



CHAPTER 27

IP Tunneling

This chapter describes IP tunneling features implemented on the Cisco 10000 series routers and includes the following topics:

- [GRE Tunnel IP Source and Destination VRF Membership, page 27-1](#)
- [Restrictions for GRE Tunnel IP Source and Destination VRF Membership, page 27-3](#)
- [How to Configure GRE Tunnel IP Source and Destination VRF Membership, page 27-3](#)
- [Configuration Examples, page 27-4](#)

GRE Tunnel IP Source and Destination VRF Membership

The Generic Routing Encapsulation (GRE) Tunnel IP Source and Destination VRF Membership feature enables both unicast and multicast traffic from subscribers to traverse a tunnel interface on the router and terminate in a VRF. Instead of the termination point being in the global routing table, the tunnel's source and destination endpoints terminate within a non-global VRF.

The following software enhancements provide the functionality required to implement this feature:

- [Tunnel VRF, page 27-1](#)
- [VRF-Aware VPDN Tunnels, page 27-2](#)

For more information, see the *GRE Tunnel IP Source and Destination VRF Membership, Release 12.2(31)SB5* feature guide, located at the following URL:

http://www.cisco.com/en/US/products/ps6566/products_feature_guides_list.html

Tunnel VRF

The Tunnel VRF feature allows you to terminate GRE tunnels in a virtual private network (VPN) routing and forwarding (VRF) instance. Using this feature, you can configure the source and destination of a tunnel to belong to any VRF table.

A VRF table stores routing data for each VPN. The VRF table defines the VPN membership of a customer site attached to the network access server (NAS). Each VRF table comprises an IP routing table, a derived Cisco Express Forwarding (CEF) table, and guidelines and routing protocol parameters that control the information that is included in the routing table.

Previously, GRE IP tunnels required the IP tunnel destination to be in the global routing table. Tunnel VRF enables you to configure the tunnel source and destination to belong to any VRF. Like existing GRE tunnels, the tunnel is disabled if no route to the tunnel destination is defined.

The **tunnel vrf** command is used to configure the Tunnel VRF feature. The VRF specified in the **tunnel vrf** command is the same VRF as the VRF associated with the physical interface over which the tunnel sends packets. This provides outer IP packet routing.

For more detailed information, see the *Generic Routing Encapsulation Tunnel IP Source and Destination VRF Membership* feature module, located at the following URL:

http://www.cisco.com/en/US/products/ps6566/products_feature_guides_list.html

VRF-Aware VPDN Tunnels

The VRF-Aware VPDN Tunnels feature allows you to create VPDN tunnels that use a customer VRF address from a VRF routing table as the tunnel endpoint. The VPDN tunnel terminates in one VRF and the associated PPP sessions terminate in a different VRF. For example, VPDN tunnels can start outside the Multiprotocol Label Switching (MPLS) VPN and terminate within the MPLS VPN.

To configure VRF-Aware VPDN Tunnels, use the **vpn** command in VPDN configuration mode. This command specifies that the source and destination IP addresses of a given VPDN group belong to the specified VRF. Before you enter the **vpn** command, you must first create the VRF instance using the **ip vrf** command. Different VRF-aware VPDN tunnels can have overlapping IP addresses across VRF instances.

The **ip vrf forwarding** command, configured in tunnel interface mode, enables VRF forwarding on an interface. The VRF associated with the tunnel in the **ip vrf forwarding** command configuration is the VRF that the packets are to be forwarded in as the packets exit the tunnel. This provides inner IP packet routing.

The Cisco 10000 series router supports the VRF-Aware VPDN Tunnels feature on the PRE2 and PRE3 and applies to the router when acting as the L2TP access concentrator (LAC) or a Layer 2 network server (LNS). As a LAC or an LNS, the router can initiate and terminate tunnels within a specified VRF.

For more information, see the *VRF-Aware VPDN Tunnels* feature module, located at the following URL:

http://www.cisco.com/en/US/products/ps6566/products_feature_guides_list.html

Feature History for GRE Tunnel IP Source and Destination VRF Membership

Cisco IOS Release	Description	Required PRE
12.3(7)XI7	This feature was integrated into Cisco IOS Release 12.3(7)XI7, enhanced to include domain support, and implemented on the LAC.	PRE2
12.2(28)SB	This feature was integrated in Cisco IOS Release 12.2(28)SB.	PRE2
12.2(31)SB5	This feature was introduced on the PRE3.	PRE3
12.2(33)SB	Support for VRF-Aware VPDN tunnels feature on LNS	PRE3 and PRE4

Restrictions for GRE Tunnel IP Source and Destination VRF Membership

- Both ends of the tunnel must reside within the same VRF.
- The VRF associated with the **tunnel vrf** command is the same as the VRF associated with the physical interface over which the tunnel sends packets (outer IP packet routing).
- The VRF associated with the tunnel by using the **ip vrf forwarding** command is the VRF that the packets are to be forwarded in as the packets exit the tunnel (inner IP packet routing).

How to Configure GRE Tunnel IP Source and Destination VRF Membership

To configure GRE Tunnel IP Source and Destination VRF Membership on the Cisco 10000 series router, perform the following configuration tasks:

- [Configuring Tunnel VRF, page 27-3](#)
- [Configuring VRF-Aware VPDN Tunnels, page 27-4](#)

Configuring Tunnel VRF

The **tunnel vrf** command enables the Tunnel VRF feature by identifying the VRF in which the tunnel destination terminates. When configuring this feature, enter the **tunnel destination** command followed by the **tunnel vrf** command as shown in the following Summary Steps.

Use the following procedure to configure tunnel VRF on the router:

SUMMARY STEPS

1. **enable**
2. **configure** {**terminal** | **memory** | **network**}
3. **interface** **tunnel** *number*
4. **ip vrf forwarding** *vrf-name*
5. **ip address** *ip-address subnet-mask*
6. **tunnel source** (*ip-address* | *type number*)
7. **tunnel destination** *ip-address* {*hostname* | *ip-address*}
8. **tunnel vrf** *vrf-name*

For more detailed information, see the *Generic Routing Encapsulation Tunnel IP Source and Destination VRF Membership* feature module, located at the following URL:

http://www.cisco.com/en/US/products/ps6566/products_feature_guides_list.html

Configuring VRF-Aware VPDN Tunnels

The **vpn** command enables the VRF-Aware VPDN Tunnels feature by associating an IP address configured in a VPDN group with a VRF. This is applied to a VPDN group as shown in the following Summary Steps.

Use the following commands to configure VRF-aware VPDN tunnels on the router:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **vpdn-group** *name*
4. **request-dialin**
5. **protocol** [**l2f** | **l2tp**| **pptp**]
6. **domain** *domain-name*
7. **exit**
8. **vpn** {**vrf** *vrf-name* | **id** *vpn-id*}
9. **source-ip** *ip-address*
10. **initiate-to ip** *ip-address* [**limit** *limit-number*] [**priority** *priority-number*]
11. **exit**



Note

For Cisco IOS Release 12.2(31)SB5 and later releases, when configuring VRF-aware VPDN tunnels on the Cisco 10000 series router, different tunnels can have overlapping IP addresses across VRF instances.

For more detailed information, see the *VRF-Aware VPDN Tunnels* feature module, located at the following URL:

http://www.cisco.com/en/US/products/ps6566/products_feature_guides_list.html

Configuration Examples

This section provides the following configuration examples:

- [Configuration Example for Tunnel VRF, page 27-4](#)
- [Configuration Examples for VRF-Aware VPDN Tunnels, page 27-5](#)

Configuration Example for Tunnel VRF

The following example shows how to enable the Tunnel VRF feature by specifying the **tunnel vrf** command after the **tunnel destination** command:

```
interface Tunnel 0
  ip vrf forwarding cust 1
  ip address 10.2.0.2 255.255.255.252
  ip pim sparse-dense-mode
  tunnel source Loopback1
```

```
tunnel destination 10.16.3.1
tunnel vrf cust2
```

Configuration Examples for VRF-Aware VPDN Tunnels

The following example shows how to enable the VRF-Aware VPDN Tunnels feature. In the example, the **vpn** command associates the IP address 172.16.1.9 with the VRF named vrf-second, which is applied to the VPDN group named group1.

```
vpdn-group group1
  request-dialin
    protocol l2tp
!
  vpn vrf vrf-second
  source-ip 172.16.1.9
  initiate-to ip 172.16.1.1
```

The following example also enables VRF-aware VPDN tunnels and associates the VRF named vpn1 with the IP address 192.64.1.4.

```
vpdn-group Test
  accept-dialin
    protocol l2tp
    virtual-template 1
  terminate-from hostname lac
  vpn vrf vpn1
  l2tp tunnel receive-window 100
  source-ip 192.64.1.4
  initiate-to ip 192.64.1.1
```

