-DM, PIM-SSM, PIM BiDiR).
• Multicast VRF is supported on Supervisor Engine 6-E, Supervisor 6L-E, Catalyst 4900M, and Catalyst 4948E.
• The capability vrf-lite subcommand under router ospf should be used when configuring OSPF as the routing protocol between the PE and the CE.

## Configuring VRFs

To configure one or more VRFs, perform this task:

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Switch(config)# ip routing</td>
<td>Enables IP routing.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Switch(config)# ip vrf vrf-name</td>
<td>Names the VRF and enters VRF configuration mode.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Switch(config-vrf)# rd route-distinguisher</td>
<td>Creates a VRF table by specifying a route distinguisher. Enter either an AS number and an arbitrary number (xxx:y) or an IP address and arbitrary number (A.B.C.D:y).</td>
</tr>
<tr>
<td>Step 5</td>
<td>Switch(config-vrf)# route-target {export</td>
<td>import</td>
</tr>
<tr>
<td>Step 6</td>
<td>Switch(config-vrf)# import map route-map</td>
<td>(Optional) Associates a route map with the VRF.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Switch(config-vrf)# interface interface-id</td>
<td>Enters interface configuration mode and specify the Layer 3 interface to be associated with the VRF. The interface can be a routed port or SVI.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Switch(config-if)# ip vrf forwarding vrf-name</td>
<td>Associates the VRF with the Layer 3 interface.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Switch(config-if)# end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
<tr>
<td>Step 10</td>
<td>Switch# show ip vrf {brief</td>
<td>detail</td>
</tr>
<tr>
<td>Step 11</td>
<td>Switch# copy running-config startup-config</td>
<td>(Optional) Saves your entries in the configuration file.</td>
</tr>
</tbody>
</table>


Use the **no ip vrf vrf-name** global configuration command to delete a VRF and to remove all interfaces from it. Use the **no ip vrf forwarding** interface configuration command to remove an interface from the VRF.
Configuring VRF-Aware Services

IP services can be configured on global interfaces and within the global routing instance. IP services are enhanced to run on multiple routing instances; they are VRF-aware. Any configured VRF in the system can be specified for a VRF-aware service.

VRF-aware services are implemented in platform-independent modules. VRF provides multiple routing instances in Cisco IOS. Each platform has its own limit on the number of VRFs it supports.

VRF-aware services have the following characteristics:
- The user can ping a host in a user-specified VRF.
- ARP entries are learned in separate VRFs. The user can display Address Resolution Protocol (ARP) entries for specific VRFs.

These services are VRF-aware:
- ARP
- Ping
- Simple Network Management Protocol (SNMP)
- Unicast Reverse Path Forwarding (uRPF)
- Syslog
- Traceroute
- FTP and TFTP
- Telnet and SSH
- NTP

Configuring the User Interface for ARP

To configure VRF-aware services for ARP, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# show ip arp vrf vrf-name</td>
<td>Displays the ARP table (static and dynamic entries) in the specified VRF.</td>
</tr>
<tr>
<td>Switch(config)# arp vrf vrf-name</td>
<td>Creates a static ARP entry in the specified VRF.</td>
</tr>
<tr>
<td>ip-address mac-address ARPA</td>
<td></td>
</tr>
</tbody>
</table>

Configuring the User Interface for PING

To perform a VRF-aware ping, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# ping vrf vrf-name ip-host</td>
<td>Pings an IP host or address in the specified VRF.</td>
</tr>
</tbody>
</table>
### Configuring the User Interface for SNMP

To configure VRF-aware services for SNMP, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Switch(config)# snmp-server trap authentication vrf</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Switch(config)# snmp-server engineID remote host vrf vpn-instance engine-id string</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Switch(config)# snmp-server host host vrf vpn-instance traps community</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Switch(config)# snmp-server host host vrf vpn-instance informs community</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Switch(config)# snmp-server user user group remote host vrf vpn-instance security model</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Switch(config)# end</td>
</tr>
</tbody>
</table>

### Configuring the User Interface for uRPF

You can configure uRPF on an interface assigned to a VRF. Source lookup is performed in the VRF table.

To configure VRF-aware services for uRPF, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Switch(config)# interface interface-id</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Switch(config-if)# no switchport</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Switch(config-if)# ip vrf forwarding vrf-name</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Switch(config-if-vrf)# ip address ip-address subnet-mask</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Switch(config-if-vrf)# ip verify unicast source reachable-via rx allow-default</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Switch(config-if-vrf)# end</td>
</tr>
</tbody>
</table>
Configuring the User Interface for Syslog

To configure VRF-aware services for syslog, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Step 2 Switch(config)# logging on</td>
<td>Enables or temporarily disables logging of storage router event message.</td>
</tr>
<tr>
<td>Step 3 Switch(config)# logging host</td>
<td>Specifies the host address of the syslog server where logging messages are to be sent.</td>
</tr>
<tr>
<td>ip-address vrf vrf-name</td>
<td></td>
</tr>
<tr>
<td>Step 4 Switch(config)# logging buffered</td>
<td>Logs messages to an internal buffer.</td>
</tr>
<tr>
<td>logging size debugging</td>
<td></td>
</tr>
<tr>
<td>Step 5 Switch(config)# logging trap</td>
<td>Limits the logging messages sent to the syslog server.</td>
</tr>
<tr>
<td>debugging</td>
<td></td>
</tr>
<tr>
<td>Step 6 Switch(config)# logging facility</td>
<td>Sends system logging messages to a logging facility.</td>
</tr>
<tr>
<td>facility</td>
<td></td>
</tr>
<tr>
<td>Step 7 Switch(config)# end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

Configuring the User Interface for Traceroute

To configure VRF-aware services for traceroute, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>traceroute vrf vrf-name ip-address</td>
<td>Specifies the name of a VPN VRF in which to find the destination address.</td>
</tr>
</tbody>
</table>

Configuring the User Interface for FTP and TFTP

You must configure some FTP and TFTP CLIs in order for FTP and TFTP to be VRF-aware. For example, if you want to use a VRF table that is attached to an interface (for example, E1/0), you need to configure the `ip [t]ftp source-interface E1/0` command to inform [t]ftp to use a specific routing table. In this example, the VRF table is used to look up the destination IP address. These changes are backward-compatible and do not affect existing behavior. You can use the source-interface CLI to send packets out a particular interface even if no VRF is configured on that interface.

To specify the source IP address for FTP connections, use the `ip ftp source-interface` show mode command. To use the address of the interface where the connection is made, use the `no` form of this command.

To configure the user interface for FTP and TFTP, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 Switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
</tbody>
</table>
Configuring Per-VRF for TACACS+ Servers

To specify the IP address of an interface as the source address for TFTP connections, use the `ip tftp source-interface` show mode command. To return to the default, use the `no` form of this command.

To configure VRF-aware for using Telnet and SSH, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# configure terminal</td>
<td>Enters global configuration mode.</td>
</tr>
<tr>
<td>Switch(config)# ip tftp source-interface interface-type interface-number</td>
<td>Specifies the source IP address for TFTP connections.</td>
</tr>
<tr>
<td>Switch(config)# end</td>
<td>Returns to privileged EXEC mode.</td>
</tr>
</tbody>
</table>

To configure VRF-aware for NTP, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# ntp server vrf vrf-name ip-host</td>
<td>Configure the NTP server in the specified VRF.</td>
</tr>
<tr>
<td>Switch# ntp peer vrf vrf-name ip-host</td>
<td>Configure the NTP peer in the specified VRF.</td>
</tr>
</tbody>
</table>

The per-VRF for TACACS+ servers feature allows you to configure per-virtual route forwarding (per-VRF) authentication, authorization, and accounting (AAA) on TACACS+ servers.

Before configuring per-VRF on a TACACS+ server, you must have configured AAA and a server group. You can create the VRF routing table (shown in Steps 3 and 4) and configure the interface (Steps 6, 7, and 8). The actual configuration of per-VRF on a TACACS+ server is done in Steps 10 through 13.
### Configuring VRF-lite

**Chapter 1**

### Configuring Per-VRF TACACS+ Servers

The following example lists all the steps to configure per-VRF TACACS+:

```plaintext
Switch> enable
Switch# configure terminal
Switch(config)# ip vrf vrf-name
Switch(config-vrf)# rd route-distinguisher
Switch(config-vrf)# exit
Switch(config)# interface interface-name
Switch(config-if)# ip vrf forwarding vrf-name
Switch(config-if)# ip address ip-address mask [secondary]
Switch(config-if)# exit
Switch(config)# aaa group server tacacs+
Switch(config)# server-private
Switch(config)# ip vrf forwarding vrf-name
Switch(config)# ip tacacs source-interface subinterface-name
Switch(config)# exit
```

For more information about configuring per-VRF for TACACS+ server, see the *Cisco IOS Per VRF for TACACS+ Server, Release 12.3(7)*.
Configuring Multicast VRFs

To configure multicast within a VRF table, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Switch(config)# ip routing</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Switch(config)# ip vrf vrf-name</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Switch(config-vrf)# ip multicast-routing vrf vrf-name</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Switch(config-vrf)# rd route-distinguisher</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Switch(config-vrf)# route-target {export</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td>Switch(config-vrf)# import map route-map</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td>Switch(config-vrf)# interface interface-id</td>
</tr>
<tr>
<td><strong>Step 9</strong></td>
<td>Switch(config-if)# ip vrf forwarding vrf-name</td>
</tr>
<tr>
<td><strong>Step 10</strong></td>
<td>Switch(config-if)# ip address ip-address mask</td>
</tr>
<tr>
<td><strong>Step 11</strong></td>
<td>Switch(config-if)# ip pim [sparse-dense mode</td>
</tr>
<tr>
<td><strong>Step 12</strong></td>
<td>Switch(config-if)# end</td>
</tr>
<tr>
<td><strong>Step 13</strong></td>
<td>Switch# show ip vrf [brief</td>
</tr>
<tr>
<td><strong>Step 14</strong></td>
<td>Switch# copy running-config startup-config</td>
</tr>
</tbody>
</table>

For more information about configuring a multicast within a Multi-VRF CE, see the Cisco IOS IP Multicast Configuration Guide, Release 12.4.

Use the `no ip vrf vrf-name` global configuration command to delete a VRF and to remove all interfaces from it. Use the `no ip vrf forwarding` interface configuration command to remove an interface from the VRF.
Configuring a VPN Routing Session

Routing within the VPN can be configured with any supported routing protocol (RIP, OSPF, or BGP) or with static routing. The configuration shown here is for OSPF, but the process is the same for other protocols.

To configure OSPF in the VPN, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>Switch(config)# router ospf process-id vrf vrf-name</td>
</tr>
<tr>
<td>Step 3</td>
<td>Switch(config-router)# log-adjacency-changes</td>
</tr>
<tr>
<td>Step 4</td>
<td>Switch(config-router)# redistribute bgp autonomous-system-number subnets</td>
</tr>
<tr>
<td>Step 5</td>
<td>Switch(config-router)# network network-number area area-id</td>
</tr>
<tr>
<td>Step 6</td>
<td>Switch(config-router)# end</td>
</tr>
<tr>
<td>Step 7</td>
<td>Switch# show ip ospf process-id</td>
</tr>
<tr>
<td>Step 8</td>
<td>Switch# copy running-config startup-config</td>
</tr>
</tbody>
</table>

Use the no router ospf process-id vrf vrf-name global configuration command to disassociate the VPN forwarding table from the OSPF routing process.

Configuring BGP PE to CE Routing Sessions

To configure a BGP PE to CE routing session, perform this task:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Switch# configure terminal</td>
</tr>
<tr>
<td>Step 2</td>
<td>Switch(config)# router bgp</td>
</tr>
<tr>
<td>Step 3</td>
<td>Switch(config-router)# network network-number area area-id</td>
</tr>
<tr>
<td>Step 4</td>
<td>Switch(config-router)# redistribute ospf process-id match internal</td>
</tr>
<tr>
<td>Step 5</td>
<td>Switch(config-router)# network network-number area area-id</td>
</tr>
<tr>
<td>Step 6</td>
<td>Switch(config-router-af)# address-family ipv4 vrf vrf-name</td>
</tr>
<tr>
<td>Step 7</td>
<td>Switch(config-router-af)# neighbor address remote-as as-number</td>
</tr>
</tbody>
</table>
Use the `no router bgp autonomous-system-number` global configuration command to delete the BGP routing process. Use the command with keywords to delete routing characteristics.

### VRF-lite Configuration Example

Figure 1-2 is a simplified example of the physical connections in a network similar to that in Figure 1-1. OSPF is the protocol used in VPN1, VPN2, and the global network. BGP is used in the CE to PE connections. The example commands show how to configure the CE switch S8 and include the VRF configuration for switches S20 and S11 and the PE router commands related to traffic with switch S8. Commands for configuring the other switches are not included but would be similar.

![VRF-lite Configuration Example](image)
**Configuring Switch S8**

On switch S8, enable routing and configure VRF.

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# ip vrf v11
Switch(config-vrf)# rd 800:1
Switch(config-vrf)# route-target export 800:1
Switch(config-vrf)# route-target import 800:1
Switch(config-vrf)# exit
Switch(config)# ip vrf v12
Switch(config-vrf)# rd 800:2
Switch(config-vrf)# route-target export 800:2
Switch(config-vrf)# route-target import 800:2
Switch(config-vrf)# exit
```

Configure the loopback and physical interfaces on switch S8. Fast Ethernet interface 3/5 is a trunk connection to the PE. Interfaces 3/7 and 3/11 connect to VPNs:

```
Switch(config)# interface loopback1
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 8.8.1.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface loopback2
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 8.8.2.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface FastEthernet3/5
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface FastEthernet3/8
Switch(config-if)# switchport access vlan 208
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface FastEthernet3/11
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit
```

Configure the VLANs used on switch S8. VLAN 10 is used by VRF 11 between the CE and the PE. VLAN 20 is used by VRF 12 between the CE and the PE. VLANs 118 and 208 are used for VRF for the VPNs that include switch S11 and switch S20, respectively:

```
Switch(config)# interface Vlan10
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 38.0.0.8 255.255.255.0
Switch(config-if)# exit
```
Chapter 1  Configuring VRF-lite

VRF-lite Configuration Example

Switch(config)# interface Vlan20
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 83.0.0.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface Vlan118
Switch(config-if)# ip vrf forwarding v12
Switch(config-if)# ip address 118.0.0.8 255.255.255.0
Switch(config-if)# exit

Switch(config)# interface Vlan208
Switch(config-if)# ip vrf forwarding v11
Switch(config-if)# ip address 208.0.0.8 255.255.255.0
Switch(config-if)# exit

Configure OSPF routing in VPN1 and VPN2:
Switch(config)# router ospf 1 vrf vl1
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router)# network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit
Switch(config)# router ospf 2 vrf vl2
Switch(config-router)# redistribute bgp 800 subnets
Switch(config-router)# network 118.0.0.0 0.0.0.255 area 0
Switch(config-router)# exit

Configure BGP for CE to PE routing:
Switch(config)# router bgp 800
Switch(config-router)# address-family ipv4 vrf vl2
Switch(config-router-af)# redistribute ospf 2 match internal
Switch(config-router-af)# neighbor 83.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 83.0.0.3 activate
Switch(config-router-af)# network 8.8.2.0 mask 255.255.255.0
Switch(config-router-af)# exit
Switch(config-router)# address-family ipv4 vrf vl1
Switch(config-router-af)# redistribute ospf 1 match internal
Switch(config-router-af)# neighbor 38.0.0.3 remote-as 100
Switch(config-router-af)# neighbor 38.0.0.3 activate
Switch(config-router-af)# network 8.8.1.0 mask 255.255.255.0
Switch(config-router-af)# end

Configuring Switch S20

Configure S20 to connect to CE:
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface Fast Ethernet 0/7
Switch(config-if)# no switchport
Switch(config-if)# ip address 208.0.0.20 255.255.255.0
Switch(config-if)# exit

Switch(config)# router ospf 101
Switch(config-router)# network 208.0.0.0 0.0.0.255 area 0
Switch(config-router)# end
Chapter 1      Configuring VRF-lite

VRF-lite Configuration Example

Configuring Switch S11

Configure S11 to connect to CE:

Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip routing
Switch(config)# interface Gigabit Ethernet 0/3
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# no ip address
Switch(config-if)# exit

Switch(config)# interface Vlan118
Switch(config-if)# ip address 118.0.0.11 255.255.255.0
Switch(config-if)# exit

Switch(config)# router ospf 101
Switch(config-router)# network 118.0.0.0 0.0.0.255 area 0
Switch(config-router)# end

Configuring the PE Switch S3

On switch S3 (the router), these commands configure only the connections to switch S8:

Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# ip vrf v1
Router(config-vrf)# rd 100:1
Router(config-vrf)# route-target export 100:1
Router(config-vrf)# route-target import 100:1
Router(config-vrf)# exit

Router(config)# ip vrf v2
Router(config-vrf)# rd 100:2
Router(config-vrf)# route-target export 100:2
Router(config-vrf)# route-target import 100:2
Router(config-vrf)# exit

Router(config)# ip cef
Router(config)# interface Loopback1
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 3.3.1.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface Loopback2
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 3.3.2.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface Fast Ethernet3/0.10
Router(config-if)# encapsulation dot1q 10
Router(config-if)# ip vrf forwarding v1
Router(config-if)# ip address 38.0.0.3 255.255.255.0
Router(config-if)# exit

Router(config)# interface Fast Ethernet3/0.20
Router(config-if)# encapsulation dot1q 20
Router(config-if)# ip vrf forwarding v2
Router(config-if)# ip address 83.0.0.3 255.255.255.0
Router(config-if)# exit
**Chapter 1 Configuring VRF-lite**

**Displaying VRF-lite Status**

To display information about VRF-lite configuration and status, perform one of the following tasks:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Switch# show ip protocols vrf vrf-name</td>
<td>Displays routing protocol information associated with a VRF.</td>
</tr>
<tr>
<td>Switch# show ip route vrf vrf-name [connected] [protocol [as-number]] [list] [mobile] [odr] [profile] [static] [summary] [supernets-only]</td>
<td>Displays IP routing table information associated with a VRF.</td>
</tr>
<tr>
<td>Switch# show ip vrf [brief</td>
<td>detail</td>
</tr>
<tr>
<td>Switch# show ip mroute vrf instance-name a.b.c.d</td>
<td>active</td>
</tr>
</tbody>
</table>

This example shows how to display multicast route table information within a VRF instance:

Switch# show ip mroute vrf mcast2 234.34.10.18

IP Multicast Routing Table

Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group, C - Connected, L - Local, P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT, M - MSDP created entry, X - Proxy Join Timer Running, A - Candidate for MSDP Advertisement, U - URD, I - Received Source Specific Host Report, Z - Multicast Tunnel, z - MDT-data group sender, Y - Joined MDT-data group, y - Sending to MDT-data group V - RD & Vector, v - Vector

Outgoing interface flags: H - Hardware switched, A - Assert winner
Timers: Uptime/Expires
Interface state: Interface, Next-Hop or VCD, State/Mode

(*, 234.34.10.18), 13:39:21/00:02:58, RP 1.1.1.1, flags: BC
Bidir-Upstream: Vlan134, RPF nbr 172.16.34.1
Outgoing interface list:
  Vlan45, Forward/Sparse-Dense, 00:00:02/00:02:57, H
Vlan134, Bidir-Upstream/Sparse-Dense, 13:35:54/00:00:00, H
For more information about the information in the displays, refer to the *Cisco IOS Switching Services Command Reference* at: