



MPLS Virtual Private Networks (VPNs)

Feature History

Release	Modification
12.0(5)T	This feature was introduced.
12.0(21)ST	This feature was implemented on the Cisco 10720 Internet router and integrated into Cisco IOS Release 12.0(21)ST.
12.0(22)S	This feature was implemented on the Cisco 12000 series Internet Router on the following line cards: the 6E3-SMB and 12E3-SMB line cards, the 6-port channelized T3 (6CT3-SMB) line card, the OC-192c/STM-64c Packet-over-SONET (POS) line card, and the Quad OC-48c STM-16c POS line card and integrated into Cisco IOS Release 12.0(22)S.
12.0(23)S	This feature was integrated into Cisco IOS Release 12.0(23)S. The ip route static inter-vrf command was introduced.
12.2(13)T	This feature was implemented on the Cisco 7200 and Cisco 7500 series routers and integrated into Cisco IOS Release 12.2(13)T. Support was added for the ip route static inter-vrf command.

This document describes the Multiprotocol Label Switching (MPLS) Virtual Private Network (VPN) feature and includes the following sections:

- [Feature Overview, page 1](#)
- [Supported Platforms, page 7](#)
- [Supported Standards, MIBs and RFCs, page 8](#)
- [Prerequisites, page 9](#)
- [Configuration Tasks, page 9](#)
- [Configuration Examples, page 12](#)
- [Command Reference, page 14](#)

Feature Overview

The IP Virtual Private Network (VPN) feature for Multiprotocol Label Switching (MPLS) allows a Cisco IOS network to deploy scalable IPv4 Layer 3 VPN backbone services. An IP VPN is the foundation companies use for deploying or administering value-added services including applications and data hosting network commerce, and telephony services to business customers. In private local area

networks (LANs), IP-based intranets have fundamentally changed the way companies conduct their business. Companies are moving their business applications to their intranets to extend over a wide area network (WAN). Companies are also embracing the needs of their customers, suppliers, and partners by using extranets (an intranet that encompasses multiple businesses). With extranets, companies reduce business process costs by facilitating supply-chain automation, electronic data interchange (EDI), and other forms of network commerce. To take advantage of this business opportunity, service providers must have an IP VPN infrastructure that delivers private network services to businesses over a public infrastructure.

IP Virtual Private Networks

To effectively implement an IP VPN in your facility, ensure that your IP VPN meets the following basic requirements:

Privacy—All IP VPNs offer privacy over a shared (public) network infrastructure. Most companies use an encrypted tunnel. This is only one of several ways to provide network and data privacy.

Scalability—For proper service delivery, VPNs must scale to serve hundreds of thousands of sites and users. Besides being a managed service, VPNs are also a management tool for service providers to control access to services. One example is Closed User Groups for data and voice services.

Flexibility—IP VPNs must handle the any-to-any traffic patterns characteristic of corporate intranets and extranets, in which data no longer flows to and from a central location. VPNs must also have the inherent flexibility to add new sites quickly, connect users over different media, and meet the increasingly sophisticated transport and bandwidth requirements of new intranet applications.

Predictable Performance—Performance needs vary widely requiring different classes of service, but the common requirement is that the performance is predictable. Examples of the ranges of performance requirements include:

- Remote access for mobile users—Require widespread connectivity
- Branch offices—Require a sustained performance level because of the interactive nature of the intranet application in a branch office
- Video conferencing—Require specific performance characteristics

MPLS Virtual Private Networks

MPLS VPNs allow service providers to deploy scalable VPNs and build the foundation to deliver value-added services, including:

Connectionless Service—A significant technical advantage of MPLS VPNs is that they are connectionless. The Internet owes its success to its basic technology, TCP/IP. TCP/IP is built on packet-based, connectionless network paradigm. This means that no prior action is necessary to establish communication between hosts, making it easy for two parties to communicate. To establish privacy in a connectionless IP environment, current VPN solutions impose a connection-oriented, point-to-point overlay on the network. Even if it runs over a connectionless network, a VPN cannot take advantage of the ease of connectivity and multiple services available in connectionless networks. When you create a connectionless VPN, you do not need tunnels and encryption for network privacy, thus eliminating significant complexity.

Centralized Service—Building VPNs in Layer 3 allows delivery of targeted services to a group of users represented by a VPN. A VPN must give service providers more than a mechanism for privately connecting users to intranet services. It must also provide a way to flexibly deliver value-added services

to targeted customers. Scalability is critical, because customers want to use services privately in their intranets and extranets. Because MPLS VPNs are seen as private intranets, you may use new IP services such as:

- Multicast
- Quality of service (QoS)
- Telephony support within a VPN
- Centralized services including content and web hosting to a VPN

You can customize several combinations of specialized services for individual customers. For example, a service that combines IP multicast with a low-latency service class enables video conferencing within an intranet.

Scalability—If you create a VPN using connection-oriented, point-to-point overlays, Frame Relay, or ATM virtual connections (VCs), the VPN's key deficiency is scalability. Specifically, connection-oriented VPNs without fully meshed connections between customer sites are not optimal. MPLS-based VPNs instead use the peer model and Layer 3 connectionless architecture to leverage a highly scalable VPN solution. The peer model requires a customer site to peer with only one provider edge (PE) router as opposed to all other CPE or customer edge (CE) routers that are members of the VPN. The connectionless architecture allows the creation of VPNs in Layer 3, eliminating the need for tunnels or VCs.

Other scalability issues of MPLS VPNs are due to the partitioning of VPN routes between PE routers and the further partitioning of VPN and IGP routes between PE routers and provider (P) routers in a core network.

- PE routers must maintain VPN routes for those VPNs who are members.
- P routers do not maintain any VPN routes.

This increases the scalability of the provider's core and ensures that no one device is a scalability bottleneck.

Security—MPLS VPNs offer the same level of security as connection-oriented VPNs. Packets from one VPN do not inadvertently go to another VPN.

Security is provided in the following areas:

- At the edge of a provider network, ensuring packets received from a customer are placed on the correct VPN.
- At the backbone, VPN traffic is kept separate. Malicious spoofing (an attempt to gain access to a PE router) is nearly impossible because the packets received from customers are IP packets. These IP packets must be received on a particular interface or subinterface to be uniquely identified with a VPN label.

Easy to Create—To take full advantage of VPNs, it must be easy for customers to create new VPNs and user communities. Because MPLS VPNs are connectionless, no specific point-to-point connection maps or topologies are required. You can add sites to intranets and extranets and form closed user groups. When you manage VPNs in this manner, it enables membership of any given site in multiple VPNs, maximizing flexibility in building intranets and extranets.

Flexible Addressing—To make a VPN service more accessible, customers of a service provider can design their own addressing plan, independent of addressing plans for other service provider customers. Many customers use private address spaces, as defined in RFC 1918, and do not want to invest the time and expense of converting to public IP addresses to enable intranet connectivity. MPLS VPNs allow customers to continue to use their present address spaces without network address translation (NAT) by

providing a public and private view of the address. A NAT is required only if two VPNs with overlapping address spaces want to communicate. This enables customers to use their own unregistered private addresses, and communicate freely across a public IP network.

Integrated Class of Service (CoS) Support—CoS is an important requirement for many IP VPN customers. It provides the ability to address two fundamental VPN requirements:

- Predictable performance and policy implementation
- Support for multiple levels of service in a MPLS VPN

Network traffic is classified and labeled at the edge of the network before traffic is aggregated according to policies defined by subscribers and implemented by the provider and transported across the provider core. Traffic at the edge and core of the network can then be differentiated into different classes by drop probability or delay.

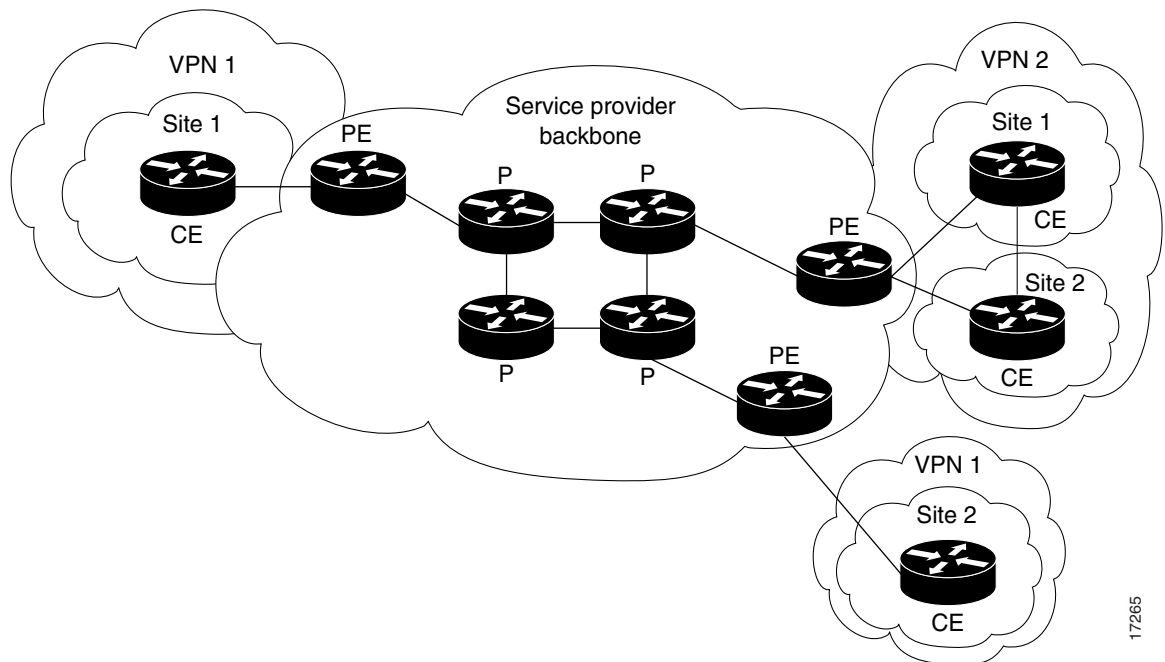
Straightforward Migration—For service providers to quickly deploy VPN services, use a straightforward migration path. MPLS VPNs are unique because you can build them over multiple network architectures, including IP, ATM, Frame Relay, and hybrid networks.

Migration for the end customer is simplified because there is no requirement to support MPLS on the customer edge (CE) router and no modifications are required to a customer's intranet.

For a list of platforms supported by MPLS VPNs, see the [“Supported Platforms” section on page 7](#).

[Figure 1](#) shows an example of a VPN with a service provider (P) backbone network, service provider edge routers (PE), and customer edge routers (CE).

Figure 1 VPNs with a Service Provider Backbone

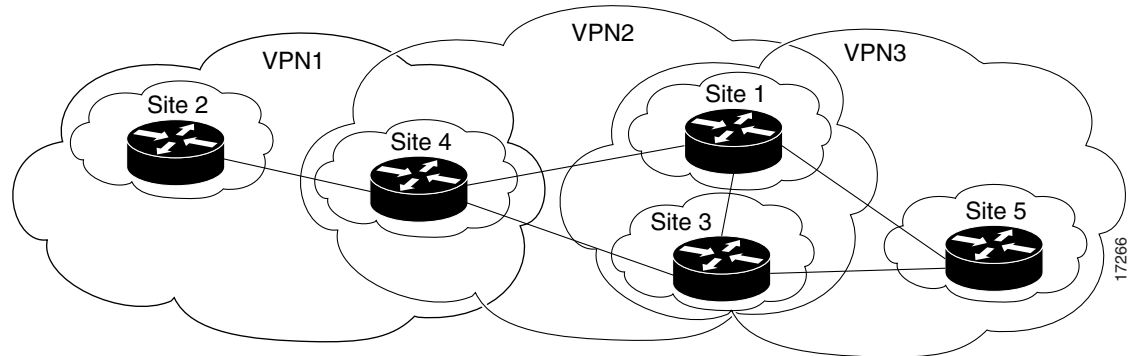


A VPN contains customer devices attached to the CE routers. These customer devices use VPNs to exchange information between devices. Only the PE routers are aware of the VPNs.

[Figure 2](#) shows five customer sites communicating within three VPNs. The VPNs can communicate with the following sites:

- VPN1—sites 2 and 4
- VPN2—sites 1, 3, and 4
- VPN3—sites 1, 3, and 5

Figure 2 Customer Sites within VPNs



VPN Operation

Each VPN is associated with one or more VPN routing/forwarding instances (VRFs). A VRF defines the VPN membership of a customer site attached to a PE router. A VRF consists of an IP routing table, a derived Cisco Express Forwarding (CEF) table, a set of interfaces that use the forwarding table, and a set of rules and routing protocol parameters that control the information that is included into the routing table.

A one-to-one relationship does not necessarily exist between customer sites and VPNs. A given site can be a member of multiple VPNs, as shown in [Figure 2](#). However, a site can only associate with only one VRF. A customer site's VRF contains all the routes available to the site from the VPNs of which it is a member.

Packet forwarding information is stored in the IP routing table and the CEF table for each VRF. A separate set of routing and CEF tables is maintained for each VRF. These tables prevent information from being forwarded outside a VPN, and also prevent packets that are outside a VPN from being forwarded to a router within the VPN.

VPN Route Target Communities

The distribution of VPN routing information is controlled through the use of VPN route target communities, implemented by Border Gateway Protocol (BGP) extended communities. Distribution of VPN routing information works as follows:

1. When a VPN route learned from a CE router is injected into BGP, a list of VPN route target extended community attributes is associated with it. Typically the list of route target community values is set from an export list of route targets associated with the VRF from which the route was learned.
2. An import list of route target extended communities is associated with each VRF. The import list defines route target extended community attributes a route must have for the route to be imported into the VRF. For example, if the import list for a particular VRF includes route target communities A, B, and C, then any VPN route that carries any of those route target extended communities—A, B, or C—is imported into the VRF.

BGP Distribution of VPN Routing Information

A service provider edge (PE) router can learn an IP prefix from a customer edge (CE) router by static configuration, through a BGP session with the CE router, or through the routing information protocol (RIP) exchange with the CE router. The IP prefix is a member of the IPv4 address family. After it learns the IP prefix, the PE converts it into a VPN-IPv4 prefix by combining it with an 8-byte route distinguisher (RD). The generated prefix is a member of the VPN-IPv4 address family. It serves to uniquely identify the customer address, even if the customer site is using globally nonunique (unregistered private) IP addresses.

The route distinguisher used to generate the VPN-IPv4 prefix is specified by a configuration command associated with the VRF on the PE router.

BGP distributes reachability information for VPN-IPv4 prefixes for each VPN. BGP communication takes place at two levels: within IP domains, known as an autonomous systems (interior BGP or IBGP) and between autonomous systems (external BGP or EBGP). PE-PE or PE-RR (route reflector) sessions are IBGP sessions, and PE-CE sessions are EBGP sessions.

BGP propagates reachability information for VPN-IPv4 prefixes among PE routers by means of the BGP multiprotocol extensions (refer to RFC 2283, Multiprotocol Extensions for BGP-4) which define support for address families other than IPv4. It does this in a way that ensures that the routes for a given VPN are learned only by other members of that VPN, enabling members of the VPN to communicate with each other.

MPLS Forwarding

Based on routing information stored in the VRF IP routing table and VRF CEF table, packets are forwarded to their destination using MPLS.

A PE router binds a label to each customer prefix learned from a CE router and includes the label in the network reachability information for the prefix that it advertises to other PE routers. When a PE router forwards a packet received from a CE router across the provider network, it labels the packet with the label learned from the destination PE router. When the destination PE router receives the labeled packet, it pops the label and uses it to direct the packet to the correct CE router. Label forwarding across the provider backbone is based on either dynamic label switching or traffic engineered paths. A customer data packet carries two levels of labels when traversing the backbone:

1. Top label directs the packet to the correct PE router.
2. Second label indicates how that PE router should forward the packet to the CE router.

Benefits

This section describes the benefits of VPNs in general and MPLS VPNs in particular.

IP VPNs are attractive because they have the following benefits:

- Reduce the cost of connecting branch offices, telecommuters, and mobile users to a corporate intranet, which operate over the public infrastructure of the Internet
- Are more cost-effective than private WANs constructed with leased lines

However, conventional VPNs do not scale well. They are based on creating and maintaining a full mesh of tunnels or permanent virtual circuits among all sites belonging to a particular VPN, using:

- IPSec
- Layer 2 tunneling protocol (L2TP)

- Layer 2 forwarding (L2F) protocol
- Generic routing encapsulation (GRE)
- Frame Relay
- ATM protocols

The overhead required to provision and manage these connection-based schemes cannot be supported in a provider network that must support hundreds or thousands of VPNs, each with tens or hundreds or thousands of sites and thousands or tens of thousands of routes.

MPLS VPNs, which are created in Layer 3, are connectionless, and therefore substantially more scalable and easier to build and manage than conventional VPNs. In addition, you can add value-added services, such as application and data hosting, network commerce, and telephony services to a particular MPLS VPN because the service provider's backbone recognizes each MPLS VPN as a separate, connectionless IP network.

MPLS VPNs offer the following benefits:

- A platform for rapid deployment of additional value-added IP services, including intranets, extranets, voice, multimedia, and network commerce
- Privacy and security equal to that provided by Layer-2 VPNs by limiting the distribution of a VPN's routes to only those routers that are members of the VPN Seamless integration with customer intranets
- Increased scalability over current VPN implementations, with thousands of sites per VPN and hundreds of thousands of VPNs per service provider IP class of service (CoS), with support for multiple classes of service and priorities within VPNs, as well as between VPNs
- Management of VPN membership and provisioning of new VPNs for rapid deployment
- Scalable any-to-any connectivity for extended intranets and extranets that encompass multiple businesses

Related Features and Technologies

VPNs may be used with the Class of Service (CoS) feature for MPLS.

Related Documents

- [MPLS Class of Service\(CoS\)](#), Cisco IOS Release 12.0(5)T feature module
- [Cisco IOS Release 12.0 Network Protocols Command Reference](#), Part 1

Supported Platforms

- Cisco 7200 series routers
- Cisco 7500 series routers
- Cisco 12000 series routers (on supported Cisco IOS S releases only)
- Cisco 10720 Internet router (on supported Cisco IOS S and ST releases only)

Determining Platform Support Through Cisco Feature Navigator

Cisco IOS software is packaged in feature sets that are supported on specific platforms. To obtain updated information about platform support for this feature, access Cisco Feature Navigator. Cisco Feature Navigator dynamically updates the list of supported platforms as new platform support is added for the feature.

Cisco Feature Navigator is a web-based tool that enables you to determine which Cisco IOS software images support a specific set of features and which features are supported in a specific Cisco IOS image. You can search by feature or release. In the release section, you can compare releases side by side to display both the features unique to each software release and the features that releases have in common.

To access Cisco Feature Navigator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

Cisco Feature Navigator is updated regularly when major Cisco IOS software releases and technology releases occur. For the most current information, go to the Cisco Feature Navigator home page at the following URL:

<http://www.cisco.com/go/fn>

Availability of Cisco IOS Software Images

Platform support for particular Cisco IOS software releases is dependent on the availability of the software images for those platforms. Software images for some platforms may be deferred, delayed, or changed without prior notice. For updated information about platform support and availability of software images for each Cisco IOS software release, refer to the online release notes or, if supported, Cisco Feature Navigator.

Supported Standards, MIBs and RFCs

Standards

No new or modified standards are supported by this feature.

MIBs

No new or modified MIBs are supported 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://tools.cisco.com/ITDIT/MIBS/servlet/index>

If Cisco MIB Locator does not support the MIB information that you need, you can also obtain a list of supported MIBs and download MIBs from the Cisco MIBs page at the following URL:

<http://www.cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml>

To access Cisco MIB Locator, you must have an account on Cisco.com. If you have forgotten or lost your account information, send a blank e-mail to cco-locksmith@cisco.com. An automatic check will verify that your e-mail address is registered with Cisco.com. If the check is successful, account details with a new random password will be e-mailed to you. Qualified users can establish an account on Cisco.com by following the directions found at this URL:

<http://www.cisco.com/register>

RFCs

- RFC 1163, *A Border Gateway Protocol*
- RFC 1164, *Application of the Border Gateway Protocol in the Internet*
- RFC 2283, *Multiprotocol Extensions for BGP-4*
- RFC 2547, *BGP/MPLS VPNs*

Prerequisites

Your network must be running the following Cisco IOS services before you configure VPN operation:

- MPLS in provider backbone routers, or GRE tunnel connectivity among all provider edge (PE) routers
- MPLS with VPN code in provider routers with VPN edge service (PE) routers
- BGP in all routers providing a VPN service
- CEF switching in every MPLS-enabled router
- CoS feature (optional)

Configuration Tasks

See the following sections to configure and verify VPNs:

- [Defining VPNs](#) (required)
- [Configuring BGP PE to PE or PE to CE Routing Sessions](#) (required)
- [Configuring RIP PE to CE Routing Sessions](#) (required)
- [Configuring Static Route PE to CE Routing Sessions](#) (required)
- [Verifying VPN Operation](#) (optional)

Defining VPNs

To define VPN routing instances, use the following commands beginning in global configuration mode on the PE router:

	Command	Purpose
Step 1	Router(config)# ip vrf <i>vrf-name</i>	Enters VRF configuration mode and define the VPN routing instance by assigning a VRF name.
Step 2	Router(config-vrf)# rd <i>route-distinguisher</i>	Creates routing and forwarding tables.
Step 3	Router(config-vrf)# route-target { import export both } <i>route-target-ext-community</i>	Creates a list of import and/or export route target communities for the specified VRF.
Step 4	Router(config-vrf)# import map <i>route-map</i>	(Optional) Associates the specified route map with the VRF.
Step 5	Router(config-if)# ip vrf forwarding <i>vrf-name</i>	Associates a VRF with an interface or subinterface.

Configuring BGP PE to PE or PE to CE Routing Sessions

To configure BGP PE to PE or PE to CE routing sessions in a provider network, use the following commands beginning in global configuration mode on the PE router:

	Command	Purpose
Step 1	Router(config)# router bgp <i>autonomous-system</i>	Configures the IBGP or EGBP routing process with the autonomous system number passed along to other IBGP or EGBP routers.
Step 2	Router(config-router)# neighbor { <i>ip-address</i> <i>peer-group-name</i> } remote-as <i>number</i>	Specifies a neighbor's IP address or IBGP/EBGP peer group identifying it to the local autonomous system.
Step 3	Router(config-router)# neighbor <i>ip-address</i> activate	Activates the advertisement of the IPv4 address family.

Configuring RIP PE to CE Routing Sessions

To configure RIP PE to CE routing sessions, use the following commands beginning in global configuration mode on the PE router:

	Command	Purpose
Step 1	Router(config)# router rip	Enables RIP.
Step 2	Router(config-router)# address-family ipv4 [unicast] vrf <i>vrf-name</i>	Defines RIP parameters for PE to CE routing sessions. The default is Off for auto-summary and synchronization in the VRF address-family submenu.
Step 3	Router(config-router)# network <i>prefix</i>	Enables RIP on the PE to CE link.

Configuring Static Route PE to CE Routing Sessions

To configure static route PE to CE routing sessions, use the following commands beginning in global configuration mode on the PE router:

	Command	Purpose
Step 1	Router(config)# ip route vrf <i>vrf-name</i>	Defines static route parameters for every PE to CE session.
Step 2	Router(config-router)# address-family ipv4 [unicast] vrf <i>vrf-name</i>	Defines static route parameters for every BGP PE to CE routing session. The default is Off for auto-summary and synchronization in the VRF address-family submode.
Step 3	Router(config-router-af)# redistribute static	Redistributes VRF static routes into the VRF BGP table.
Step 4	Router(config-router-af)# redistribute static connected	Redistributes directly connected networks into the VRF BGP table.
Step 5	Router(config-router-af)# exit-address-family	Exits address family configuration mode.
Step 6	Router(config-router)# end	(Optional) Exits to privileged EXEC mode.

Verifying VPN Operation

To verify VPN operation, use the following commands in privileged EXEC mode:

	Command	Purpose
Step 1	Router# show ip vrf	Displays the set of defined VRFs and interfaces.
Step 2	Router# show ip vrf [{ brief detail interfaces }] <i>vrf-name</i>	Displays information about defined VRFs and associated interfaces.
Step 3	Router# show ip route vrf <i>vrf-name</i>	Displays the IP routing table for a VRF.
Step 4	Router# show ip protocols vrf <i>vrf-name</i>	Displays the routing protocol information for a VRF.
Step 5	Router# show ip cef vrf <i>vrf-name</i>	Displays the CEF forwarding table associated with a VRF.
Step 6	Router# show ip interface <i>interface-number</i>	Displays the VRF table associated with an interface.
Step 7	Router# show ip bgp vpnv4 all [labels]	Displays information about all BGP routes.
Step 8	Router# show mpls forwarding vrf <i>vrf-name</i> [<i>prefix mask/length</i>] [detail]	Displays label forwarding entries that correspond to VRF routes advertised by this router.

Configuration Examples

This section provides a sample configuration file from a PE router.

```

ip cef distributed          ! CEF switching is pre-requisite for label Switching
frame-relay switching
!
ip vrf vrf1                ! Define VPN Routing instance vrf1
rd 100:1
route-target both 100:1   ! Configure import and export route-targets for vrf1
!
ip vrf vrf2                ! Define VPN Routing instance vrf2
rd 100:2
route-target both 100:2   ! Configure import and export route-targets for vrf2
route-target import 100:1 ! Configure an additional import route-target for vrf2
import map vrf2_import    ! Configure import route-map for vrf2
!
interface lo0
ip address 10.13.0.13 255.255.255.255
!
interface atm9/0/0        ! Backbone link to another Provider router
!
interface atm9/0/0.1 tag-switching
ip unnumbered loopback0
no ip directed-broadcast
mpls atm vpi 2-5
mpls ip

interface atm5/0
no ip address
no ip directed-broadcast
atm clock INTERNAL
no atm ilmi-keepalive

interface Ethernet1/0
ip address 3.3.3.5 255.255.0.0
no ip directed-broadcast
no ip mroute-cache
no keepalive

interface Ethernet5/0/1          ! Set up Ethernet interface
ip vrf forwarding vrf1          ! as VRF link to a CE router
ip address 10.20.0.13 255.255.255.0
!
interface hssi 10/1/0
hssi internal-clock
encaps fr
frame-relay intf-type dce
frame-relay lmi-type ansi
!
interface hssi 10/1/0.16 point-to-point
ip vrf forwarding vrf2
ip address 10.20.1.13 255.255.255.0
frame-relay interface-dlci 16    ! Set up Frame Relay PVC
!                                ! subinterface as link to another
!                                ! CE router
!
router bgp 1                      ! Configure BGP sessions
no synchronization
no bgp default ipv4-activate     ! Deactivate default IPv4 advertisements
neighbor 10.15.0.15 remote-as 1  ! Define IBGP session with another PE
neighbor 10.15.0.15 update-source lo0
!

```

```
address-family vpnv4 unicast          ! Activate PE exchange of VPNv4 NLRI
neighbor 10.15.0.15 activate
exit-address-family
!
address-family ipv4 unicast vrf vrf1  ! Define BGP PE-CE session for vrf1
redistribute static
redistribute connected
neighbor 10.20.0.60 remote-as 65535
neighbor 10.20.0.60 activate
no auto-summary
exit-address-family
!
address-family ipv4 unicast vrf vrf2  ! Define BGP PE-CE session for vrf2
redistribute static
redistribute connected
neighbor 10.20.1.11 remote-as 65535
neighbor 10.20.1.11 update-source h10/1/0.16
neighbor 10.20.1.11 activate
no auto-summary
exit-address-family
!
! Define a VRF static route
ip route vrf vrf1 12.0.0.0 255.0.0.0 e5/0/1 10.20.0.60
!
route-map vrf2_import permit 10 ! Define import route-map for vrf2.
...
```

Command Reference

This section documents new and modified commands. All other commands used with this feature are documented in the Cisco IOS Release 12.0 command references.

- [address-family](#)
- [clear ip route vrf](#)
- [debug ip bgp](#)
- [exit-address-family](#)
- [import map](#)
- [ip route static inter-vrf](#)
- [ip route vrf](#)
- [ip vrf](#)
- [ip vrf forwarding](#)
- [neighbor activate](#)
- [rd](#)
- [route-target](#)
- [show ip bgp vpnv4](#)
- [show ip cef vrf](#)
- [show ip protocols vrf](#)
- [show ip route vrf](#)
- [show ip vrf](#)
- [show tag-switching forwarding vrf](#)

address-family

To enter the address family submode for configuring routing protocols, such as Border Gateway Protocol (BGP), Routing Information Protocol (RIP) and static routing, use the **address-family** command in router configuration mode. To disable the address family submode for configuring routing protocols, use the **no** form of this command.

VPN-IPv4 unicast

```
address-family vpnv4 [unicast]
```

```
no address-family vpnv4 [unicast]
```

IPv4 unicast

```
address-family ipv4 [unicast]
```

```
no address-family ipv4 [unicast]
```

IPv4 unicast with CE router

```
address-family ipv4 [unicast] vrf vrf-name
```

```
no address-family ipv4 [unicast] vrf vrf-name
```

Syntax Description

ipv4	Configures sessions that carry standard IPv4 address prefixes.
vpnv4	Configures sessions that carry customer VPN-IPv4 prefixes, each of which has been made globally unique by adding an 8-byte route distinguisher.
unicast	(Optional) Specifies unicast prefixes.
vrf vrf-name	Specifies the name of a VPN routing/forwarding instance (VRF) to associate with submode commands.

Defaults

Routing information for address family IPv4 is advertised by default when you configure a BGP session using the **neighbor...remote-as** command unless you execute the **no bgp default ipv4-activate** command.

Command Modes

Router configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.

Usage Guidelines

Using the **address-family** command puts you in address family configuration submode (prompt: `(config-router-af)#`). Within this submode, you can configure address-family specific parameters for routing protocols, such as BGP, that can accommodate multiple Layer 3 address families.

To leave address family configuration submode and return to router configuration mode, type **exit-address-family**, or simply **exit**.

Examples

The following example shows how to put the router into address family configuration submode for the VPNv4 address family. Within the submode, you can configure advertisement of NLRI for the VPNv4 address family using **neighbor activate** and other related commands:

```
Router(config)# router bgp 100

Router(config-router)# address-family vpnv4

Router(config-router-af)#
```

The following example shows how to put the router into address family configuration submode for the IPv4 address family. Use this form of the command, which specifies a VRF, only to configure routing exchanges between provider edge (PE) and customer edge (CE) devices. This address-family command causes subsequent commands entered in the submode to be executed in the context of VRF vrf2.

```
Router(config)# router bgp 100

Router(config-router)# address-family ipv4 unicast vrf vrf2

Router(config-router-af)#
```

Within the submode, you can use **neighbor activate** and other related commands to accomplish the following:

- Configure advertisement of IPv4 NLRI between the PE and CE routers.
- Configure translation of the IPv4 NLRI (that is, translate IPv4 into VPNv4 for NLRI received from the CE, and translate VPNv4 into IPv4 for NLRI to be sent from the PE to the CE).
- Enter the routing parameters that apply to this VRF.

Related Commands

Command	Description
exit-address-family	Exits from the address family submode
neighbor activate	Enables the exchange of information with a BGP neighboring router.

clear ip route vrf

To remove routes from the Virtual Private Network (VPN) routing/forwarding (VRF) routing table, use the **clear ip route vrf** command in privileged EXEC mode.

```
clear ip route vrf vrf-name [* | network [mask]]
```

Syntax Description		
<i>vrf-name</i>		Name of the VPN routing/forwarding instance (VRF) for the static route.
*		Deletes all routes for a given VRF.
<i>network</i>		Destination to be removed, in dotted-decimal format.
<i>mask</i>		(Optional) Mask for the specified network destination, in dotted-decimal format.

Defaults No default behavior or values.

Command Modes Privileged EXEC

Command History	Release	Modifications
	12.0(5)T	This command was introduced.
	12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
	12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
	12.0(23)S	This command was integrated into Cisco IOS 12.0(23)S.
	12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.

Usage Guidelines Use this command to clear routes from the routing table. Use the asterisk (*) to delete all routes from the forwarding table for a specified VRF, or enter the address and mask of a particular network to delete the route to that network.

Examples The following command shows how to remove the route to the network 10.13.0.0 in the vpn1 routing table:

```
Router# clear ip route vrf vpn1 10.13.0.0
```

Related Commands	Command	Description
	show ip route vrf	Displays the IP routing table associated with a VRF.

debug ip bgp

To display information related to processing Border Gateway Protocol (BGP) routing, use the **debug ip bgp** command in privileged EXEC mode. To disable the display of BGP information, use the **no** form of this command.

debug ip bgp [*A.B.C.D.* | **dampening** | **events** | **in** | **keepalives** | **out** | **updates** | **vpn4**]

no debug ip bgp [*A.B.C.D.* | **dampening** | **events** | **in** | **keepalives** | **out** | **updates** | **vpn4**]

Syntax Description

<i>A.B.C.D.</i>	(Optional) Displays the BGP neighbor IP address.
dampening	(Optional) Displays BGP dampening.
events	(Optional) Displays BGP events.
in	(Optional) BGP inbound information.
keepalives	(Optional) Displays BGP keepalives.
out	(Optional) Displays BGP outbound information.
updates	(Optional) Displays BGP updates.
vpn4	(Optional) Displays VPNv4 NLRI information.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.

Examples

The following example displays the output from this command:

```
Router# debug ip bgp vpn4

03:47:14:vpn:bgp_vpnv4_bnetinit:100:2:58.0.0.0/8
03:47:14:vpn:bnettable add:100:2:58.0.0.0 / 8
03:47:14:vpn:bestpath_hook route_tag_change for vpn2:58.0.0.0/255.0.0.0(ok)
03:47:14:vpn:bgp_vpnv4_bnetinit:100:2:57.0.0.0/8
03:47:14:vpn:bnettable add:100:2:57.0.0.0 / 8
03:47:14:vpn:bestpath_hook route_tag_change for vpn2:57.0.0.0/255.0.0.0(ok)
03:47:14:vpn:bgp_vpnv4_bnetinit:100:2:14.0.0.0/8
03:47:14:vpn:bnettable add:100:2:14.0.0.0 / 8
03:47:14:vpn:bestpath_hook route_tag_chacle ip bgp *nge for vpn2:14.0.0.0/255.0.0.0(ok)
```

exit-address-family

To exit from the address family submode, use the **exit-address-family** command in address family submode.

exit-address-family

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Command Modes Address family submode

Command History	Release	Modification
	12.0(5)T	This command was introduced.
	12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
	12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
	12.0(23)S	This command was integrated into Cisco IOS 12.0(23)S.
	12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.

Usage Guidelines This command can be abbreviated to **exit**.

Examples The following example shows how to exit the address-family command submode:

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

Related Commands	Command	Description
	address-family	Enters the address family submode used to configure routing protocols.

import map

To configure an import route map for a Virtual Private Network (VPN) routing/forwarding instance (VRF), use the **import map** command in VRF submode.

import map *route-map*

Syntax Description	<i>route-map</i>	Specifies the route map to be used as an import route map for the VRF.
---------------------------	------------------	--

Defaults A VRF has no import route map unless one is configured using the **import map** command.

Command Modes VRF submode

Command History	Command	Modification
	12.0(5)T	This command was introduced.
	12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
	12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
	12.0(23)S	This command was integrated into Cisco IOS 12.0(23)S.
	12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.

Usage Guidelines Use an **import map** command when an application requires finer control over the routes imported into a VRF than provided by the import and export extended communities configured for the importing and exporting VRF.

The **import-map** command associates a route map with the specified VRF. You can filter routes that are eligible for import into a VRF, based on the route target extended community attributes of the route, through the use of a route map. The route map might deny access to selected routes from a community that is on the import list.

Examples The following example shows how to configure an import route map for a VRF:

```
Router(config)# ip vrf vrf_blue
Router(config-vrf)# import map blue_import_map
```

Related Commands	Command	Description
	ip vrf	Enters VRF configuration mode.
	route-target	Configures import and export extended community attributes for the VRF.
	show ip vrf	Displays information about a VRF or all VRFs.

ip route static inter-vrf

To allow static routes to point to Virtual Private Network (VPN) routing/forwarding (VRF) interfaces in VRFs other than those to which the static route belongs, use the **ip route static inter-vrf** command in global configuration mode. To prevent static routes from pointing to VRF interfaces in VRFs to which they do not belong, use the **no** form of this command.

ip route static inter-vrf

no ip route static inter-vrf

Syntax Description This command has no arguments or keywords.

Defaults By default, static routes are allowed to point to VRF interfaces in any VRF.

Command Modes Global configuration

Command History	Release	Modification
	12.0(23)S	This command was introduced.
	12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.

Usage Guidelines The **ip route static inter-vrf** command is turned on by default. The **no ip route static inter-vrf** command causes the respective routing table (global or VRF) to reject the installation of static routes if the outgoing interface belongs to a different VRF than the static route being configured. This prevents security problems that can occur when static routes that point to a VRF interface in a different VRF are misconfigured. You are notified when a static route is rejected, then you can reconfigure it.

For example, a static route is defined on a provider edge (PE) router to forward Internet traffic to a customer on the interface pos1/0, as follows:

```
Router(config)# ip route 10.1.1.1 255.255.255.255 pos 1/0
```

Mistakenly, the same route is configured with the next-hop as the VRF interface pos10/0:

```
Router(config)# ip route 10.1.1.1 255.255.255.255 pos 10/0
```

By default, Cisco IOS accepts the command and starts forwarding the traffic to both pos1/0 (Internet) and pos10/0 (VPN) interfaces.

If the static route is already configured that points to a VRF other than the one to which the route belongs when you issue the **no ip route static inter-vrf** command, the offending route is uninstalled from the routing table and a message similar to the following is sent to the console:

```
01:00:06: %IPRT-3-STATICROUTESACROSSVRF: Un-installing static route x.x.x.x/32 from global routing table with outgoing interface intx/x
```

If you enter the **no ip route static inter-vrf** command before a static route is configured that points to a VRF interface in a different VRF, the static route is not installed in the routing table and a message is sent to the console.

In the following example, configuring the **no ip route static inter-vrf** command prevents traffic from following an unwanted path. A VRF static route points to a global interface or any other VRF interface as shown in the following **ip route vrf** commands:

- Interface ser1/0.0 is a global interface:

```
Router(config)# ip route vrf vpn1 10.10.1.1 255.255.255.255 ser1/0.0
```

- Interface ser1/0.1 is in vpn2:

```
Router(config)# ip route vrf vpn1 10.10.1.1 255.255.255.255 ser1/0.1
```

With the **no ip route static inter-vrf** command configured, these static routes are not installed into the vpn1 routing table because the static routes point to an interface that is not in the same VRF.

If you require a VRF static route to point to a global interface, you can use the **global** keyword with the **ip route vrf** command:

```
Router(config)# ip route vrf vpn1 10.12.1.1 255.255.255.255 ser1/0.0 7.0.0.1 global
```

The **global** keyword allows the VRF static route to point to a global interface even when the **no ip route static inter-vrf** command is configured.

Examples

The following example shows how to prevent static routes that point to VRF interfaces in a different VRF:

```
Router(config)# no ip route static inter-vrf
```

Related Commands

Command	Description
ip route vrf	Establishes static routes for a VRF.

ip route vrf

To establish static routes for a Virtual Private Network (VPN) routing/forwarding instance (VRF), use the **ip route vrf** command in global configuration mode. To disable static routes, use the **no** form of this command.

```
ip route vrf vrf-name prefix mask [next-hop-address] [interface {interface-number}] [global]
[distance] [permanent] [tag tag]
```

```
no ip route vrf vrf-name prefix mask [next-hop-address] [interface {interface-number}] [global]
[distance] [permanent] [tag tag]
```

Syntax Description

<i>vrf-name</i>	Name of the VPN routing/forwarding instance (VRF) for the static route.
<i>prefix</i>	IP route prefix for the destination, in dotted-decimal format.
<i>mask</i>	Prefix mask for the destination, in dotted-decimal format.
<i>next-hop-address</i>	(Optional) IP address of the next hop (the forwarding router that can be used to reach that network).
<i>interface</i>	(Optional) Type of network interface to use: ATM, Ethernet, loopback, POS (packet over SONET), or null.
<i>interface-number</i>	Number identifying the network interface to use.
global	Specifies that the given next hop address is in the non-VRF routing table.
<i>distance</i>	(Optional) An administrative distance for this route.
permanent	(Optional) Specifies that this route will not be removed, even if the interface shuts down.
tag <i>tag</i>	(Optional) Label value that can be used for controlling redistribution of routes through route maps.

Defaults

No default behavior or values.

Command Modes

Global configuration

Command History

Release	Modifications
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.

Usage Guidelines

Use a static route when the Cisco IOS software cannot dynamically build a route to the destination.

If you specify an administrative distance when you set up a route, you are flagging a static route that can be overridden by dynamic information. For example, Interior Gateway Routing Protocol (IGRP)-derived routes have a default administrative distance of 100. To set a static route to be overridden by an IGRP dynamic route, specify an administrative distance greater than 100. Static routes each have a default administrative distance of 1.

Static routes that point to an interface are advertised through Routing Information Protocol (RIP), IGRP, and other dynamic routing protocols, regardless of whether the routes are redistributed into those routing protocols. That is, static routes configured by specifying an interface lose their static nature when installed into the routing table.

However, if you define a static route to an interface not defined in a network command, no dynamic routing protocols advertise the route unless a redistribute static command is specified for these protocols.

Examples

The following command shows how to reroute packets addressed to network 137.23.0.0 in VRF vpn3 to router 131.108.6.6:

```
Router(config)# ip route vrf vpn3 137.23.0.0 255.255.0.0 131.108.6.6
```

Related Commands

Command	Description
show ip route vrf	Displays the IP routing table associated with a VRF.

ip vrf

To configure a Virtual Private Network (VPN) routing/forwarding (VRF) routing table, use the **ip vrf** command in global configuration mode. To remove a VRF routing table, use the **no** form of this command.

ip vrf *vrf-name*

no ip vrf *vrf-name*

Syntax Description

<i>vrf-name</i>	Name assigned to a VRF.
-----------------	-------------------------

Defaults

No VRFs are defined. No import or export lists are associated with a VRF. No route maps are associated with a VRF.

Command Modes

Global configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.

Usage Guidelines

The **ip vrf** *vrf-name* command creates a VRF routing table and a CEF (forwarding) table, both named *vrf-name*. Associated with these tables is the default route distinguisher value *route-distinguisher*.

Examples

The following example shows how to import a route map to a VRF:

```
Router(config)# ip vrf vpn1

Router(config-vrf)# rd 100:2

Router(config-vrf)# route-target both 100:2

Router(config-vrf)# route-target import 100:1
```

Related Commands

Command	Description
ip vrf forwarding	Associates a VRF with an interface or subinterface.

ip vrf forwarding

To associate a Virtual Private Network (VPN) routing/forwarding instance (VRF) with an interface or subinterface, use the **ip vrf forwarding** command in interface configuration mode. To disassociate a VRF, use the **no** form of this command.

```
ip vrf forwarding vrf-name
```

```
no ip vrf forwarding vrf-name
```

Syntax Description

<i>vrf-name</i>	Name assigned to a VRF.
-----------------	-------------------------

Defaults

The default for an interface is the global routing table.

Command Modes

Interface configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.

Usage Guidelines

Use this command to associate an interface with a VRF. Executing this command on an interface removes the IP address. The IP address should be reconfigured.

Examples

The following example shows how to link a VRF to ATM interface 0/0:

```
Router(config)# interface atm0/0
```

```
Router(config-if)# ip vrf forwarding vpn1
```

Related Commands

Command	Description
ip vrf	Defines a VRF.
ip route vrf	Establishes static routes for a VRF.

neighbor activate

To enable the exchange of information with a Border Gateway Protocol (BGP) neighboring router, use the **neighbor activate** command in router configuration mode. To disable the exchange of an address with a neighboring router, use the **no** form of this command.

neighbor {*ip-address* | *peer-group-name*} **activate**

no neighbor {*ip-address* | *peer-group-name*} **activate**

Syntax Description

<i>ip-address</i>	IP address of the neighboring router.
<i>peer-group-name</i>	Name of BGP peer group.

Defaults

The exchange of addresses with neighbors is enabled by default for the Virtual Private Network (VPN) IPv4 address family. You can disable IPv4 address exchange using the general command **no default bgp ipv4 activate**, or you can disable it for a particular neighbor by using the **no** form of this command.

For all other address families, address exchange is disabled by default. You can explicitly activate the default command by using the appropriate address family submode.

Command Modes

Router configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.

Usage Guidelines

Use this command to enable or disable the exchange of addresses with a neighboring router.

Examples

The following example shows how to activate the exchange of the customer IP address 10.15.0.15 to a neighboring router.

```
Router(config)# router bgp 100

Router(config-router)# neighbor 10.15.0.15 remote-as 100

Router(config-router)# neighbor 10.15.0.15 update-source loopback0

Router(config-router)# address-family vpnv4 unicast

Router(config-router-af)# neighbor 10.15.0.15 activate

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

■ neighbor activate

Related Commands	Command	Description
	address-family	Enters the address family submode.
	exit-address-family	Exits the address family submode.

rd

To create routing and forwarding tables for a Virtual Private Network (VPN) routing/forwarding instance (VRF), use the **rd** command in VRF configuration submode.

rd *route-distinguisher*

Syntax Description	<i>route-distinguisher</i>	Adds an 8-byte value to an IPv4 prefix to create a VPN IPv4 prefix.
---------------------------	----------------------------	---

Defaults	There is no default. A route distinguisher (RD) must be configured for a VRF to be functional.
-----------------	--

Command Modes	VRF configuration submode
----------------------	---------------------------

Command History	Release	Modification
	12.0(5)T	This command was introduced.
	12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
	12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
	12.0(23)S	This command was integrated into Cisco IOS 12.0(23)S.
	12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.

Usage Guidelines	An RD creates routing and forwarding tables and specifies the default route distinguisher for a VPN. The RD is added to the beginning of the customer's IPv4 prefixes to change them into globally unique VPN-IPv4 prefixes.
-------------------------	--

An RD is either

- ASN-related—Composed of an autonomous system number and an arbitrary number.
- IP-address-related—Composed of an IP address and an arbitrary number.

You can enter an RD in either of these formats:

16-bit AS number: your 32-bit number

For example, 101:3

32-bit IP address: your 16-bit number

For example, 192.168.122.15:1

Examples

The following example shows how to configure a default RD for two VRFs. The example shows the use of both AS-related and IP address-related RDs:

```
Router(config)# ip vrf vrf_blue  
  
Router(config-vrf)# rd 100:3  
  
Router(config-vrf)# ip vrf vrf_red  
  
Router(config-vrf)# rd 173.13.0.12:200
```

Related Commands

Command	Description
rd	Enters VRF configuration mode.
show ip vrf	Displays information about a VRF.

route-target

To create a route-target extended community for a Virtual Private Network (VPN) routing/forwarding instance (VRF), use the **route-target** command in VRF configuration submode. To disable the configuration of a route-target community option, use the **no** form of this command.

```
route-target { import | export | both } route-target-ext-community
```

```
no route-target { import | export | both } route-target-ext-community
```

Syntax Description

import	Imports routing information from the target VPN extended community.
export	Exports routing information to the target VPN extended community.
both	Imports both import and export routing information to the target VPN extended community.
<i>route-target-ext-community</i>	Adds the route-target extended community attributes to the VRF's list of import, export, or both (import and export) route-target extended communities.

Defaults

A VRF has no route-target extended community attributes associated with it until the attributes are specified by the **route-target** command.

Command Modes

VRF configuration submode

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.

Usage Guidelines

The **route-target** command creates lists of import and export route target extended communities for the specified VRF. Execute the command one time for each target community. Learned routes that carry a specific route target extended community are imported into all VRFs configured with that extended community as an import route target. Routes learned from a VRF site (for example, by Border Gateway Protocol (BGP), Routing Information Protocol (RIP), or static route configuration) contain export route targets for extended communities configured for the VRF added as route attributes to control the VRFs into which the route is imported.

The route-target specifies a target VPN extended community. Like a route-distinguisher, an extended community is composed of either an autonomous system number and an arbitrary number, or an IP address and an arbitrary number. You can enter the numbers in either of these formats:

- *16-bit AS number: your 32-bit number*
For example, 101:3
- *32-bit IP address: your 16-bit number*
For example, 192.168.122.15:1

Examples

The following example shows how to configure route-target extended community attributes for a VRF. The result of the command sequence is that VRF *vrf_blue* has two export extended communities (1000:1 and 1000:2) and two import extended communities (1000:1 and 173.27.0.130:200).

```
Router(config)# ip vrf vrf_blue

Router(config-vrf)# route-target both 1000:1

Router(config-vrf)# route-target export 1000:2

Router(config-vrf)# route-target import 173.27.0.130:200
```

Related Commands

Command	Description
import map	Configures an import route map for the VRF.
ip vrf	Enters VRF configuration mode.

show ip bgp vpnv4

To display Virtual Private network (VPN) address information from the Border Gateway Protocol (BGP) table, use the **show ip bgp vpnv4** command in privileged EXEC mode.

```
show ip bgp vpnv4 {all | rd route-distinguisher | vrf vrf-name} [ip-prefix/length [longer-prefixes]
[output-modifiers]] [network-address [mask] [longer-prefixes] [output-modifiers]] [cidr-only]
[community] [community-list] [dampened-paths] [filter-list] [flap-statistics]
[inconsistent-as] [neighbors] [paths [line]] [peer-group] [quote-regexp] [regexp]
[summary] [tags]
```

Syntax Description

all	Displays the complete VPNv4 database.
rd <i>route-distinguisher</i>	Displays NLRI that have a matching route distinguisher.
vrf <i>vrf-name</i>	Displays NLRI associated with the named VRF.
<i>ip-prefix/length</i>	(Optional) IP prefix address (in dotted decimal format) and length of mask (0 to 32).
longer-prefixes	(Optional) Displays the entry, if any, that exactly matches the specified prefix parameter, as well as all entries that match the prefix in a “longest-match” sense. That is, prefixes for which the specified prefix is an initial substring.
<i>output-modifiers</i>	(Optional) For a list of associated keywords and arguments, use context-sensitive help.
<i>network-address</i>	(Optional) IP address of a network in the BGP routing table.
<i>mask</i>	(Optional) Mask of the network address, in dotted decimal format.
cidr-only	(Optional) Displays only routes that have nonnatural net masks.
community	(Optional) Displays routes matching this community.
community-list	(Optional) Displays routes matching this community list.
dampened-paths	(Optional) Displays paths suppressed due to dampening (BGP route from peer is up and down).
filter-list	(Optional) Displays routes conforming to the filter list.
flap-statistics	(Optional) Displays flap statistics of routes.
inconsistent-as	(Optional) Displays only routes that have inconsistent autonomous systems of origin.
neighbors	(Optional) Displays details about TCP and BGP neighbor connections.
paths	(Optional) Displays path information.
<i>line</i>	(Optional) A regular expression to match the BGP AS paths.
peer-group	(Optional) Displays information about peer groups.
quote-regexp	(Optional) Displays routes matching the AS path “regular expression.”
regexp	(Optional) Displays routes matching the AS path regular expression.
summary	(Optional) Displays BGP neighbor status.
tags	(Optional) Displays incoming and outgoing BGP labels for each NLRI.

Defaults

No default behavior or values.

■ show ip bgp vpnv4

Command Modes Privileged EXEC

Command History	Release	Modification
	12.0(5)T	This command was introduced.
	12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
	12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
	12.0(23)S	This command was integrated into Cisco IOS 12.0(23)S.
	12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.

Usage Guidelines Use this command to display VPNv4 information from the BGP database. The **show ip bgp vpnv4 all** command displays all available VPNv4 information. The **show ip bgp vpnv4 summary** command displays BGP neighbor status.

Examples The following example shows output for all available VPNv4 information in a BGP routing table:

```
Router# show ip bgp vpnv4 all

BGP table version is 18, local router ID is 14.14.14.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

      Network          Next Hop           Metric   LocPrf   Weight   Path
Route Distinguisher: 100:1 vrf1
*> 11.0.0.0           50.0.0.1           0         0         0         101 i
*>i12.0.0.0           13.13.13.13        0         100        0         102 i
*> 50.0.0.0           50.0.0.1           0         0         0         101 i
*>i51.0.0.0           13.13.13.13        0         100        0         102 i
```

[Table 1](#) describes the fields shown in the example.

Table 1 show ip bgp vpnv4 Field Descriptions

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the address of the BGP next hop.
Metric	Displays the BGP metric.
LocPrf	Displays the local preference.
Weight	Displays the BGP weight.
Path	Displays the BGP path per route.

The following example shows how to display a table of labels for NLRIs that have a route-distinguisher value of 100:1.

```
Router# show ip bgp vpnv4 rd 100:1 tags

      Network      Next Hop      In tag/Out tag
Route Distinguisher: 100:1 (vrf1)
  2.0.0.0          10.20.0.60    34/notag
  10.0.0.0         10.20.0.60    35/notag
  12.0.0.0         10.20.0.60    26/notag
                  10.20.0.60    26/notag
  13.0.0.0         10.15.0.15    notag/26
```

Table 2 describes the fields shown in the example.

Table 2 *show ip bgp vpnv4 rd tags Field Descriptions*

Field	Description
Network	Displays the network address from the BGP table.
Next Hop	Displays the BGP next hop address.
In Tag	Displays the label (if any) assigned by this router.
Out Tag	Displays the label assigned by the BGP next hop router.

The following example shows VPNv4 routing entries for the VRF called vrf1.

```
Router# show ip bgp vpnv4 vrf vrf1

BGP table version is 18, local router ID is 14.14.14.14
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop Metric LocPrf Weight Path
Route Distinguisher: 100:1 (vrf1)
*> 11.0.0.0      50.0.0.1 0 0 101 i
*>i12.0.0.0     13.13.13.13 0 100 0 102 i
*> 50.0.0.0      50.0.0.1 0 0 101 i
*>i151.0.0.0    13.13.13.13 0 100 0 102 i
```

Table 3 describes the fields shown in the example.

Table 3 *show ip bgp vpnv4 Field Descriptions*

Field	Description
Network	Displays network address from the BGP table.
Next Hop	Displays address of the BGP next hop.
Metric	Displays the BGP metric.
LocPrf	Displays the local preference.
Weight	Displays the BGP weight.
Path	Displays the BGP path per route.

Related Commands

Command	Description
show ip vrf	Displays VRFs and associated interfaces.

show ip cef vrf

To display the CEF forwarding table associated with a Virtual Private Network (VPN) routing/forwarding instance (VRF), use the **show ip cef vrf** command in privileged EXEC mode.

```
show ip cef vrf vrf-name [ip-prefix [mask [longer-prefixes]] [detail] [output-modifiers]] [interface
interface-number] [adjacency [interface interface-number] [detail] [discard] [drop] [glean]
[null] [punt] [output-modifiers]] [detail [output-modifiers]] [non-recursive [detail]
[output-modifiers]] [summary [output-modifiers]] [traffic [prefix-length] [output-modifiers]]
[unresolved [detail] [output-modifiers]]
```

Syntax Description

<i>vrf-name</i>	Name assigned to the VRF.
<i>ip-prefix</i>	(Optional) IP prefix of entries to show, in dotted decimal format (A.B.C.D).
<i>mask</i>	(Optional) Mask of the IP prefix, in dotted decimal format.
longer-prefixes	(Optional) Displays table entries for all of the more specific routes.
detail	(Optional) Displays detailed information for each CEF table entry.
<i>output-modifiers</i>	(Optional) For a list of associated keywords and arguments, use context-sensitive help.
<i>interface</i>	(Optional) Type of network interface to use: ATM, Ethernet, Loopback, POS (packet over SONET) or Null.
<i>interface-number</i>	Number identifying the network interface to use.
adjacency	(Optional) Displays all prefixes resolving through adjacency.
discard	(Optional) Discards adjacency.
drop	(Optional) Drops adjacency.
glean	(Optional) Gleans adjacency.
null	(Optional) Null adjacency.
punt	(Optional) Punts adjacency.
non-recursive	(Optional) Displays only nonrecursive routes.
summary	(Optional) Displays a CEF table summary.
traffic	(Optional) Displays traffic statistics.
prefix-length	(Optional) Displays traffic statistics by prefix size.
unresolved	(Optional) Displays only unresolved routes.

Defaults

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.

Release	Modification
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.

Usage Guidelines

Used with only the *vrf-name* argument, the **show ip cef vrf** command shows a shortened display of the CEF table.

Used with the **detail** keyword, the **show ip cef vrf** command shows detailed information for all CEF table entries.

Examples

This example shows the forwarding table associated with the VRF called vrf1:

```
Router# show ip cef vrf vrf1

Prefix          Next Hop          Interface
0.0.0.0/32      receive
11.0.0.0/8      50.0.0.1          Ethernet1/3
12.0.0.0/8      52.0.0.2          POS6/0
50.0.0.0/8      attached          Ethernet1/3
50.0.0.0/32     receive
50.0.0.1/32     50.0.0.1          Ethernet1/3
50.0.0.2/32     receive
50.255.255.255/32 receive
51.0.0.0/8      52.0.0.2          POS6/0
224.0.0.0/24    receive
255.255.255.255/32 receive
```

Table 4 describes the fields shown in the example.

Table 4 *show ip cef vrf* Field Descriptions

Field	Description
Prefix	Specifies the network prefix.
Next Hop	Specifies the BGP next hop address.
Interface	Specifies the VRF interface.

Related Commands

Command	Description
show ip route vrf	Displays the IP routing table associated with a VRF.
show ip vrf	Displays VRF interfaces.

show ip protocols vrf

To display the routing protocol information associated with a Virtual Private Network (VPN) routing/forwarding instance (VRF), use the **show ip protocols vrf** command in privileged EXEC mode.

show ip protocols vrf *vrf-name*

Syntax Description	<i>vrf-name</i>	Name assigned to a VRF.
--------------------	-----------------	-------------------------

Defaults No default behavior or values.

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.0(5)T	This command was introduced.
	12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
	12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
	12.0(23)S	This command was integrated into Cisco IOS 12.0(23)S.
	12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.

Usage Guidelines Use this command to display routing information associated with a VRF.

Examples The following example displays information about a VRF called vpn2:

```
Router# show ip protocols vrf vpn2

Routing Protocol is "bgp 100"
  Sending updates every 60 seconds, next due in 0 sec
  Outgoing update filter list for all interfaces is
  Incoming update filter list for all interfaces is
  IGP synchronization is disabled
  Automatic route summarization is disabled
  Redistributing:connected, static
  Routing for Networks:
  Routing Information Sources:
    Gateway         Distance      Last Update
    13.13.13.13      200           02:20:54
    18.18.18.18      200           03:26:15
  Distance:external 20 internal 200 local 200
```

[Table 5](#) describes the fields shown in the example.

Table 5 *show ip protocols vrf Field Descriptions*

Field	Description
Gateway	Displays the IP address of the router identifier for all routers in the network.
Distance	Displays the metric used to access the destination route.
Last update	Displays the last time the routing table was updated from the source.

Related Commands

Command	Description
show ip vrf	Displays VRF interfaces.

show ip route vrf

To display the IP routing table associated with a Virtual Private Network (VPN) routing/forwarding instance (VRF), use the **show ip route vrf** command in privileged EXEC mode.

```
show ip route vrf vrf-name [connected] [protocol [as-number] [tag] [output-modifiers]]
[list number [output-modifiers]] [profile] [static [output-modifiers]]
[summary [output-modifiers]] [supernets-only [output-modifiers]]
```

Syntax Description

<i>vrf-name</i>	Name assigned to the VRF.
connected	(Optional) Displays all connected routes in a VRF.
<i>protocol</i>	(Optional) To specify a routing protocol, use one of the following keywords: bgp , egp , eigrp , hello , igrp , isis , ospf , or rip .
<i>as-number</i>	(Optional) Autonomous system number.
<i>tag</i>	(Optional) Cisco IOS routing area label.
<i>output-modifiers</i>	(Optional) For a list of associated keywords and arguments, use context-sensitive help.
list number	(Optional) Specifies the IP access list to display.
profile	(Optional) Displays the IP routing table profile.
static	(Optional) Displays static routes.
summary	(Optional) Displays a summary of routes.
supernets-only	(Optional) Displays supernet entries only.

Command Modes

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.

Usage Guidelines

This command displays specified information from the IP routing table of a VRF.

Examples

This example shows the IP routing table associated with the VRF called vrf1:

```
Router# show ip route vrf vrf1
```

```
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR
       T - traffic engineered route
```

Gateway of last resort is not set

```
B   51.0.0.0/8 [200/0] via 13.13.13.13, 00:24:19
C   50.0.0.0/8 is directly connected, Ethernet1/3
B   11.0.0.0/8 [20/0] via 50.0.0.1, 02:10:22
B   12.0.0.0/8 [200/0] via 13.13.13.13, 00:24:20
```

This example shows BGP entries in the IP routing table associated with the VRF called vrf1:

```
Router# show ip route vrf vrf1 bgp
```

```
B 51.0.0.0/8 [200/0] via 13.13.13.13, 03:44:14
B 11.0.0.0/8 [20/0] via 51.0.0.1, 03:44:12
B 12.0.0.0/8 [200/0] via 13.13.13.13, 03:43:14
```

Related Commands

Command	Description
show ip cef vrf	Displays the CEF forwarding table associated with a VRF.
show ip vrf	Displays VRFs and associated interfaces.

show ip vrf

To display the set of defined Virtual Private Network (VPN) routing/forwarding instances (VRF) and associated interfaces, use the **show ip vrf** command in privileged EXEC mode.

```
show ip vrf [{brief | detail | interfaces}] [vrf-name] [output-modifiers]
```

Syntax Description

brief	(Optional) Displays concise information on the VRF(s) and associated interfaces.
detail	(Optional) Displays detailed information on the VRF(s) and associated interfaces.
interfaces	(Optional) Displays detailed information about all interfaces bound to a particular VRF, or any VRF.
<i>vrf-name</i>	Name assigned to a VRF.
<i>output-modifiers</i>	(Optional) For a list of associated keywords and arguments, use context-sensitive help.

Defaults

When no optional parameters are specified, the command shows concise information about all configured VRFs.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.

Usage Guidelines

Use this command to display information about VRFs. Two levels of detail are available: use the **brief** keyword or no keyword to display concise information, or use the **detail** keyword to display all information. To display information about all interfaces bound to a particular VRF, or to any VRF, use the **interfaces** keyword.

Examples

This example shows brief information for the VRFs currently configured:

```
Router# show ip vrf
```

```

Name                Default RD          Interfaces
vrf1                 100:1              Ethernet1/3
vrf2                 100:2              Ethernet0/3
```

Table 6 describes the fields shown in the example.

Table 6 *show vrf Field Descriptions*

Field	Description
Name	Specifies the VRF name.
Default RD	Specifies the default route distinguisher.
Interfaces	Specifies the network interfaces.

This example shows detailed information for the VRF called vrf1:

```
Router# show ip vrf detail vrf1

VRF vrf1; default RD 100:1
  Interfaces:
    Ethernet1/3
  Connected addresses are in global routing table
  Export VPN route-target communities
    RT:100:1
  Import VPN route-target communities
    RT:100:1
  No import route-map
```

Table 7 describes the fields shown in this example.

Table 7 *show ip vrf detail Field Descriptions*

Field	Description
Interfaces	Specifies the network interfaces.
Export	Specifies VPN route-target export communities.
Import	Specifies VPN route-target import communities.

This example shows the interfaces bound to a particular VRF:

```
router# show ip vrf interfaces

Interface      IP-Address      VRF              Protocol
Ethernet2      130.22.0.33    blue_vrf         up
Ethernet4      130.77.0.33    hub              up
router#
```

Table 8 describes the fields shown in the example.

Table 8 *show ip vrf interfaces Field Descriptions*

Field	Description
Interface	Specifies the network interfaces for a VRF.
IP-Address	Specifies the IP address of a VRF interface.
VRF	Specifies the VRF name.
Protocol	Displays the state of the protocol (up/down) for each VRF interface.

■ show ip vrf

Related Commands	Command	Description
	import map	Configures an import route map for a VRF.
	ip vrf	Enters VRF configuration mode.
	ip vrf forwarding	Associates a VRF with an interface or subinterface.
	rd	Configures a default RD for a VRF.
	route-target	Configures import and export extended community attributes for the VRF.

show tag-switching forwarding vrf

To display label forwarding information for advertised Virtual Private Network (VPN) routing/forwarding (VRF) routes, use the **show tag-switching forwarding vrf** command in privileged EXEC mode. To disable the display of label forwarding information, use the **no** form of this command.

show tag-switching forwarding vrf *vrf-name* [*ip-prefix/length* [*mask*]] [**detail**]
[*output-modifiers*]

no show tag-switching forwarding vrf *vrf-name* [*ip-prefix/length* [*mask*]] [**detail**]
[*output-modifiers*]

Syntax Description

<i>vrf-name</i>	Displays NLRIs associated with the named VRF.
<i>ip-prefix/length</i>	(Optional) IP prefix address (in dotted decimal format) and length of mask (0 to 32).
<i>mask</i>	(Optional) Destination network mask, in dotted decimal format.
detail	(Optional) Displays detailed information on the VRF routes.
<i>output-modifiers</i>	(Optional) For a list of associated keywords and arguments, use context-sensitive help.

Command Types

No default behavior or values.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(21)ST	This command was integrated into Cisco IOS 12.0(21)ST.
12.0(22)S	This command was integrated into Cisco IOS 12.0(22)S.
12.0(23)S	This command was integrated into Cisco IOS 12.0(23)S.
12.2(13)T	This command was integrated into Cisco IOS 12.2(13)T.

Usage Guidelines

Use this command to display label forwarding entries associated with a particular VRF or IP prefix.

Examples

The following example shows label forwarding entries that correspond to the VRF called vpn1:

```
Router# show tag-switching forwarding vrf vrf1 detail
```

■ show tag-switching forwarding vrf

Related Commands	Command	Description
	show ip cef vrf	Displays VRFs and associated interfaces.
	show tag-switching forwarding-table	Displays the contents of the LFIB.

Glossary

ATM edge LSR—A router that is connected to the ATM LSR cloud through LSC-ATM interfaces. The ATM edge LSR adds labels to unlabeled packets and strips labels from labeled packets.

ATM-LSR—A label switch router with a number of LSC-ATM interfaces. The router forwards the cells among these interfaces using labels carried in the VPI/VCI field.

BGP—Border Gateway Protocol. Interdomain routing protocol that exchanges reachability information with other BGP systems. It is defined in RFC 1163.

CEF—Cisco Express Forwarding. An advanced Layer 3 IP switching technology. CEF optimizes network performance and scalability for networks with large and dynamic traffic patterns.

CE router—customer edge router. A router that is part of a customer network and that interfaces to a provider edge (PE) router. CE routers are not aware of associated VPNs.

CoS—class of service. A feature that provides scalable, differentiated types of service across an MPLS network.

GRE—generic routing encapsulation. A tunneling protocol developed by Cisco that can encapsulate a wide variety of protocol packet types inside IP tunnels, creating a virtual point-to-point link to Cisco routers at remote points over an IP internetwork. By connecting multiprotocol subnetworks in a single-protocol backbone environment, IP tunneling that uses GRE allows network expansion across a single-protocol backbone environment.

IGP—Interior Gateway Protocol. An Internet protocol used to exchange routing information within an autonomous system. Examples of common IBGPs include IGRP, OSPF, and RIP.

IS-IS—Intermediate System-to-Intermediate System. OSI link-state hierarchical routing protocol in which ISs (routers) exchange routing information based on a single metric to determine network topology.

LSA—link-state advertisement. A broadcast packet used by link-state protocols. The LSA contains information about neighbors and path costs and is used by the receiving router to maintain a routing table.

LSP—label-switched path. A sequence of hops (R0...Rn) in which a packet travels from R0 to Rn through label switching mechanisms. A label-switched path can be established dynamically, based on normal routing mechanisms, or through configuration.

LSP tunnel—label-switched path tunnel. A configured connection between two routers, in which MPLS is used to carry the packet.

MPLS—Multiprotocol Label Switching. An emerging industry standard. Switching method that forwards IP traffic using a label. This label instructs the routers and the switches in the network where to forward the packets based on preestablished IP routing information.

NLRI—Network Layer Reachability Information. BGP sends routing update messages containing NLRI to describe a route and how to get there. In this context, an NLRI is a prefix. A BGP update message carries one or more NLRI prefixes and the attributes of a route for the NLRI prefixes; the route attributes include a BGP next hop gateway address, community values, and other information.

PE router—provider edge router. A router that is part of a service provider's network connected to a customer edge (CE) router. All VPN processing occurs in the PE router.

RD—route distinguisher. An 8-byte value that is concatenated with an IPv4 prefix to create a unique VPN IPv4 prefix.

RIP—Routing Information Protocol. An IGP used to exchange routing information within an autonomous system, RIP uses hop count as a routing metric.

traffic engineering—The techniques and processes used to cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods had been used.

traffic engineering tunnel—A label-switched path tunnel that is used for engineering traffic. It is set up through means other than normal Layer 3 routing and is used to direct traffic over a path different from the one that Layer 3 routing would cause it to take.

tunneling—Architecture providing the services necessary to implement any standard point-to-point data encapsulation scheme.

VPN—Virtual Private Network. A secure IP-based network that shares resources on one or more physical networks. A VPN contains geographically dispersed sites that can communicate securely over a shared backbone.

VPNv4—Indicate a VPN-IPv4 prefix. These prefixes are customer VPN addresses, each of which has been made unique by the addition of an 8-byte route distinguisher.

VRF—VPN routing/forwarding instance. A VRF consists of an IP routing table, a derived forwarding table, a set of interfaces that use the forwarding table, and a set of rules and routing protocols that determine what goes into the forwarding table. In general, a VRF includes the routing information that defines a customer VPN site that is attached to a PE router.