Implementing MPLS Layer 3 VPNs

A Multiprotocol Label Switching (MPLS) Layer 3 Virtual Private Network (VPN) consists of a set of sites that are interconnected by means of an MPLS provider core network. At each customer site, one or more customer edge (CE) routers attach to one or more provider edge (PE) routers.

This module provides the conceptual and configuration information for MPLS Layer 3 VPNs on Cisco IOS XR software.

Note You must acquire an evaluation or permanent license in order to use MPLS Layer 3 VPN functionality. However, if you are upgrading from a previous version of the software, MPLS Layer 3 VPN functionality will continue to work using an implicit license for 90 days (during which time, you can purchase a permanent license). For more information about licenses, see the *Software Entitlement on the Cisco ASR 9000 Series Router* module in the *System Management Configuration Guide for Cisco ASR 9000 Series Routers*.

Prerequisites for Implementing MPLS L3VPN

The following prerequisites are required to configure MPLS Layer 3 VPN:

- To perform these configuration tasks, your Cisco IOS XR software system administrator must assign you to a user group associated with a task group that includes the corresponding command task IDs. All command task IDs are listed in individual command references and in the *Cisco IOS XR Task ID Reference Guide*.
- If you suspect user group assignment is preventing you from using a command, contact your AAA administrator for assistance.

- You must be in a user group associated with a task group that includes the proper task IDs for:
  - BGP commands
  - MPLS commands (generally)
  - MPLS Layer 3 VPN commands
- To configure MPLS Layer 3 VPNs, routers must support MPLS forwarding and Forwarding Information Base (FIB).

The following prerequisites are required for configuring MPLS VPN Inter-AS with autonomous system boundary routers (ASBRs) exchanging VPN-IPV4 addresses or IPv4 routes and MPLS labels:

- Before configuring external Border Gateway Protocol (eBGP) routing between autonomous systems or subautonomous systems in an MPLS VPN, ensure that all MPLS VPN routing instances and sessions are properly configured (see the How to Implement MPLS Layer 3 VPNs, for procedures)
- These following tasks must be performed:
  - Define VPN routing instances
  - Configure BGP routing sessions in the MPLS core
  - Configure PE-to-PE routing sessions in the MPLS core
  - Configure BGP PE-to-CE routing sessions
  - Configure a VPN-IPv4 eBGP session between directly connected ASBRs

MPLS L3VPN Restrictions

The following restrictions apply when configuring MPLS VPN Inter-AS with ASBRs exchanging IPv4 routes and MPLS labels:

- For networks configured with eBGP multihop, a label switched path (LSP) must be configured between non adjacent routers.
- Inter-AS supports IPv4 routes only. IPv6 is not supported.

Note The physical interfaces that connect the BGP speakers must support FIB and MPLS.

Information About MPLS Layer 3 VPNs

To implement MPLS Layer 3 VPNs, you need to understand the following concepts:

MPLS L3VPN Overview

Before defining an MPLS VPN, VPN in general must be defined. A VPN is:

- An IP-based network delivering private network services over a public infrastructure
- A set of sites that are allowed to communicate with each other privately over the Internet or other public or private networks

Conventional VPNs are created by configuring a full mesh of tunnels or permanent virtual circuits (PVCs) to all sites in a VPN. This type of VPN is not easy to maintain or expand, as adding a new site requires changing each edge device in the VPN.

MPLS-based VPNs are created in Layer 3 and are based on the peer model. The peer model enables the service provider and the customer to exchange Layer 3 routing information. The service provider relays the data between the customer sites without customer involvement.

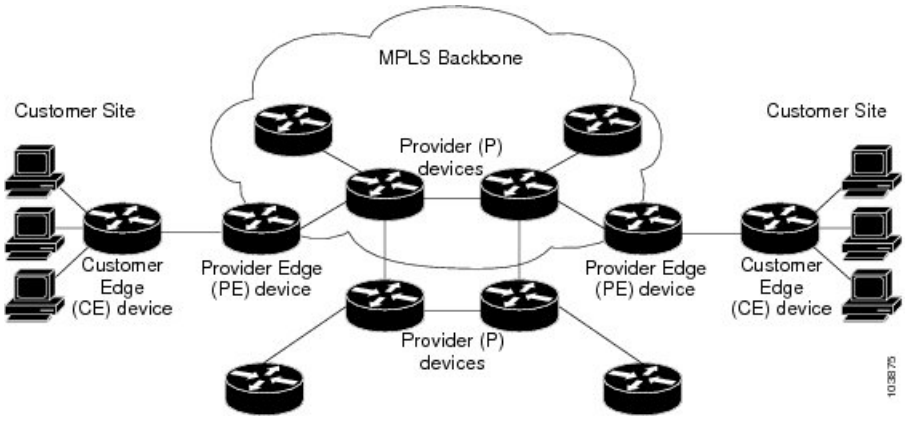
MPLS VPNs are easier to manage and expand than conventional VPNs. When a new site is added to an MPLS VPN, only the edge router of the service provider that provides services to the customer site needs to be updated.

The components of the MPLS VPN are described as follows:

- Provider (P) router—Router in the core of the provider network. P routers run MPLS switching and do not attach VPN labels to routed packets. VPN labels are used to direct data packets to the correct private network or customer edge router.
- PE router—Router that attaches the VPN label to incoming packets based on the interface or subinterface on which they are received, and also attaches the MPLS core labels. A PE router attaches directly to a CE router.
- Customer (C) router—Router in the Internet service provider (ISP) or enterprise network.
- Customer edge (CE) router—Edge router on the network of the ISP that connects to the PE router on the network. A CE router must interface with a PE router.

This following figures shows a basic MPLS VPN topology.

Figure 1: Basic MPLS VPN Topology



MPLS L3VPN Benefits

MPLS L3VPN provides the following benefits:

- Service providers can deploy scalable VPNs and deliver value-added services.

- Connectionless service guarantees that no prior action is necessary to establish communication between hosts.
- Centralized Service: Building VPNs in Layer 3 permits delivery of targeted services to a group of users represented by a VPN.
- Scalability: Create scalable VPNs using connection-oriented, point-to-point overlays, Frame Relay, or ATM virtual connections.
- Security: Security is provided at the edge of a provider network (ensuring that packets received from a customer are placed on the correct VPN) and in the backbone.
- Integrated Quality of Service (QoS) support: QoS provides the ability to address predictable performance and policy implementation and support for multiple levels of service in an MPLS VPN.
- Straightforward Migration: Service providers can deploy VPN services using a straightforward migration path.
- Migration for the end customer is simplified. There is no requirement to support MPLS on the CE router and no modifications are required for a customer intranet.

How MPLS L3VPN Works

MPLS VPN functionality is enabled at the edge of an MPLS network. The PE router performs the following tasks:

- Exchanges routing updates with the CE router
- Translates the CE routing information into VPN version 4 (VPNv4) routes.
- Exchanges VPNv4 and VPNv6 routes with other PE routers through the Multiprotocol Border Gateway Protocol (MP-BGP)

Virtual Routing and Forwarding Tables

Each VPN is associated with one or more VPN routing and forwarding (VRF) instances. A VRF defines the VPN membership of a customer site attached to a PE router. A VRF consists of the following components:

- An IP version 4 (IPv4) unicast routing table
- A derived FIB table
- A set of interfaces that use the forwarding table
- A set of rules and routing protocol parameters that control the information that is included in the routing table

These components are collectively called a VRF instance.

A one-to-one relationship does not necessarily exist between customer sites and VPNs. A site can be a member of multiple VPNs. However, a site can associate with only one VRF. A 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 FIB table for each VRF. A separate set of routing and FIB 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 Routing Information: Distribution

The distribution of VPN routing information is controlled through the use of VPN route target communities, implemented by BGP extended communities. VPN routing information is distributed as follows:

- When a VPN route that is learned from a CE router is injected into a BGP, a list of VPN route target extended community attributes is associated with it. Typically, the list of route target community extended values is set from an export list of route targets associated with the VRF from which the route was learned.
- An import list of route target extended communities is associated with each VRF. The import list defines route target extended community attributes that 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 extended 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 PE router can learn an IP prefix from the following sources:

- A CE router by static configuration
- An eBGP session with the CE router
- A Routing Information Protocol (RIP) exchange with the CE router
- Open Shortest Path First (OSPF), Enhanced Interior Gateway Routing Protocol (EIGRP), and RIP as Interior Gateway Protocols (IGPs)

The IP prefix is a member of the IPv4 address family. After the PE router learns the IP prefix, the PE converts it into the VPN-IPv4 prefix by combining it with a 64-bit route distinguisher. The generated prefix is a member of the VPN-IPv4 address family. It uniquely identifies 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 the **rd** 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 the IP domain, known as an autonomous system.
- Between autonomous systems.

PE to PE or PE to route reflector (RR) sessions are iBGP sessions, and PE to CE sessions are eBGP sessions. PE to CE eBGP sessions can be directly or indirectly connected (eBGP multihop).

BGP propagates reachability information for VPN-IPv4 prefixes among PE routers by the BGP protocol extensions (see RFC 2283, Multiprotocol Extensions for BGP-4), which define support for address families other than IPv4. Using the extensions 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 the VRF FIB 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:

- The top label directs the packet to the correct PE router.
- The second label indicates how that PE router should forward the packet to the CE router.

More labels can be stacked if other features are enabled. For example, if traffic engineering (TE) tunnels with fast reroute (FRR) are enabled, the total number of labels imposed in the PE is four (Layer 3 VPN, Label Distribution Protocol (LDP), TE, and FRR).

Automatic Route Distinguisher Assignment

To take advantage of iBGP load balancing, every network VRF must be assigned a unique route distinguisher. VRF requires a route distinguisher for BGP to distinguish between potentially identical prefixes received from different VPNs.

With thousands of routers in a network each supporting multiple VRFs, configuration and management of route distinguishers across the network can present a problem. Cisco IOS XR software simplifies this process by assigning unique route distinguisher to VRFs using the **rd auto** command.

To assign a unique route distinguisher for each router, you must ensure that each router has a unique BGP router-id. If so, the **rd auto** command assigns a Type 1 route distinguisher to the VRF using the following format: *ip-address:number*. The IP address is specified by the BGP router-id statement and the number (which is derived as an unused index in the 0 to 65535 range) is unique across theVRFs.

Finally, route distinguisher values are checkpointed so that route distinguisher assignment to VRF is persistent across failover or process restart. If an route distinguisher is explicitely configured for a VRF, this value is not overridden by the autoroute distinguisher.

MPLS L3VPN Major Components

An MPLS-based VPN network has three major components:

- VPN route target communities—A VPN route target community is a list of all members of a VPN community. VPN route targets need to be configured for each VPN community member.
- Multiprotocol BGP (MP-BGP) peering of the VPN community PE routers—MP-BGP propagates VRF reachability information to all members of a VPN community. MP-BGP peering needs to be configured in all PE routers within a VPN community.
- MPLS forwarding—MPLS transports all traffic between all VPN community members across a VPN service-provider network.

A one-to-one relationship does not necessarily exist between customer sites and VPNs. A given site can be a member of multiple VPNs. However, a site can associate with only one VRF. A customer-site VRF contains all the routes available to the site from the VPNs of which it is a member

Inter-AS Support for L3VPN

This section contains the following topics:

Inter-AS Support: Overview

An autonomous system (AS) is a single network or group of networks that is controlled by a common system administration group and uses a single, clearly defined routing protocol.

As VPNs grow, their requirements expand. In some cases, VPNs need to reside on different autonomous systems in different geographic areas. In addition, some VPNs need to extend across multiple service providers (overlapping VPNs). Regardless of the complexity and location of the VPNs, the connection between autonomous systems must be seamless.

An MPLS VPN Inter-AS provides the following benefits:

- Allows a VPN to cross more than one service provider backbone.

  Service providers, running separate autonomous systems, can jointly offer MPLS VPN services to the same end customer. A VPN can begin at one customer site and traverse different VPN service provider backbones before arriving at another site of the same customer. Previously, MPLS VPN could traverse only a single BGP autonomous system service provider backbone. This feature lets multiple autonomous systems form a continuous, seamless network between customer sites of a service provider.

- Allows a VPN to exist in different areas.

  A service provider can create a VPN in different geographic areas. Having all VPN traffic flow through one point (between the areas) allows for better rate control of network traffic between the areas.

- Allows confederations to optimize iBGP meshing.

  Internal Border Gateway Protocol (iBGP) meshing in an autonomous system is more organized and manageable. You can divide an autonomous system into multiple, separate subautonomous systems and then classify them into a single confederation. This capability lets a service provider offer MPLS VPNs across the confederation, as it supports the exchange of labeled VPN-IPv4 Network Layer Reachability Information (NLRI) between the subautonomous systems that form the confederation.

Inter-AS and ASBRs

Separate autonomous systems from different service providers can communicate by exchanging IPv4 NLRI and IPv6 in the form of VPN-IPv4 addresses. The ASBRs use eBGP to exchange that information. Then an Interior Gateway Protocol (IGP) distributes the network layer information for VPN-IPV4 prefixes throughout each VPN and each autonomous system. The following protocols are used for sharing routing information:

- Within an autonomous system, routing information is shared using an IGP.
- Between autonomous systems, routing information is shared using an eBGP. An eBGP lets service providers set up an interdomain routing system that guarantees the loop-free exchange of routing information between separate autonomous systems.

  The primary function of an eBGP is to exchange network reachability information between autonomous systems, including information about the list of autonomous system routes. The autonomous systems

use EBGP border edge routers to distribute the routes, which include label switching information. Each border edge router rewrites the next-hop and MPLS labels.

Inter-AS configurations supported in an MPLS VPN can include:

- Interprovider VPN—MPLS VPNs that include two or more autonomous systems, connected by separate border edge routers. The autonomous systems exchange routes using eBGP. No IGP or routing information is exchanged between the autonomous systems.
- BGP Confederations—MPLS VPNs that divide a single autonomous system into multiple subautonomous systems and classify them as a single, designated confederation. The network recognizes the confederation as a single autonomous system. The peers in the different autonomous systems communicate over eBGP sessions; however, they can exchange route information as if they were iBGP peers.

Confederations

A confederation is multiple subautonomous systems grouped together. A confederation reduces the total number of peer devices in an autonomous system. A confederation divides an autonomous system into subautonomous systems and assigns a confederation identifier to the autonomous systems. A VPN can span service providers running in separate autonomous systems or multiple subautonomous systems that form a confederation.

In a confederation, each subautonomous system is fully meshed with other subautonomous systems. The subautonomous systems communicate using an IGP, such as Open Shortest Path First (OSPF) or Intermediate System-to-Intermediate System (IS-IS). Each subautonomous system also has an eBGP connection to the other subautonomous systems. The confederation eBGP (CEBGP) border edge routers forward next-hop-self addresses between the specified subautonomous systems. The next-hop-self address forces the BGP to use a specified address as the next hop rather than letting the protocol choose the next hop.

You can configure a confederation with separate subautonomous systems two ways:

- Configure a router to forward next-hop-self addresses between only the CEBGP border edge routers (both directions). The subautonomous systems (iBGP peers) at the subautonomous system border do not forward the next-hop-self address. Each subautonomous system runs as a single IGP domain. However, the CEBGP border edge router addresses are known in the IGP domains.
- Configure a router to forward next-hop-self addresses between the CEBGP border edge routers (both directions) and within the iBGP peers at the subautonomous system border. Each subautonomous system runs as a single IGP domain but also forwards next-hop-self addresses between the PE routers in the domain. The CEBGP border edge router addresses are known in the IGP domains.

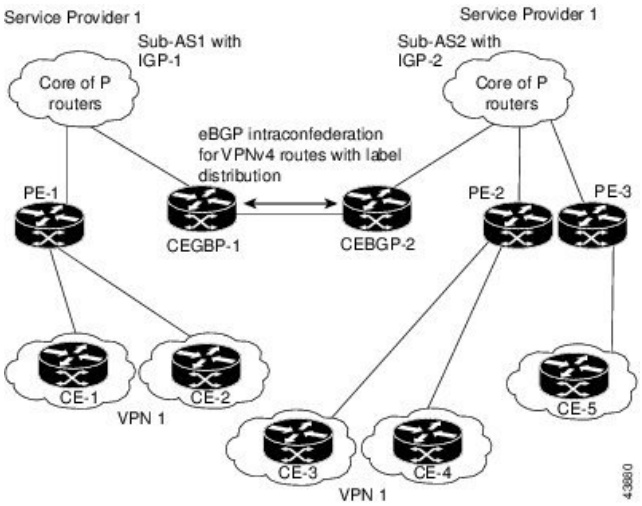
Note eBGP Connection Between Two Subautonomous Systems in a Confederation figure illustrates how two autonomous systems exchange routes and forward packets. Subautonomous systems in a confederation use a similar method of exchanging routes and forwarding packets.

The figure below illustrates a typical MPLS VPN confederation configuration. In this configuration:

- The two CEBGP border edge routers exchange VPN-IPv4 addresses with labels between the two autonomous systems.

- The distributing router changes the next-hop addresses and labels and uses a next-hop-self address.
- IGP-1 and IGP-2 know the addresses of CEBGP-1 and CEBGP-2.

Figure 2: eBGP Connection Between Two Subautonomous Systems in a Confederation



In this confederation configuration:

- CEBGP border edge routers function as neighboring peers between the subautonomous systems. The subautonomous systems use eBGP to exchange route information.
- Each CEBGP border edge router (CEBGP-1 and CEBGP-2) assigns a label for the router before distributing the route to the next subautonomous system. The CEBGP border edge router distributes the route as a VPN-IPv4 address by using the multiprotocol extensions of BGP. The label and the VPN identifier are encoded as part of the NLRI.
- Each PE and CEBGP border edge router assigns its own label to each VPN-IPv4 address prefix before redistributing the routes. The CEBGP border edge routers exchange IPV-IPv4 addresses with the labels. The next-hop-self address is included in the label (as the value of the eBGP next-hop attribute). Within the subautonomous systems, the CEBGP border edge router address is distributed throughout the iBGP neighbors, and the two CEBGP border edge routers are known to both confederations.
- For more information about how to configure confederations, see the Configuring MPLS Forwarding for ASBR Confederations, on page 58 .

MPLS VPN Inter-AS BGP Label Distribution

Note This section is not applicable to Inter-AS over IP tunnels.

You can set up the MPLS VPN Inter-AS network so that the ASBRs exchange IPv4 routes with MPLS labels of the provider edge (PE) routers. Route reflectors (RRs) exchange VPN-IPv4 routes by using multihop, multiprotocol external Border Gateway Protocol (eBGP). This method of configuring the Inter-AS system is often called MPLS VPN Inter-AS BGP Label Distribution.

Configuring the Inter-AS system so that the ASBRs exchange the IPv4 routes and MPLS labels has the following benefits:

- Saves the ASBRs from having to store all the VPN-IPv4 routes. Using the route reflectors to store the VPN-IPv4 routes and distributes them to the PE routers results in improved scalability compared with configurations in which the ASBR holds all the VPN-IPv4 routes and distributes the routes based on VPN-IPv4 labels.
- Having the route reflectors hold the VPN-IPv4 routes also simplifies the configuration at the border of the network.
- Enables a non-VPN core network to act as a transit network for VPN traffic. You can transport IPv4 routes with MPLS labels over a non-MPLS VPN service provider.
- Eliminates the need for any other label distribution protocol between adjacent label switch routers (LSRs). If two adjacent LSRs are also BGP peers, BGP can handle the distribution of the MPLS labels. No other label distribution protocol is needed between the two LSRs.

Exchanging IPv4 Routes with MPLS labels

Note This section is not applicable to Inter-AS over IP tunnels.

You can set up a VPN service provider network to exchange IPv4 routes with MPLS labels. You can configure the VPN service provider network as follows:

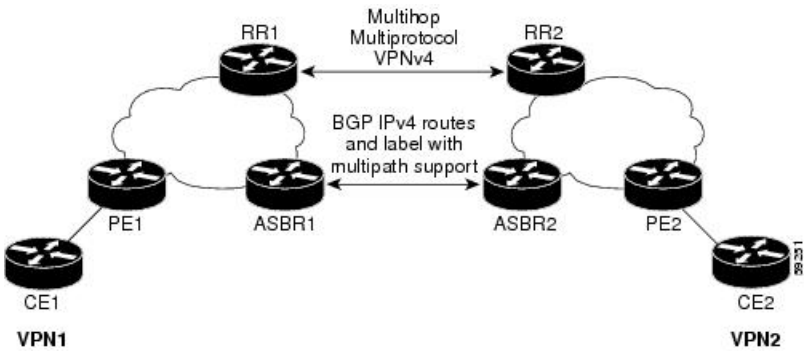
- Route reflectors exchange VPN-IPv4 routes by using multihop, multiprotocol eBGP. This configuration also preserves the next-hop information and the VPN labels across the autonomous systems.
- A local PE router (for example, PE1 in the figure below) needs to know the routes and label information for the remote PE router (PE2).

  This information can be exchanged between the PE routers and ASBRs in one of two ways:

  - Internal Gateway Protocol (IGP) and Label Distribution Protocol (LDP): The ASBR can redistribute the IPv4 routes and MPLS labels it learned from eBGP into IGP and LDP and from IGP and LDP into eBGP.
  - Internal Border Gateway Protocol (iBGP) IPv4 label distribution: The ASBR and PE router can use direct iBGP sessions to exchange VPN-IPv4 and IPv4 routes and MPLS labels.

Alternatively, the route reflector can reflect the IPv4 routes and MPLS labels learned from the ASBR to the PE routers in the VPN. This reflecting of learned IPv4 routes and MPLS labels is accomplished by enabling the ASBR to exchange IPv4 routes and MPLS labels with the route reflector. The route reflector also reflects the VPN-IPv4 routes to the PE routers in the VPN. For example, in VPN1, RR1 reflects to PE1 the VPN-IPv4 routes it learned and IPv4 routes and MPLS labels learned from ASBR1. Using the route reflectors to store the VPN-IPv4 routes and forward them through the PE routers and ASBRs allows for a scalable configuration.

Figure 3: VPNs Using eBGP and iBGP to Distribute Routes and MPLS Labels



BGP Routing Information

BGP routing information includes the following items:

- Network number (prefix), which is the IP address of the destination.
- Autonomous system (AS) path, which is a list of the other ASs through which a route passes on the way to the local router. The first AS in the list is closest to the local router; the last AS in the list is farthest from the local router and usually the AS where the route began.
- Path attributes, which provide other information about the AS path, for example, the next hop.

BGP Messages and MPLS Labels

MPLS labels are included in the update messages that a router sends. Routers exchange the following types of BGP messages:

- Open messages—After a router establishes a TCP connection with a neighboring router, the routers exchange open messages. This message contains the number of the autonomous system to which the router belongs and the IP address of the router that sent the message.
- Update messages—When a router has a new, changed, or broken route, it sends an update message to the neighboring router. This message contains the NLRI, which lists the IP addresses of the usable routes. The update message includes any routes that are no longer usable. The update message also includes path attributes and the lengths of both the usable and unusable paths. Labels for VPN-IPv4 routes are encoded in the update message, as specified in RFC 2858. The labels for the IPv4 routes are encoded in the update message, as specified in RFC 3107.
- Keepalive messages—Routers exchange keepalive messages to determine if a neighboring router is still available to exchange routing information. The router sends these messages at regular intervals. (Sixty seconds is the default for Cisco routers.) The keepalive message does not contain routing data; it contains only a message header.
- Notification messages—When a router detects an error, it sends a notification message.

Sending MPLS Labels with Routes

When BGP (eBGP and iBGP) distributes a route, it can also distribute an MPLS label that is mapped to that route. The MPLS label mapping information for the route is carried in the BGP update message that contains the information about the route. If the next hop is not changed, the label is preserved.

When you issue the **show bgp neighbors** *ip-address* command on both BGP routers, the routers advertise to each other that they can then send MPLS labels with the routes. If the routers successfully negotiate their ability to send MPLS labels, the routers add MPLS labels to all outgoing BGP updates.

Generic Routing Encapsulation Support for L3VPN

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate many types of packets to enable data transmission using a tunnel. The GRE tunneling protocol enables:

- High assurance Internet Protocol encryptor (HAIPE) devices for encryption over the public Internet and nonsecure connections.
- Service providers (that do not run MPLS in their core network) to provide VPN services along with the security services.

GRE is used with IP to create a virtual point-to-point link to routers at remote points in a network. For detailed information about configuring GRE tunnel interfaces, see the *Implementing Generic Routing Encapsulation* module of the *MPLS Layer 3 VPN Configuration Guide for Cisco ASR 9000 Series Routers*.

Note GRE is used with IP to create a virtual point-to-point link to routers at remote points in a network. For detailed information about configuring GRE tunnel interfaces, refer to the *Cisco IOS XR Interfaces and Hardware Components Configuration Guide*. For a PE to PE (core) link, enable LDP (with implicit null) on the GRE interfaces for L3VPN.

GRE Restriction for L3VPN

The following restrictions are applicable to L3VPN forwarding over GRE:

- Carrier Supporting Carrier (CsC) or Inter-AS is not supported.
- GRE-based L3VPN does not interwork with MPLS or IP VPNs.
- GRE tunnel is supported only as a core link(PE-PE, PE-P, P-P, P-PE). A PE-CE (edge) link is not supported.
- VPNv6 forwarding using GRE tunnels is not supported.

VPNv4 Forwarding Using GRE Tunnels

This section describes the working of VPNv4 forwarding over GRE tunnels. The following description assumes that GRE is used only as a core link between the encapsulation and decapsulation provider edge (PE) routers that are connected to one or more customer edge (CE) routers.

Ingress of Encapsulation Router

On receiving prefixes from the CE routers, Border Gateway Protocol (BGP) assigns the VPN label to the prefixes that need to be exported. These VPN prefixes are then forwarded to the Forwarding Information Base (FIB) using the Route Information Base (RIB) or the label switched database (LSD). The FIB then populates the prefix in the appropriate VRF table. The FIB also populates the label in the global label table. Using BGP, the prefixes are then relayed to the remote PE router (decapsulation router).

Egress of Encapsulation Router

The forwarding behavior on egress of the encapsulation PE router is similar to the MPLS VPN label imposition. Regardless of whether the VPN label imposition is performed on the ingress or egress side, the GRE tunnel forwards a packet that has an associated label. This labeled packet is then encapsulated with a GRE header and forwarded based on the IP header.

Ingress of Decapsulation Router

The decapsulation PE router learns the VPN prefixes and label information from the remote encapsulation PE router using BGP. The next-hop information for the VPN prefix is the address of the GRE tunnel interface connecting the two PE routers. BGP downloads these prefixes to the RIB. The RIB downloads the routes to the FIB and the FIB installs the routes in the hardware.

Egress of Decapsulation Router

The egress forwarding behavior on the decapsulation PE router is similar to VPN disposition and forwarding, based on the protocol type of the inner payload.

Carrier Supporting Carrier Support for L3VPN

This section provides conceptual information about MPLS VPN Carrier Supporting Carrier (CSC) functionality and includes the following topics:

- CSC Prerequisites
- CSC Benefits
- Configuration Options for the Backbone and Customer Carriers

Throughout this document, the following terminology is used in the context of CSC:

backbone carrier—Service provider that provides the segment of the backbone network to the other provider. A backbone carrier offers BGP and MPLS VPN services.

customer carrier—Service provider that uses the segment of the backbone network. The customer carrier may be an Internet service provider (ISP) or a BGP/MPLS VPN service provider.

CE router—A customer edge router is part of a customer network and interfaces to a provider edge (PE) router. In this document, the CE router sits on the edge of the customer carrier network.

PE router—A provider edge router is part of a service provider's network connected to a customer edge (CE) router. In this document, the PE router sits on the edge of the backbone carrier network

ASBR—An autonomous system boundary router connects one autonomous system to another.

CSC Prerequisites

The following prerequisites are required to configure CSC:

- You must be able to configure MPLS VPNs with end-to-end (CE-to-CE router) pings working.
- You must be able to configure Interior Gateway Protocols (IGPs), MPLS Label Distribution Protocol (LDP), and Multiprotocol Border Gateway Protocol (MP-BGP).
- You must ensure that CSC-PE and CSC-CE routers support BGP label distribution.

Note BGP is the only supported label distribution protocol on the link between CE and PE.

CSC Benefits

This section describes the benefits of CSC to the backbone carrier and customer carriers.

Benefits to the Backbone Carrier

- The backbone carrier can accommodate many customer carriers and give them access to its backbone.
- The MPLS VPN carrier supporting carrier feature is scalable.
- The MPLS VPN carrier supporting carrier feature is a flexible solution.

Benefits to the Customer Carriers

- The MPLS VPN carrier supporting carrier feature removes from the customer carrier the burden of configuring, operating, and maintaining its own backbone.
- Customer carriers who use the VPN services provided by the backbone carrier receive the same level of security that Frame Relay or ATM-based VPNs provide.
- Customer carriers can use any link layer technology to connect the CE routers to the PE routers .
- The customer carrier can use any addressing scheme and still be supported by a backbone carrier.

Benefits of Implementing MPLS VPN CSC Using BGP

The benefits of using BGP to distribute IPv4 routes and MPLS label routes are:

- BGP takes the place of an IGP and LDP in a VPN forwarding and routing instance (VRF) table.
- BGP is the preferred routing protocol for connecting two ISPs.

Configuration Options for the Backbone and Customer Carriers

To enable CSC, the backbone and customer carriers must be configured accordingly:

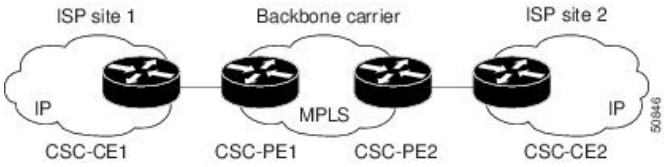
- The backbone carrier must offer BGP and MPLS VPN services.
- The customer carrier can take several networking forms. The customer carrier can be:
  - An ISP with an IP core (see the "Customer Carrier: ISP with IP Core").
  - An MPLS service provider with or without VPN services (see "Customer Carrier: MPLS Service Provider").

Note An IGP in the customer carrier network is used to distribute next hops and loopbacks to the CSC-CE. IBGP with label sessions are used in the customer carrier network to distribute next hops and loopbacks to the CSC-CE.

Customer Carrier: ISP with IP Core

The following figure shows a network configuration where the customer carrier is an ISP. The customer carrier has two sites, each of which is a point of presence (POP). The customer carrier connects these sites using a VPN service provided by the backbone carrier. The backbone carrier uses MPLS or IP tunnels to provide VPN services. The ISP sites use IP.

Figure 4: Network: Customer Carrier Is an ISP

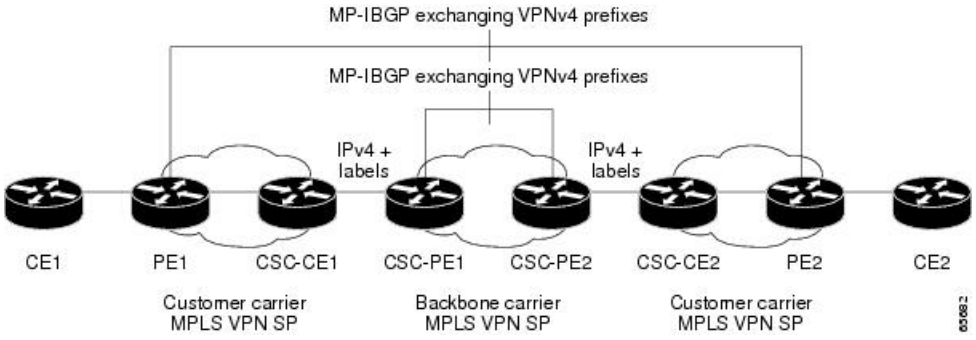


The links between the CE and PE routers use eBGP to distribute IPv4 routes and MPLS labels. Between the links, the PE routers use multiprotocol iBGP to distribute VPNv4 routes.

Customer Carrier: MPLS Service Provider

The following figure shows a network configuration where the backbone carrier and the customer carrier are BGP/MPLS VPN service providers. The customer carrier has two sites. The customer carrier uses MPLS in its network while the backbone carrier may use MPLS or IP tunnels in its network.

Figure 5: Network: Customer Carrier Is an MPLS VPN Service Provider



In Network: Customer Carrier Is an MPLS VPN Service Provider configuration, the customer carrier can configure its network in one of these ways:

- The customer carrier can run an IGP and LDP in its core network. In this case, the CSC-CE1 router in the customer carrier redistributes the eBGP routes it learns from the CSC-PE1 router of the backbone carrier to an IGP
- The CSC-CE1 router of the customer carrier system can run an IPv4 and labels iBGP session with the PE1 router.

LDP CSC IPv6

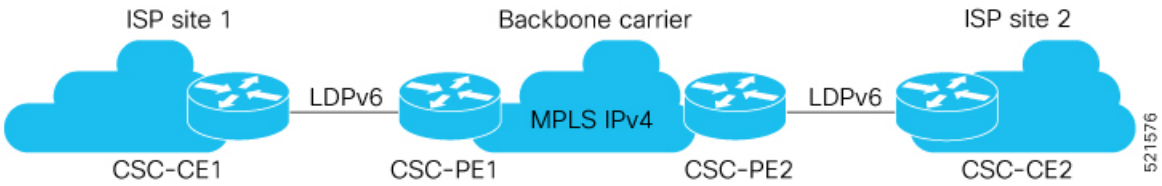
Table 1: Feature History Table

Feature Name	Release Information	Feature Description
LDP CSC IPv6	Release 7.4.1	The feature enables LDPv6 to run between CSC-PE and CSC-CE devices and carry IPv6 customer carrier traffic over the IPv4 backbone carrier network. LDP carries the labels that are exchanged in dedicated Virtual Private Network routing and forwarding (VRF) instances. IGP carries the routes between CSC-PE and CSC-CE routers.

IPv6 support for MPLS LDP enables the set up of label switched paths (LSPs) for IPv6 prefixes. This feature allows the IPv6 CSC-CE sites to communicate with each other over an MPLS IPv4 core network using MPLS LSPs. This feature enables the backbone carrier network running an MPLS IPv4 infrastructure to offer IPv6 services without any major changes in the infrastructure.

The topology shows two customers, CSC-CE1 and CSC-CE2, connecting their remote sites through the backbone carrier. The PE device of the backbone network connects with both customers through MPLS but under different VRFs according to interface-VRF mapping. The MPLS label distribution protocol for PE-CE connectivity is LDPv6 and requires them to run in a customer VRF context on the PE device.

Figure 6: LDP CSC IPv6



The links between the CE and PE routers use LDPv6 to distribute IPv6 routes and MPLS labels. The links between the PE routers use MPLS IPv4 network to distribute VPNv6 routes.

Configure LDP CSC IPv6

Perform the following tasks to configure LDP CSC IPv6.

- Configure LDPv6
- Configure BGP
- Configure ospfv3

Configuration Example

This section provides the configuration example.

```
/* CSC-PE1 Configuration */

/* Configure LDPv6 */
```

```
Router# configure
Router(config)# mpls ldp
Router(config-ldp)# vrf vpn2
Router(config-ldp-vrf)# router-id 10.0.0.1
Router(config-ldp-vrf)# address-family ipv6
Router(config-ldp-vrf-af)# discovery transport-address 10:10:10::1
Router(config-ldp-vrf-af)# exit
Router(config-ldp-vrf)# interface Bundle-Ether104.2
Router(config-ldp-vrf-if)# address-family ipv6
Router(config-ldp-vrf-if-af)# exit
Router(config-ldp-vrf-if)# exit
Router(config-ldp-vrf)# interface TenGigE0/0/0/12/3.2
Router(config-ldp-vrf-if)# address-family ipv6
Router(config-ldp-vrf-if-af)# commit

/* Configure BGP */
Router# configure
Router(config)# router bgp 100
Router(config-bgp)# nsr
Router(config-bgp)# bgp router-id 172.16.0.1
Router(config-bgp)# bgp redistribute-internal
Router(config-bgp)# bgp graceful-restart
Router(config-bgp)# bgp log neighbor changes detail
Router(config-bgp)# ibgp policy out enforce-modifications
Router(config-bgp)# address-family vpnv4 unicast
Router(config-bgp-af)# address-family vpnv6 unicast
Router(config-bgp-af)# neighbor-group vpn
Router(config-bgp-nbrgrp)# remote-as 100
Router(config-bgp-nbrgrp)# update-source Loopback0
Router(config-bgp-nbrgrp)# address-family vpnv4 unicast
Router(config-bgp-nbrgrp-af)# address-family vpnv6 unicast
Router(config-bgp-nbrgrp-af)# neighbor 192.168.0.1
Router(config-bgp-nbr)# use neighbor-group vpn
Router(config-bgp-nbr)# vrf vpn2
Router(config-bgp-vrf)# rd 1:2
Router(config-bgp-vrf)# address-family ipv4 unicast
Router(config-bgp-vrf-af)# exit
Router(config-bgp-vrf)# address-family ipv6 unicast
Router(config-bgp-vrf-af)# label mode per-prefix
Router(config-bgp-vrf-af)# maximum-paths ebgp 32
Router(config-bgp-vrf-af)# maximum-paths ibgp 32 unequal-cost
Router(config-bgp-vrf-af)# redistribute ospfv3 lab1 metric 19
Router(config-bgp-vrf-af)# commit

/* OSPF Configuration */
Router# configure
Router(config)# router ospfv3 LAB1
Router(config-ospfv3)# nsr
Router(config-ospfv3)# graceful-restart
Router(config-ospfv3)# vrf vpn2
Router(config-ospfv3-vrf)# mtu-ignore
Router(config-ospfv3-vrf)# graceful-restart
Router(config-ospfv3-vrf)# router-id 10.0.0.1
Router(config-ospfv3-vrf)# redistribute bgp 100 metric 19
Router(config-ospfv3-vrf)# area 0
Router(config-ospfv3-vrf-ar)# interface Loopback2
Router(config-ospfv3-vrf-ar-if)# passive
Router(config-ospfv3-vrf-ar-if)# interface Bundle-Ether104.2
Router(config-ospfv3-vrf-ar-if)# network point-to-point
Router(config-ospfv3-vrf-ar-if)# interface TenGigE0/0/0/12/3.2
Router(config-ospfv3-vrf-ar-if)# network point-to-point
Router(config-ospfv3-vrf-ar-if)# interface TenGigE0/1/0/7/3.2
```

```
Router(config-ospfv3-vrf-ar-if)# network point-to-point
Router(config-ospfv3-vrf-ar-if)# commit


/* CSC-CE1 Configuration */

/* Configure LDPv6 */
Router# configure
Router(config)# mpls ldp
Router(config-ldp)# vrf vpn2
Router(config-ldp-vrf)# router-id 209.165.201.1
Router(config-ldp-vrf)# address-family ipv6
Router(config-ldp-vrf-af)# discovery transport-address 209.165.201.1::1
Router(config-ldp-vrf-af)# exit
Router(config-ldp-vrf)# interface TenGigE0/3/0/29.2
Router(config-ldp-vrf-if)# address-family ipv6
Router(config-ldp-vrf-if-af)# exit
Router(config-ldp-vrf-if)# exit
Router(config-ldp-vrf)# interface Bundle-Ether104.2
Router(config-ldp-vrf-if)# address-family ipv6
Router(config-ldp-vrf-if-af)# commit

/* Configure BGP */
BGP configuration on CSC-CE is optional for LDP CSC IPv6 feature.
This configuration is required only if you want to run BGP between CSC-CEs.
Router# configure
Router(config)# router bgp 200
Router(config-bgp)# nsr
Router(config-bgp)# bgp router-id 209.165.201.2
Router(config-bgp)# bgp graceful-restart
Router(config-bgp)# bgp log neighbor changes detail
Router(config-bgp)# ibgp policy out enforce-modifications
Router(config-bgp)# address-family ipv6 unicast
Router(config-bgp-af)# address-family vpnv6 unicast
Router(config-bgp-af)# neighbor-group v6-csc
Router(config-bgp-nbrgrp)# remote-as 200
Router(config-bgp-nbrgrp)# address-family ipv6 unicast
Router(config-bgp-nbrgrp-af)# next-hop-self
Router(config-bgp-nbrgrp-af)# soft-reconfiguration inbound always
Router(config-bgp-nbrgrp-af)# neighbor-group v6-ixia
Router(config-bgp-nbrgrp)# remote-as 65001
Router(config-bgp-nbrgrp)# address-family ipv6 unicast
Router(config-bgp-nbrgrp-af)# route-policy pass in
Router(config-bgp-nbrgrp-af)# route-policy pass out
Router(config-bgp-nbrgrp-af)# as-override
Router(config-bgp-nbrgrp-af)# vrf vpn2
Router(config-bgp-vrf)# rd 4:2
Router(config-bgp-vrf)# address-family ipv6 unicast
Router(config-bgp-vrf-af)# label mode per-prefix
Router(config-bgp-vrf-af)# maximum-paths ibgp 8
Router(config-bgp-vrf-af)# neighbor 5:5:5::2
Router(config-bgp-vrf-nbr)# use neighbor-group v6-csc
Router(config-bgp-vrf-nbr)# update-source Loopback2
Router(config-bgp-vrf-nbr)# neighbor 104:1:1:2::2
Router(config-bgp-vrf-nbr)# use neighbor-group v6-ixia
Router(config-bgp-vrf-nbr)# commit


/* OSPF Configuration */
Router# configure
Router(config)# router ospfv3 LAB1
Router(config-ospfv3)# nsr
Router(config-ospfv3)# graceful-restart
```

```
Router(config-ospfv3)# vrf vpn2
Router(config-ospfv3-vrf)# mtu-ignore
Router(config-ospfv3-vrf)# graceful-restart
Router(config-ospfv3-vrf)# router-id 209.165.201.1
Router(config-ospfv3-vrf)# capability vrf-lite
Router(config-ospfv3-vrf)# area 0
Router(config-ospfv3-vrf-ar)# interface Loopback2
Router(config-ospfv3-vrf-ar-if)# passive
Router(config-ospfv3-vrf-ar-if)# interface Bundle-Ether104.2
Router(config-ospfv3-vrf-ar-if)# network point-to-point
Router(config-ospfv3-vrf-ar-if)# interface TenGigE0/3/0/29.2
Router(config-ospfv3-vrf-ar-if)# network point-to-point
Router(config-ospfv3-vrf-ar-if)# interface TenGigE0/3/0/18.2
Router(config-ospfv3-vrf-ar-if)# network point-to-point
Router(config-ospfv3-vrf-ar-if)# commit
```

Running Configuration

This section shows LDP CSC IPv6 running configuration

```
/* CSC-PE1 Configuration */

/* LDPv6 Configuration */
mpls ldp
 vrf vpn2
  router-id 10.0.0.1
  address-family ipv6
   discovery transport-address 10:10:10::1
  interface Bundle-Ether104.2
   address-family ipv6
interface TenGigE0/0/0/12/3.2
   address-family ipv6

/* BGP Configuration */
router bgp 100
 nsr
 bgp router-id 172.16.0.1
 bgp redistribute-internal
 bgp graceful-restart
 bgp log neighbor changes detail
 ibgp policy out enforce-modifications
 address-family vpnv4 unicast
 address-family vpnv6 unicast
neighbor-group vpn
  remote-as 100
  update-source Loopback0
  address-family vpnv4 unicast
  address-family vpnv6 unicast
neighbor 192.168.0.1
  use neighbor-group vpn
vrf vpn2
  rd 1:2
  address-family ipv4 unicast
  !
  address-family ipv6 unicast
   label mode per-prefix
   maximum-paths ebgp 32
   maximum-paths ibgp 32 unequal-cost
   redistribute ospfv3 lab1 metric 19

/* OSPF Configuration */
router ospfv3 lab1
```

```
 nsr
graceful-restart
vrf vpn2
  mtu-ignore
  graceful-restart
  router-id 1.1.1.2
  redistribute bgp 100 metric 19
  area 0
   interface Loopback2
    passive
  interface Bundle-Ether104.2
    network point-to-point
interface TenGigE0/0/0/12/3.2
    network point-to-point
interface TenGigE0/1/0/7/3.2
    network point-to-point


/* CSC-CE1 Configuration */

/* LDPv6 Configuration */
mpls ldp
 vrf vpn2
  router-id 209.165.201.1
  address-family ipv6
   discovery transport-address 209.165.201.1::2
  !
  interface TenGigE0/3/0/29.2
address-family ipv6
   !
  !
  interface Bundle-Ether104.2
   address-family ipv6
   !

/* BGP Configuration */
router bgp 200
 nsr
 bgp router-id 209.165.201.2
 bgp graceful-restart
 bgp log neighbor changes detail
 ibgp policy out enforce-modifications
 address-family ipv6 unicast
address-family vpnv6 unicast
neighbor-group v6-csc
  remote-as 200
  address-family ipv6 unicast
   next-hop-self
   soft-reconfiguration inbound always
neighbor-group v6-ixia
  remote-as 65001
  address-family ipv6 unicast
   route-policy pass in
   route-policy pass out
   as-override
vrf vpn2
  rd 4:2
  address-family ipv6 unicast
   label mode per-prefix
   maximum-paths ibgp 8
  neighbor 209.165.202.129::2
   use neighbor-group v6-csc
   update-source Loopback2
  neighbor 104:1:1:2::2
```

```
   use neighbor-group v6-ixia

/* OSPF Configuration */
router ospfv3 lab1
 nsr
 graceful-restart
 vrf vpn2
  graceful-restart
  router-id 4.4.1.2
  capability vrf-lite
  area 0
   interface Loopback2
    passive
   interface Bundle-Ether104.2
    network point-to-point
interface TenGigE0/3/0/29.2
    network point-to-point
interface TenGigE0/3/0/18.2
    network point-to-point
!
```

Verification

Verify the LDP CSC IPv6 configuration.

```
Router:CSC-PE1# show mpls ldp summary all
VRFs      : 254 (254 oper)
AFIs      : IPv4 (127), IPv6 (127)
Routes    : 9041 prefixes (789 ipv4, 8252 ipv6)
Bindings  : 68 prefixes (6 ipv4, 62 ipv6)
    Local     : 68 (6 ipv4, 62 ipv6)
    Remote    : 81 (6 ipv4, 75 ipv6)
Neighbors : 2000 (1 NSR, 1 GR)
Adj Groups: 2000
Hello Adj : 2255 (257 ipv4, 1998 ipv6)
Addresses : 3025 (390 ipv4, 2635 ipv6)
Interfaces: 2277 LDP configured (259 ipv4, 2018 ipv6)
            (4 auto-config)
Collaborators:
                     Connected  Registered
                     ---------  ------------------
    SysDB            Y          Y
    IM               Y          Y
    RSI              Y          -
    IP-ARM           Y          -
    IPv4-RIB         Y          Y (127/127 tables)
    IPv6-RIB         Y          Y (127/127 tables)

    LSD              Y          Y
    LDP-NSR-Partner  Y          -
    L2VPN-AToM       Y          -
    mLDP             -          N

Router:CSC-PE1# show mpls ldp vrf vpn2
parameters
LDP Parameters:
  Role: Active
  Protocol Version: 1
  RouDiscovery:
    Link Hellos:     Holdtime:15 sec, Interval:5 sec
    Targeted Hellos: Holdtime:90 sec, Interval:10 sec
    Quick-start: Enabled (by default)
    Transport address:
```

```
      IPv6: 1:1:1::2
Router ID: 1.1.1.2
  Null Label:
    IPv6: Implicit
  Session:
    Hold time: 180 sec
    Keepalive interval: 60 sec
    Backoff: Initial:15 sec, Maximum:120 sec
    Global MD5 password: Disabled
Graceful Restart:
    Enabled
    Reconnect Timeout:120 sec, Forwarding State Holdtime:180 sec
  NSR: Enabled, Sync-ed
  Timeouts:
    Housekeeping periodic timer: 10 sec
    Local binding: 300 sec
    Forwarding state in LSD: 360 sec
  Delay in AF Binding Withdrawl from peer: 180 sec
  Max:
    5000 interfaces (4000 attached, 1000 TE tunnel), 2000 peers
  OOR state
    Memory: Normal

Router:CSC-CE1# show mpls ldp vrf vpn2 ipv6 discovery detail
Local LDP Identifier: 209.165.201.1:0
Discovery Sources:
  Interfaces:
    Bundle-Ether104.2 (0x41e0) : xmit/recv
      VRF: 'vpn2' (0x60000004)
      Source address: fe80::226:51ff:fecc:6762; Transport address: 209.165.201.1::2
      Hello interval: 5 sec (due in 4.2 sec)
      Quick-start: Enabled
      LDP Id: 10.0.0.1:0
          Source address: fe80::72e4:22ff:fe57:209e; Transport address: 10:10:10::1
          Hold time: 15 sec (local:15 sec, peer:15 sec)
                     (expiring in 14.8 sec)
          Established: Apr  5 14:18:22.000 (1d01h ago)
          Last session connection failures:
             Apr  5 15:08:55.074: TCP connection closed
                 (Last up for 00:50:02)
Apr  5 15:08:55.074: TCP connection closed
                 (Last up for 00:50:02)
TenGigE0/3/0/29.2 (0xa007880) : xmit/recv
      VRF: 'vpn2' (0x60000004)
      Source address: fe80::2a7:42ff:fe56:fc75; Transport address: 09.165.201.1::2
      Hello interval: 5 sec (due in 977 msec)
      Quick-start: Enabled
      LDP Id: 1.1.1.2:0
          Source address: fe80::822d:bfff:fe17:e9b3; Transport address: 10:10:10::1
          Hold time: 15 sec (local:15 sec, peer:15 sec)
                     (expiring in 13.1 sec)
          Established: Apr  5 14:18:19.731 (1d01h ago)
          Last session connection failures:
             Apr  5 15:08:55.074: TCP connection closed
                 (Last up for 00:50:02)
```

How to Implement MPLS Layer 3 VPNs

This section contains instructions for the following tasks:

Configuring the Core Network

Configuring the core network includes the following tasks:

Assessing the Needs of MPLS VPN Customers

Before configuring an MPLS VPN, the core network topology must be identified so that it can best serve MPLS VPN customers. Perform this task to identify the core network topology.

SUMMARY STEPS

1. Identify the size of the network.
2. Identify the routing protocols in the core.
3. Determine if MPLS High Availability support is required.
4. Determine if BGP load sharing and redundant paths are required.

DETAILED STEPS

Procedure

Step 1 Identify the size of the network.

Identify the following to determine the number of routers and ports required:

- How many customers will be supported?
- How many VPNs are required for each customer?
- How many virtual routing and forwarding (VRF) instances are there for each VPN?

Step 2 Identify the routing protocols in the core.

Determine which routing protocols are required in the core network.

Step 3 Determine if MPLS High Availability support is required.

MPLS VPN nonstop forwarding and graceful restart are supported on select routers and Cisco IOS XR software releases.

Step 4 Determine if BGP load sharing and redundant paths are required.

Determine if BGP load sharing and redundant paths in the MPLS VPN core are required.

Configuring Routing Protocols in the Core

To configure a routing protocol, see the *Routing Configuration Guide for Cisco ASR 9000 Series Routers*.

Configuring MPLS in the Core

To enable MPLS on all routers in the core, you must configure a Label Distribution Protocol (LDP). You can use either of the following as an LDP:

- MPLS LDP—See the *Implementing MPLS Label Distribution Protocol* chapter in the *MPLS Configuration Guide for Cisco ASR 9000 Series Routers* for configuration information.

- MPLS Traffic Engineering Resource Reservation Protocol (RSVP)—See *Implementing RSVP for MPLS-TE* module in the *MPLS Configuration Guide for Cisco ASR 9000 Series Routers* for configuration information.

Determining if FIB Is Enabled in the Core

Forwarding Information Base (FIB) must be enabled on all routers in the core, including the provider edge (PE) routers. For information on how to determine if FIB is enabled, see the *Implementing Cisco Express Forwarding* module in the *IP Addresses and Services Configuration Guide for Cisco ASR 9000 Series Routers*.

Configuring Multiprotocol BGP on the PE Routers and Route Reflectors

Perform this task to configure multiprotocol BGP (MP-BGP) connectivity on the PE routers and route reflectors.

SUMMARY STEPS

1. **configure**
2. **router bgp** *autonomous-system-number*
3. **address-family vpnv4 unicast** or **address-family vpnv6 unicast**
4. **neighbor** *ip-address* **remote-as** *autonomous-system-number*
5. **address-family vpnv4 unicast** or **address-family vpnv6 unicast**
6. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

Step 1 **configure**

Example:

```
RP/0/RSP0/CPU0:router# configure
```

Enters the Global Configuration mode.

Step 2 **router bgp** *autonomous-system-number*

Example:

```
RP/0/RSP0/CPU0:router(config)# router bgp 120
```

Enters BGP configuration mode allowing you to configure the BGP routing process.

Step 3 **address-family vpnv4 unicast** or **address-family vpnv6 unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp)# address-family vpnv4 unicast
```

Enters VPNv4 or VPNv6 address family configuration mode for the VPNv4 or VPNv6 address family.

Step 4 **neighbor** *ip-address* **remote-as** *autonomous-system-number*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp)# neighbor 172.168.40.24 remote-as 2002
```

Creates a neighbor and assigns it a remote autonomous system number.

Step 5 **address-family vpnv4 unicast** or **address-family vpnv6 unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family vpnv4 unicast
```

Enters VPNv4 or VPNv6 address family configuration mode for the VPNv4 or VPNv6 address family.

Step 6 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Connecting MPLS VPN Customers

To connect MPLS VPN customers to the VPN, perform the following tasks:

Defining VRFs on the PE Routers to Enable Customer Connectivity

Perform this task to define VPN routing and forwarding (VRF) instances.

SUMMARY STEPS

1. **configure**
2. **vrf** *vrf-name*
3. **address-family ipv4 unicast**
4. **import route-policy** *policy-name*
5. **import route-target** [*as-number:nn* | *ip-address:nn*]
6. **export route-policy** *policy-name*
7. **export route-target** [*as-number:nn* | *ip-address:nn*]
8. **exit**
9. **exit**
10. **router bgp** *autonomous-system-number*
11. **vrf** *vrf-name*
12. **rd** { *as-number* | *ip-address* | **auto** }
13. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

Step 1 **configure**

Example:

```
RP/0/RSP0/CPU0:router# configure
```

Enters Global Configuration mode.

Step 2 **vrf** *vrf-name*

Example:

```
RP/0/RSP0/CPU0:router(config)# vrf vrf_1
```

Configures a VRF instance and enters VRF configuration mode.

Step 3 **address-family ipv4 unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-vrf)# address-family ipv4 unicast
```

Enters VRF address family configuration mode for the IPv4 address family.

Step 4 **import route-policy** *policy-name*

Example:

```
RP/0/RSP0/CPU0:router(config-vrf-af)# import route-policy policy_A
```

Specifies a route policy that can be imported into the local VPN.

Step 5 **import route-target** [*as-number:nn* | *ip-address:nn*]

Example:

```
RP/0/RSP0/CPU0:router(config-vrf-af)# import route-target 120:1
```

Allows exported VPN routes to be imported into the VPN if one of the route targets of the exported route matches one of the local VPN import route targets.

Step 6 **export route-policy** *policy-name*

Example:

```
RP/0/RSP0/CPU0:router(config-vrf-af)# export route-policy policy_B
```

Specifies a route policy that can be exported from the local VPN.

Step 7 **export route-target** [*as-number:nn* | *ip-address:nn*]

Example:

```
RP/0/RSP0/CPU0:router(config-vrf-af)# export route-target 120:2
```

Associates the local VPN with a route target. When the route is advertised to other provider edge (PE) routers, the export route target is sent along with the route as an extended community.

Step 8 **exit**

Example:

```
RP/0/RSP0/CPU0:router(config-vrf-af)# exit
```

Exits VRF address family configuration mode and returns the router to VRF configuration mode.

Step 9 **exit**

Example:

```
RP/0/RSP0/CPU0:router(config-vrf)# exit
```

Exits VRF configuration mode and returns the router to Global Configuration mode.

Step 10 **router bgp** *autonomous-system-number*

Example:

```
RP/0/RSP0/CPU0:router(config)# router bgp 120
```

Enters BGP configuration mode allowing you to configure the BGP routing process.

Step 11 **vrf** *vrf-name*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp)# vrf vrf_1
```

Configures a VRF instance and enters VRF configuration mode for BGP routing.

Step 12 **rd** { *as-number* | *ip-address* | **auto** }

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-vrf)# rd auto
```

Automatically assigns a unique route distinguisher (RD) to vrf_1.

Step 13 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.

- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Configuring VRF Interfaces on PE Routers for Each VPN Customer

Perform this task to associate a VPN routing and forwarding (VRF) instance with an interface or a subinterface on the PE routers.

Note You must remove IPv4/IPv6 addresses from an interface prior to assigning, removing, or changing an interface's VRF. If this is not done in advance, any attempt to change the VRF on an IP interface is rejected.

SUMMARY STEPS

1. **configure**
2. **interface** *type interface-path-id*
3. **vrf** *vrf-name*
4. **ipv4 address** *ipv4-address mask*
5. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

Step 1 **configure**

Example:

```
RP/0/RSP0/CPU0:router# configure
```

Enters Global Configuration mode.

Step 2 **interface** *type interface-path-id*

Example:

```
RP/0/RSP0/CPU0:router(config)# interface TenGigE 0/3/0/0
```

Enters interface configuration mode.

Step 3 **vrf** *vrf-name*

Example:

```
RP/0/RSP0/CPU0:router(config-if)# vrf vrf_A
```

Configures a VRF instance and enters VRF configuration mode.

Step 4 **ipv4 address** *ipv4-address mask*

Example:

```
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 192.168.1.27 255.255.255.0
```

Configures a primary IPv4 address for the specified interface.

Step 5 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Configuring BGP as the Routing Protocol Between the PE and CE Routers

Perform this task to configure PE-to-CE routing sessions using BGP.

SUMMARY STEPS

1. **configure**
2. **router bgp** *autonomous-system-number*
3. **bgp router-id** {*ip-address*}
4. **vrf** *vrf-name*
5. **address-family ipv4 unicast**
6. **label mode** *per-ce*
7. Do one of the following:
   - **redistribute connected** [**metric** *metric-value*] [**route-policy** *route-policy-name*]
   - **redistribute isis** *process-id* [**level** {**1** | **1-inter-area** | **2** }] [**metric** *metric-value*] [**route-policy** *route-policy-name*]
   - **redistribute ospf** *process-id* [**match** { **external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] }] [**metric** *metric-value*] [**route-policy** *route-policy-name*]
   - **redistribute static** [**metric** *metric-value*] [**route-policy** *route-policy-name*]
8. **aggregate-address** *address/mask-length* [**as-set**] [**as-confed-set**] [**summary-only**] [**route-policy** *route-policy-name*]
9. **network** {*ip-address/prefix-length* | *ip-address mask* } [**route-policy** *route-policy-name*]
10. **exit**
11. **neighbor** *ip-address*
12. **remote-as** *autonomous-system-number*
13. **password** { **clear** | **encrypted** } *password*
14. **ebgp-multihop** [*ttl-value*]
15. **address-family ipv4 unicast**
16. **allowas-in** [*as-occurrence-number*]

17. **route-policy** *route-policy-name* **in**
18. **route-policy** *route-policy-name* **out**
19. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

Step 1 **configure**

Example:

```
RP/0/RSP0/CPU0:router# configure
```

Enters Global Configuration mode.

Step 2 **router bgp** *autonomous-system-number*

Example:

```
RP/0/RSP0/CPU0:router(config)# router bgp 120
```

Enters Border Gateway Protocol (BGP) configuration mode allowing you to configure the BGP routing process.

Step 3 **bgp router-id** {*ip-address*}

Example:

```
RP/0/RSP0/CPU0:router(config-bgp)# bgp router-id 192.168.70.24
```

Configures the local router with a router ID of 192.168.70.24.

Step 4 **vrf** *vrf-name*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp)# vrf vrf_1
```

Configures a VPN routing and forwarding (VRF) instance and enters VRF configuration mode for BGP routing.

Step 5 **address-family ipv4 unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-vrf)# address-family ipv4 unicast
```

Enters VRF address family configuration mode for the IPv4 address family.

Step 6 **label mode** *per-ce*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-vrf-af)# label mode per-ce
```

Sets the MPLS VPN label allocation mode for each customer edge (CE) label mode allowing the provider edge (PE) router to allocate one label for every immediate next-hop.

You can configure **label mode** *per-vrf* and *per-prefix*, and from Release 24.1.1, you can configure *per-vrf-46*. For more information, see the label mode command in the *Routing Command Reference for Cisco ASR 9000 Series Routers*.

Step 7 Do one of the following:

- **redistribute connected** [**metric** *metric-value*] [**route-policy** *route-policy-name*]
- **redistribute isis** *process-id* [**level** {**1** | **1-inter-area** | **2** }] [**metric** *metric-value*] [**route-policy** *route-policy-name*]
- **redistribute ospf** *process-id* [**match** { **external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] }] [**metric** *metric-value*] [**route-policy** *route-policy-name*]
- **redistribute static** [**metric** *metric-value*] [**route-policy** *route-policy-name*]

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-vrf-af)# redistribute connected
```

Causes routes to be redistributed into BGP. The routes that can be redistributed into BGP are:

- Connected
- Intermediate System-to-Intermediate System (IS-IS)
- Open Shortest Path First (OSPF)
- Static

Step 8 **aggregate-address** *address/mask-length* [**as-set**] [**as-confed-set**] [**summary-only**] [**route-policy** *route-policy-name*]

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-vrf-af)# aggregate-address 10.0.0.0/8 as-set
```

Creates an aggregate address. The path advertised for this route is an autonomous system set consisting of all elements contained in all paths that are being summarized.

- The **as-set** keyword generates autonomous system set path information and community information from contributing paths.
- The **as-confed-set** keyword generates autonomous system confederation set path information from contributing paths.
- The **summary-only** keyword filters all more specific routes from updates.
- The **route-policy** *route-policy-name* keyword and argument specify the route policy used to set the attributes of the aggregate route.

Step 9 **network** {*ip-address/prefix-length* | *ip-address mask* } [**route-policy** *route-policy-name*]

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-vrf-af)# network 172.20.0.0/16
```

Configures the local router to originate and advertise the specified network.

Step 10 **exit**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-vrf-af)# exit
```

Exits VRF address family configuration mode and returns the router to VRF configuration mode for BGP routing.

Step 11 **neighbor** *ip-address*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-vrf)# neighbor 172.168.40.24
```

Places the router in VRF neighbor configuration mode for BGP routing and configures the neighbor IP address 172.168.40.24 as a BGP peer.

Step 12 **remote-as** *autonomous-system-number*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr)# remote-as 2002
```

Creates a neighbor and assigns it a remote autonomous system number.

Step 13 **password** { **clear** | **encrypted** } *password*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr)# password clear pswd123
```

Configures neighbor 172.168.40.24 to use MD5 authentication with the password pswd123.

Step 14 **ebgp-multihop** [*ttl-value*]

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr)# ebgp-multihop
```

Allows a BGP connection to neighbor 172.168.40.24.

Step 15 **address-family ipv4 unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr)# address-family ipv4 unicast
```

Enters VRF neighbor address family configuration mode for BGP routing.

Step 16 **allowas-in** [*as-occurrence-number*]

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr-af)# allowas-in 3
```

Replaces the neighbor autonomous system number (ASN) with the PE ASN in the AS path three times.

Step 17 **route-policy** *route-policy-name* **in**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr-af)# route-policy In-Ipv4 in
```

Applies the In-Ipv4 policy to inbound IPv4 unicast routes.

Step 18 **route-policy** *route-policy-name* **out**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-vrf-nbr-af)# route-policy In-Ipv4 in
```

Applies the In-Ipv4 policy to outbound IPv4 unicast routes.

Step 19 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Configuring RIPv2 as the Routing Protocol Between the PE and CE Routers

Perform this task to configure provider edge (PE)-to-customer edge (CE) routing sessions using Routing Information Protocol version 2 (RIPv2).

SUMMARY STEPS

1. **configure**
2. **router rip**
3. **vrf** *vrf-name*
4. **interface** *type instance*
5. **site-of-origin** { *as-number : number* | *ip-address : number* }
6. **exit**
7. Do one of the following:
   - **redistribute bgp** *as-number* [[**external** | **internal** | **local**] [**route-policy** *name*]
   - **redistribute connected** [**route-policy** *name*]
   - **redistribute isis** *process-id* [**level-1** | **level-1-2** | **level-2**] [**route-policy** *name*]
   - **redistribute eigrp** *as-number* [**route-policy** *name*]
   - **redistribute ospf** *process-id* [**match** { **external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] }] [**route-policy** *name*]
   - **redistribute static** [**route-policy** *name*]

8. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

Step 1 **configure**

Example:

```
RP/0/RSP0/CPU0:router# configure
```

Enters Global Configuration mode.

Step 2 **router rip**

Example:

```
RP/0/RSP0/CPU0:router(config)# router rip
```

Enters the Routing Information Protocol (RIP) configuration mode allowing you to configure the RIP routing process.

Step 3 **vrf** *vrf-name*

Example:

```
RP/0/RSP0/CPU0:router(config-rip)# vrf vrf_1
```

Configures a VPN routing and forwarding (VRF) instance and enters VRF configuration mode for RIP routing.

Step 4 **interface** *type instance*

Example:

```
RP/0/RSP0/CPU0:router(config-rip-vrf)# interface TenGigE 0/3/0/0
```

Enters VRF interface configuration mode.

Step 5 **site-of-origin** { *as-number : number* | *ip-address : number* }

Example:

```
RP/0/RSP0/CPU0:router(config-rip-vrf-if)# site-of-origin 200:1
```

Identifies routes that have originated from a site so that the re-advertisement of that prefix back to the source site can be prevented. Uniquely identifies the site from which a PE router has learned a route.

Step 6 **exit**

Example:

```
RP/0/RSP0/CPU0:router(config-rip-vrf-if)# exit
```

Exits VRF interface configuration mode, and returns the router to VRF configuration mode for RIP routing.

Step 7 Do one of the following:

- **redistribute bgp** *as-number* [[**external** | **internal** | **local**] [**route-policy** *name*]
- **redistribute connected** [**route-policy** *name*]
- **redistribute isis** *process-id* [**level-1** | **level-1-2** | **level-2**] [**route-policy** *name*]
- **redistribute eigrp** *as-number* [**route-policy** *name*]
- **redistribute ospf** *process-id* [**match** { **external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] }] [**route-policy** *name*]
- **redistribute static** [**route-policy** *name*]

Example:

```
RP/0/RSP0/CPU0:router(config-rip-vrf)# redistribute connected
```

Causes routes to be redistributed into RIP. The routes that can be redistributed into RIP are:

- Border Gateway Protocol (BGP)
- Connected
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Intermediate System-to-Intermediate System (IS-IS)
- Open Shortest Path First (OSPF)
- Static

Step 8 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Configuring Static Routes Between the PE and CE Routers

Perform this task to configure provider edge (PE)-to-customer edge (CE) routing sessions that use static routes.

Note You must remove IPv4/IPv6 addresses from an interface prior to assigning, removing, or changing an interface's VRF. If this is not done in advance, any attempt to change the VRF on an IP interface is rejected.

SUMMARY STEPS

1. **configure**
2. **router static**

3. **vrf** *vrf-name*
4. **address-family ipv4 unicast**
5. *prefix/mask* [**vrf** *vrf-name*] { *ip-address* | *type interface-path-id* }
6. *prefix/mask* [**vrf** *vrf-name*] **bfd fast-detect**
7. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

Step 1 **configure**

Example:

```
RP/0/RSP0/CPU0:router# configure
```

Enters Global Configuration mode.

Step 2 **router static**

Example:

```
RP/0/RSP0/CPU0:router(config)# router static
```

Enters static routing configuration mode allowing you to configure the static routing process.

Step 3 **vrf** *vrf-name*

Example:

```
RP/0/RSP0/CPU0:router(config-static)# vrf vrf_1
```

Configures a VPN routing and forwarding (VRF) instance and enters VRF configuration mode for static routing.

Step 4 **address-family ipv4 unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-static-vrf)# address-family ipv4 unicast
```

Enters VRF address family configuration mode for the IPv4 address family.

Step 5 *prefix/mask* [**vrf** *vrf-name*] { *ip-address* | *type interface-path-id* }

Example:

```
RP/0/RSP0/CPU0:router(config-static-vrf-afi)# 172.168.40.24/24 vrf vrf_1 10.1.1.1
```

Assigns the static route to vrf_1.

Step 6 *prefix/mask* [**vrf** *vrf-name*] **bfd fast-detect**

Example:

```
RP/0/RSP0/CPU0:router(config-static-vrf-afi)# 172.168.40.24/24 vrf vrf_1 bfd fast-detect
```

Enables bidirectional forwarding detection (BFD) to detect failures in the path between adjacent forwarding engines.

This option is available is when the forwarding router address is specified in Step 5 .

Step 7 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Configuring OSPF as the Routing Protocol Between the PE and CE Routers

Perform this task to configure provider edge (PE)-to-customer edge (CE) routing sessions that use Open Shortest Path First (OSPF).

SUMMARY STEPS

1. **configure**
2. **router ospf** *process-name*
3. **vrf** *vrf-name*
4. **router-id** {*router-id* | type interface-path-id}
5. Do one of the following:
   - **redistribute bgp** *process-id* [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
   - **redistribute connected** [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
   - **redistribute ospf** *process-id* [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]}] [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
   - **redistribute static** [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
   - **redistribute eigrp** *process-id* [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]]} [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
   - **redistribute rip** [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
6. **area** *area-id*
7. **interface** type interface-path-id
8. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

Step 1 **configure**

Example:

```
RP/0/RSP0/CPU0:router# configure
```

Enters Global Configuration mode.

Step 2 **router ospf** *process-name*

Example:

```
RP/0/RSP0/CPU0:router(config)# router ospf 109
```

Enters OSPF configuration mode allowing you to configure the OSPF routing process.

Step 3 **vrf** *vrf-name*

Example:

```
RP/0/RSP0/CPU0:router(config-ospf)# vrf vrf_1
```

Configures a VPN routing and forwarding (VRF) instance and enters VRF configuration mode for OSPF routing.

Step 4 **router-id** {*router-id* | type interface-path-id}

Example:

```
RP/0/RSP0/CPU0:router(config-ospf-vrf)# router-id 172.20.10.10
```

Configures the router ID for the OSPF routing process.

Step 5 Do one of the following:

- **redistribute bgp** *process-id* [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
- **redistribute connected** [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
- **redistribute ospf** *process-id* [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]}] [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
- **redistribute static** [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
- **redistribute eigrp** *process-id* [**match** {**external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**]]} [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]
- **redistribute rip** [**metric** *metric-value*] [**metric-type** {**1** | **2**}] [**route-policy** *policy-name*] [**tag** *tag-value*]

Example:

```
RP/0/RSP0/CPU0:router(config-ospf-vrf)# redistribute connected
```

Causes routes to be redistributed into OSPF. The routes that can be redistributed into OSPF are:

- Border Gateway Protocol (BGP)
- Connected
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- OSPF
- Static
- Routing Information Protocol (RIP)

Step 6 **area** *area-id*

Example:

```
RP/0/RSP0/CPU0:router(config-ospf-vrf)# area 0
```

Configures the OSPF area as area 0.

Step 7 **interface** type interface-path-id

Example:

```
RP/0/RSP0/CPU0:router(config-ospf-vrf-ar)# interface TenGigE 0/3/0/0
```

Associates interface TenGigE 0/3/0/0 with area 0.

Step 8 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Configuring EIGRP as the Routing Protocol Between the PE and CE Routers

Perform this task to configure provider edge (PE)-to-customer edge (CE) routing sessions that use Enhanced Interior Gateway Routing Protocol (EIGRP).

Using EIGRP between the PE and CE routers allows you to transparently connect EIGRP customer networks through an MPLS-enable Border Gateway Protocol (BGP) core network so that EIGRP routes are redistributed through the VPN across the BGP network as internal BGP (iBGP) routes.

Before you begin

BGP is configured in the network. See the *Implementing BGP* module in the *Routing Configuration Guide for Cisco ASR 9000 Series Routers*

Note You must remove IPv4/IPv6 addresses from an interface prior to assigning, removing, or changing an interface's VRF. If this is not done in advance, any attempt to change the VRF on an IP interface is rejected.

SUMMARY STEPS

1. **configure**
2. **router eigrp** *as-number*
3. **vrf** *vrf-name*
4. **address-family ipv4**
5. **router-id** *router-id*
6. **autonomous-system** *as-number*
7. **default-metric** *bandwidth delay reliability loading mtu*
8. **redistribute** { { **bgp** | **connected** | **isis** | **ospf** | **rip** | **static** } [*as-number* | *instance-name*] } [**route-policy** *name*]
9. **interface** *type interface-path-id*
10. **site-of-origin** { *as-number:number* | *ip-address : number* }
11. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

Step 1 **configure**

Example:

```
RP/0/RSP0/CPU0:router# configure
```

Enters Global Configuration mode.

Step 2 **router eigrp** *as-number*

Example:

```
RP/0/RSP0/CPU0:router(config)# router eigrp 24
```

Enters EIGRP configuration mode allowing you to configure the EIGRP routing process.

Step 3 **vrf** *vrf-name*

Example:

```
RP/0/RSP0/CPU0:router(config-eigrp)# vrf vrf_1
```

Configures a VPN routing and forwarding (VRF) instance and enters VRF configuration mode for EIGRP routing.

Step 4 **address-family ipv4**

Example:

```
RP/0/RSP0/CPU0:router(config-eigrp-vrf)# address family ipv4
```

Enters VRF address family configuration mode for the IPv4 address family.

Step 5 **router-id** *router-id*

Example:

```
RP/0/RSP0/CPU0:router(config-eigrp-vrf-af)# router-id 172.20.0.0
```

Configures the router ID for the Enhanced Interior Gateway Routing Protocol (EIGRP) routing process.

Step 6 **autonomous-system** *as-number*

Example:

```
RP/0/RSP0/CPU0:router(config-eigrp-vrf-af)# autonomous-system 6
```

Configures the EIGRP routing process to run within a VRF.

Step 7 **default-metric** *bandwidth delay reliability loading mtu*

Example:

```
RP/0/RSP0/CPU0:router(config-eigrp-vrf-af)# default-metric 100000 4000 200 45 4470
```

Sets the metrics for an EIGRP.

Step 8 **redistribute** { { **bgp** | **connected** | **isis** | **ospf** | **rip** | **static** } [*as-number* | *instance-name*] } [**route-policy** *name*]

Example:

```
RP/0/RSP0/CPU0:router(config-eigrp-vrf-af)# redistribute connected
```

Causes connected routes to be redistributed into EIGRP.

Step 9 **interface** *type interface-path-id*

Example:

```
RP/0/RSP0/CPU0:router(config-eigrp-vrf-af)# interface TenGigE 0/3/0/0
```

Associates interface TenGigE 0/3/0/0 with the EIGRP routing process.

Step 10 **site-of-origin** { *as-number:number* | *ip-address : number* }

Example:

```
RP/0/RSP0/CPU0:router(config-eigrp-vrf-af-if)# site-of-origin 201:1
```

Configures site of origin (SoO) on interface TenGigE 0/3/0/0.

Step 11 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.

- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Configuring EIGRP Redistribution in the MPLS VPN

Perform this task for every provider edge (PE) router that provides VPN services to enable Enhanced Interior Gateway Routing Protocol (EIGRP) redistribution in the MPLS VPN.

Before you begin

The metric can be configured in the route-policy configuring using the **redistribute** command (or configured with the **default-metric** command). If an external route is received from another EIGRP autonomous system or a non-EIGRP network without a configured metric, the route is not installed in the EIGRP database. If an external route is received from another EIGRP autonomous system or a non-EIGRP network without a configured metric, the route is not advertised to the CE router. See the *Implementing EIGRP*module in the *Routing Configuration Guide for Cisco ASR 9000 Series Routers*.

Restriction Redistribution between native EIGRP VPN routing and forwarding (VRF) instances is not supported. This behavior is designed.

SUMMARY STEPS

1. **configure**
2. **router eigrp** *as-number*
3. **vrf** *vrf-name*
4. **address-family ipv4**
5. **redistribute bgp** [*as-number*] [**route-policy** *policy-name*]
6. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

Step 1 **configure**

Example:

```
RP/0/RSP0/CPU0:router# configure
```

Enters Global Configuration mode.

Step 2 **router eigrp** *as-number*

Example:

```
RP/0/RSP0/CPU0:router(config)# router eigrp 24
```

Enters EIGRP configuration mode allowing you to configure the EIGRP routing process.

Step 3 **vrf** *vrf-name*

Example:

```
RP/0/RSP0/CPU0:router(config-eigrp)# vrf vrf_1
```

Configures a VRF instance and enters VRF configuration mode for EIGRP routing.

Step 4 **address-family ipv4**

Example:

```
RP/0/RSP0/CPU0:router(config-eigrp-vrf)# address family ipv4
```

Enters VRF address family configuration mode for the IPv4 address family.

Step 5 **redistribute bgp** [*as-number*] [**route-policy** *policy-name*]

Example:

```
RP/0/RSP0/CPU0:router(config-eigrp-vrf-af)# redistribute bgp 24 route-policy policy_A
```

Causes Border Gateway Protocol (BGP) routes to be redistributed into EIGRP.

Step 6 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Providing VPN Connectivity Across Multiple Autonomous Systems with MPLS VPN Inter-AS with ASBRs Exchanging IPv4 Routes and MPLS Labels

Note This section is not applicable to Inter-AS over IP tunnels.

This section contains instructions for the following tasks:

Configuring ASBRs to Exchange IPv4 Routes and MPLS Labels

Perform this task to configure the autonomous system boundary routers (ASBRs) to exchange IPv4 routes and MPLS labels.

SUMMARY STEPS

1. **configure**
2. **router bgp** *autonomous-system-number*
3. **address-family ipv4 unicast**
4. **allocate-label all**
5. **neighbor** *ip-address*
6. **remote-as** *autonomous-system-number*
7. **address-family ipv4 labeled-unicast**
8. **route-policy** *route-policy-name* **in**
9. **route-policy** *route-policy-name* **out**
10. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

Step 1 **configure**

Example:

```
RP/0/RSP0/CPU0:router# configure
```

Enters Global Configuration mode.

Step 2 **router bgp** *autonomous-system-number*

Example:

```
RP/0/RSP0/CPU0:router(config)# router bgp 120
RP/0/RSP0/CPU0:router(config-bgp)#
```

Enters Border Gateway Protocol (BGP) configuration mode allowing you to configure the BGP routing process.

Step 3 **address-family ipv4 unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp)# address-family ipv4 unicast
RP/0/RSP0/CPU0:router(config-bgp-af)#
```

Enters global address family configuration mode for the IPv4 unicast address family.

Step 4 **allocate-label all**

Example:

```
RP/0/CPU0:router(config-bgp-af)# allocate-label all
```

Allocates the MPLS labels for a specific IPv4 unicast or VPN routing and forwarding (VRF) IPv4 unicast routes so that the BGP router can send labels with BGP routes to a neighboring router that is configured for a labeled-unicast session.

Step 5 **neighbor** *ip-address*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-af)# neighbor 172.168.40.24

RP/0/RSP0/CPU0:router(config-bgp-nbr)#
```

Places the router in neighbor configuration mode for BGP routing and configures the neighbor IP address 172.168.40.24 as a BGP peer.

Step 6 **remote-as** *autonomous-system-number*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 2002
```

Creates a neighbor and assigns it a remote autonomous system number.

Step 7 **address-family ipv4 labeled-unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family ipv4 labeled-unicast
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)
```

Enters neighbor address family configuration mode for the IPv4 labeled-unicast address family.

Step 8 **route-policy** *route-policy-name* **in**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-policy pass-all in
```

Applies a routing policy to updates that are received from a BGP neighbor.

- Use the *route-policy-name* argument to define the name of the of route policy. The example shows that the route policy name is defined as pass-all.
- Use the **in** keyword to define the policy for inbound routes.

Step 9 **route-policy** *route-policy-name* **out**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-policy pass-all out
```

Applies a routing policy to updates that are sent to a BGP neighbor.

- Use the *route-policy-name* argument to define the name of the of route policy. The example shows that the route policy name is defined as pass-all.
- Use the **out** keyword to define the policy for outbound routes.

Step 10 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Configuring the Route Reflectors to Exchange VPN-IPv4 Routes

Perform this task to enable the route reflectors to exchange VPN-IPv4 routes by using multihop. This task specifies that the next-hop information and the VPN label are to be preserved across the autonomous system.

SUMMARY STEPS

1. **configure**
2. **router bgp** *autonomous-system-number*
3. **neighbor** *ip-address*
4. **remote-as** *autonomous-system-number*
5. **ebgp-multihop** [*ttl-value*]
6. **update-source** *type interface-path-id*
7. **address-family vpnv4 unicast**
8. **route-policy** *route-policy-name* **in**
9. **route-policy** *route-policy-name* **out**
10. **next-hop-unchanged**
11. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

Step 1 **configure**

Example:

```
RP/0/RSP0/CPU0:router# configure
```

Enters Global Configuration mode.

Step 2 **router bgp** *autonomous-system-number*

Example:

```
RP/0/RSP0/CPU0:router(config)# router bgp 120
RP/0/RSP0/CPU0:router(config-bgp)#
```

Enters Border Gateway Protocol (BGP) configuration mode allowing you to configure the BGP routing process.

Step 3 **neighbor** *ip-address*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp)# neighbor 172.168.40.24
RP/0/RSP0/CPU0:router(config-bgp-nbr)#
```

Places the router in neighbor configuration mode for BGP routing and configures the neighbor IP address 172.168.40.24 as a BGP peer.

Step 4 **remote-as** *autonomous-system-number*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 2002
```

Creates a neighbor and assigns it a remote autonomous system number.

Step 5 **ebgp-multihop** [*ttl-value*]

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)# ebgp-multihop
```

Enables multihop peerings with external BGP neighbors.

Step 6 **update-source** *type interface-path-id*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)# update-source loopback0
```

Allows BGP sessions to use the primary IP address from a particular interface as the local address.

Step 7 **address-family vpnv4 unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family vpnv4 unicast
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)#
```

Configures VPNv4 address family.

Step 8 **route-policy** *route-policy-name* **in**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-policy pass-all in
```

Applies a routing policy to updates that are received from a BGP neighbor.

- Use the *route-policy-name* argument to define the name of the of route policy. The example shows that the route policy name is defined as pass-all.
- Use the **in** keyword to define the policy for inbound routes.

Step 9 **route-policy** *route-policy-name* **out**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-policy pass-all out
```

Applies a routing policy to updates that are sent to a BGP neighbor.

- Use the *route-policy-name* argument to define the name of the of route policy. The example shows that the route policy name is defined as pass-all.
- Use the **out** keyword to define the policy for outbound routes.

Step 10 **next-hop-unchanged**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# next-hop-unchanged
```

Disables overwriting of the next hop before advertising to external Border Gateway Protocol (eBGP) peers.

Step 11 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Configuring the Route Reflector to Reflect Remote Routes in its AS

Perform this task to enable the route reflector (RR) to reflect the IPv4 routes and labels learned by the autonomous system boundary router (ASBR) to the provider edge (PE) routers in the autonomous system. This task is accomplished by making the ASBR and PE route reflector clients of the RR.

SUMMARY STEPS

1. **configure**
2. **router bgp** *autonomous-system-number*
3. **address-family ipv4 unicast**
4. **allocate-label all**
5. **neighbor** *ip-address*
6. **remote-as** *autonomous-system-number*
7. **update-source** *type interface-path-id*
8. **address-family ipv4 labeled-unicast**
9. **route-reflector-client**
10. **neighbor** *ip-address*
11. **remote-as** *autonomous-system-number*
12. **update-source** *type interface-path-id*
13. **address-family ipv4 labeled-unicast**
14. **route-reflector-client**

15. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

Step 1 **configure**

Example:

```
RP/0/RSP0/CPU0:router# configure
```

Enters Global Configuration mode.

Step 2 **router bgp** *autonomous-system-number*

Example:

```
RP/0/RSP0/CPU0:router(config)# router bgp 120
```

Enters Border Gateway Protocol (BGP) configuration mode allowing you to configure the BGP routing process.

Step 3 **address-family ipv4 unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp)# address-family ipv4 unicast
RP/0/RSP0/CPU0:router(config-bgp-af)#
```

Enters global address family configuration mode for the IPv4 unicast address family.

Step 4 **allocate-label all**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-af)# allocate-label all
```

Allocates the MPLS labels for a specific IPv4 unicast or VPN routing and forwarding (VRF) IPv4 unicast routes so that the BGP router can send labels with BGP routes to a neighboring router that is configured for a labeled-unicast session.

Step 5 **neighbor** *ip-address*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-af)# neighbor 172.168.40.24
RP/0/RSP0/CPU0:router(config-bgp-nbr)#
```

Places the router in neighbor configuration mode for BGP routing and configures the neighbor IP address 172.168.40.24 as an ASBR eBGP peer.

Step 6 **remote-as** *autonomous-system-number*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 2002
```

Creates a neighbor and assigns it a remote autonomous system number.

Step 7 **update-source** *type interface-path-id*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)# update-source loopback0
```

Allows BGP sessions to use the primary IP address from a particular interface as the local address.

Step 8 **address-family ipv4 labeled-unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family ipv4 labeled-unicast
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)#
```

Enters neighbor address family configuration mode for the IPv4 labeled-unicast address family.

Step 9 **route-reflector-client**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-reflector-client
```

Configures the router as a BGP route reflector and neighbor 172.168.40.24 as its client.

Step 10 **neighbor** *ip-address*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# neighbor 10.40.25.2
RP/0/RSP0/CPU0:router(config-bgp-nbr)#
```

Places the router in neighbor configuration mode for BGP routing and configures the neighbor IP address .40.25.2 as an VPNv4 iBGP peer.

Step 11 **remote-as** *autonomous-system-number*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 2002
```

Creates a neighbor and assigns it a remote autonomous system number.

Step 12 **update-source** *type interface-path-id*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)# update-source loopback0
```

Allows BGP sessions to use the primary IP address from a particular interface as the local address.

Step 13 **address-family ipv4 labeled-unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family ipv4 labeled-unicast
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)#
```

Enters neighbor address family configuration mode for the IPv4 labeled-unicast address family.

Step 14 **route-reflector-client**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-reflector-client
```

Configures the neighbor as a route reflector client.

Step 15 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Providing VPN Connectivity Across Multiple Autonomous Systems with MPLS VPN Inter-AS with ASBRs Exchanging VPN-IPv4 Addresses

This section contains instructions for the following tasks:

Configuring the ASBRs to Exchange VPN-IPv4 Addresses for IP Tunnels

Perform this task to configure an external Border Gateway Protocol (eBGP) autonomous system boundary router (ASBR) to exchange VPN-IPv4 routes with another autonomous system.

SUMMARY STEPS

1. **configure**
2. **router bgp** *autonomous-system-number*
3. **address-family** { **ipv4 tunnel** }
4. **address-family** { **vpnv4 unicast** }
5. **neighbor** *ip-address*
6. **remote-as** *autonomous-system-number*
7. **address-family** { **vpnv4 unicast** }
8. **route-policy** *route-policy-name* { **in** }
9. **route-policy** *route-policy-name* { **out** }

10. **neighbor** *ip-address*
11. **remote-as** *autonomous-system-number*
12. **update-source** *type interface-path-id*
13. **address-family** { **ipv4 tunnel** }
14. **address-family** { **vpnv4 unicast** }
15. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

Step 1 **configure**

Example:

```
RP/0/RSP0/CPU0:router# configure
```

Enters the Global Configuration mode.

Step 2 **router bgp** *autonomous-system-number*

Example:

```
RP/0/RSP0/CPU0:router(config)# router bgp 120
RP/0/RSP0/CPU0:router(config-bgp)#
```

Enters Border Gateway Protocol (BGP) configuration mode allowing you to configure the BGP routing process.

Step 3 **address-family** { **ipv4 tunnel** }

Example:

```
RP/0/RSP0/CPU0:router(config-bgp)# address-family ipv4 tunnel
RP/0/RSP0/CPU0:router(config-bgp-af)#
```

Configures IPv4 tunnel address family.

Step 4 **address-family** { **vpnv4 unicast** }

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-af)# address-family vpnv4 unicast
```

Configures VPNv4 address family.

Step 5 **neighbor** *ip-address*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-af)# neighbor 172.168.40.24
RP/0/RSP0/CPU0:router(config-bgp-nbr)#
```

Places the router in neighbor configuration mode for BGP routing and configures the neighbor IP address 172.168.40.24 as an ASBR eBGP peer.

Step 6 **remote-as** *autonomous-system-number*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 2002
```

Creates a neighbor and assigns it a remote autonomous system number.

Step 7 **address-family** { **vpnv4 unicast** }

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family vpnv4 unicast
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)#
```

Configures VPNv4 address family.

Step 8 **route-policy** *route-policy-name* { **in** }

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-policy pass-all in
```

Applies a routing policy to updates that are received from a BGP neighbor.

- Use the *route-policy-name* argument to define the name of the of route policy. The example shows that the route policy name is defined as pass-all.
- Use the **in** keyword to define the policy for inbound routes.

Step 9 **route-policy** *route-policy-name* { **out** }

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-policy pass-all out
```

Applies a routing policy to updates that are sent from a BGP neighbor.

- Use the *route-policy-name* argument to define the name of the route policy. The example shows that the route policy name is defined as pass-all.
- Use the **out** keyword to define the policy for outbound routes.

Step 10 **neighbor** *ip-address*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# neighbor 175.40.25.2
RP/0/RSP0/CPU0:router(config-bgp-nbr)#
```

Places the router in neighbor configuration mode for BGP routing and configures the neighbor IP address 175.40.25.2 as an VPNv4 iBGP peer.

Step 11 **remote-as** *autonomous-system-number*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 2002
```

Creates a neighbor and assigns it a remote autonomous system number.

Step 12 **update-source** *type interface-path-id*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)# update-source loopback0
```

Allows BGP sessions to use the primary IP address from a particular interface as the local address.

Step 13 **address-family** { **ipv4 tunnel** }

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family ipv4 tunnel
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)#
```

Configures IPv4 tunnel address family.

Step 14 **address-family** { **vpnv4 unicast** }

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# address-family vpnv4 unicast
```

Configures VPNv4 address family.

Step 15 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Configuring a Static Route to an ASBR Peer

Perform this task to configure a static route to an ASBR peer.

SUMMARY STEPS

1. **configure**
2. **router static**
3. **address-family ipv4 unicast**
4. **A.B.C.D/length** *next-hop*
5. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

Step 1 **configure**

Example:

```
RP/0/RSP0/CPU0:router# configure
```

Enters the Global Configuration mode.

Step 2 **router static**

Example:

```
RP/0/RSP0/CPU0:router(config)# router static
RP/0/RSP0/CPU0:router(config-static)#
```

Enters router static configuration mode.

Step 3 **address-family ipv4 unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-static)# address-family ipv4 unicast
RP/0/RSP0/CPU0:router(config-static-afi)#
```

Enables an IPv4 address family.

Step 4 **A.B.C.D/length** *next-hop*

Example:

```
RP/0/RSP0/CPU0:router(config-static-afi)# 10.10.10.10/32 10.9.9.9
```

Enters the address of the destination router (including IPv4 subnet mask).

Step 5 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Configuring EBGP Routing to Exchange VPN Routes Between Subautonomous Systems in a Confederation

Perform this task to configure external Border Gateway Protocol (eBGP) routing to exchange VPN routes between subautonomous systems in a confederation.

Note To ensure that host routes for VPN-IPv4 eBGP neighbors are propagated (by means of the Interior Gateway Protocol [IGP]) to other routers and PE routers, specify the **redistribute connected** command in the IGP configuration portion of the confederation eBGP (CEBGP) router. If you are using Open Shortest Path First (OSPF), make sure that the OSPF process is not enabled on the CEBGP interface in which the “redistribute connected” subnet exists.

SUMMARY STEPS

1. **configure**
2. **router bgp** *autonomous-system-number*
3. **bgp confederation peers** *peer autonomous-system-number*
4. **bgp confederation identifier** *autonomous-system-number*
5. **address-family vpnv4 unicast**
6. **neighbor** *ip-address*
7. **remote-as** *autonomous-system-number*
8. **address-family vpnv4 unicast**
9. **route-policy** *route-policy-name* **in**
10. **route-policy** *route-policy-name* **out**
11. **next-hop-self**
12. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

Step 1 **configure**

Example:

```
RP/0/RSP0/CPU0:router# configure
```

Enters Global Configuration mode.

Step 2 **router bgp** *autonomous-system-number*

Example:

```
RP/0/RSP0/CPU0:router(config)# router bgp 120
RP/0/RSP0/CPU0:router(config-bgp)#
```

Enters BGP configuration mode allowing you to configure the BGP routing process.

Step 3 **bgp confederation peers** *peer autonomous-system-number*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp)# bgp confederation peers 8
```

Configures the peer autonomous system number that belongs to the confederation.

Step 4 **bgp confederation identifier** *autonomous-system-number*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp)# bgp confederation identifier 5
```

Specifies the autonomous system number for the confederation ID.

Step 5 **address-family vpnv4 unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp)# address-family vpnv4 unicast
RP/0/RSP0/CPU0:router(config-bgp-af)#
```

Configures VPNv4 address family.

Step 6 **neighbor** *ip-address*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-af)# neighbor 10.168.40.24
RP/0/RSP0/CPU0:router(config-bgp-nbr)#
```

Places the router in neighbor configuration mode for BGP routing and configures the neighbor IP address 10.168.40.24 as a BGP peer.

Step 7 **remote-as** *autonomous-system-number*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)# remote-as 2002
```

Creates a neighbor and assigns it a remote autonomous system number.

Step 8 **address-family vpnv4 unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family vpnv4 unicast
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)#
```

Configures VPNv4 address family.

Step 9 **route-policy** *route-policy-name* **in**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-policy In-Ipv4 in
```

Applies a routing policy to updates received from a BGP neighbor.

Step 10 **route-policy** *route-policy-name* **out**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# route-policy Out-Ipv4 out
```

Applies a routing policy to updates advertised to a BGP neighbor.

Step 11 **next-hop-self**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)# next-hop-self
```

Disables next-hop calculation and let you insert your own address in the next-hop field of BGP updates.

Step 12 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Configuring MPLS Forwarding for ASBR Confederations

Perform this task to configure MPLS forwarding for autonomous system boundary router (ASBR) confederations (in BGP) on a specified interface.

Note This configuration adds the implicit NULL rewrite corresponding to the peer associated with the interface, which is required to prevent BGP from automatically installing rewrites by LDP (in multihop instances).

SUMMARY STEPS

1. **configure**
2. **router bgp** *as-number*
3. **mpls activate**
4. **interface** *type interface-path-id*
5. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

Step 1 **configure**

Example:

```
RP/0/RSP0/CPU0:router# configure
```

Enters Global Configuration mode.

Step 2 **router bgp** *as-number*

Example:

```
RP/0/RSP0/CPU0:router(config)# router bgp 120
RP/0/RSP0/CPU0:router(config-bgp)
```

Enters BGP configuration mode allowing you to configure the BGP routing process.

Step 3 **mpls activate**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp)# mpls activate
RP/0/RSP0/CPU0:router(config-bgp-mpls)#
```

Enters BGP MPLS activate configuration mode.

Step 4 **interface** *type interface-path-id*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-mpls)# interface GigabitEthernet 0/3/0/0
```

Enables MPLS on the interface.

Step 5 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Configuring a Static Route to an ASBR Confederation Peer

Perform this task to configure a static route to an Inter-AS confederation peer. For more detailed information, see “Configuring a Static Route to a Peer" section.

SUMMARY STEPS

1. **configure**
2. **router static**
3. **address-family ipv4 unicast**
4. **A.B.C.D/length** *next-hop*
5. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

Step 1 **configure**

Example:

```
RP/0/RSP0/CPU0:router# configure
```

Enters Global Configuration mode.

Step 2 **router static**

Example:

```
RP/0/RSP0/CPU0:router(config)# router static
RP/0/RSP0/CPU0:router(config-static)#
```

Enters router static configuration mode.

Step 3 **address-family ipv4 unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-static)# address-family ipv4 unicast
RP/0/RSP0/CPU0:router(config-static-afi)#
```

Enables an IPv4 address family.

Step 4 **A.B.C.D/length** *next-hop*

Example:

```
RP/0/RSP0/CPU0:router(config-static-afi)# 10.10.10.10/32 10.9.9.9
```

Enters the address of the destination router (including IPv4 subnet mask).

Step 5 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Configuring Carrier Supporting Carrier

Perform the tasks in this section to configure Carrier Supporting Carrier (CSC):

Identifying the Carrier Supporting Carrier Topology

Before you configure the MPLS VPN CSC with BGP, you must identify both the backbone and customer carrier topology.

Note You can connect multiple CSC-CE routers to the same PE, or you can connect a single CSC-CE router to multiple CSC-PEs using more than one CSC-CE interface to provide redundancy and multiple path support in a CSC topology.

Perform this task to identify the carrier supporting carrier topology.

SUMMARY STEPS

1. Identify the type of customer carrier, ISP, or MPLS VPN service provider.
2. Identify the CE routers.
3. Identify the customer carrier core router configuration.
4. Identify the customer carrier edge (CSC-CE) routers.
5. Identify the backbone carrier router configuration.

DETAILED STEPS

Procedure

Step 1 Identify the type of customer carrier, ISP, or MPLS VPN service provider.

Sets up requirements for configuration of carrier supporting carrier network.

Step 2 Identify the CE routers.

Sets up requirements for configuration of CE to PE connections.

Step 3 Identify the customer carrier core router configuration.

Sets up requirements for configuration between core (P) routers and between P routers and edge routers (PE and CSC-CE routers).

Step 4 Identify the customer carrier edge (CSC-CE) routers.

Sets up requirements for configuration of CSC-CE to CSC-PE connections.

Step 5 Identify the backbone carrier router configuration.

Sets up requirements for configuration between CSC core routers and between CSC core routers and edge routers (CSC-CE and CSC-PE routers).

Configuring the Backbone Carrier Core

Configuring the backbone carrier core requires setting up connectivity and routing functions for the CSC core and the CSC-PE routers. To do so, you must complete the following high-level tasks:

- Verify IP connectivity in the CSC core.
- Verify LDP configuration in the CSC core.

Note This task is not applicable to CSC over IP tunnels.

- Configure VRFs for CSC-PE routers.
- Configure multiprotocol BGP for VPN connectivity in the backbone carrier.

Configuring the CSC-PE and CSC-CE Routers

Perform the following tasks to configure links between a CSC-PE router and the carrier CSC-CE router for an MPLS VPN CSC network that uses BGP to distribute routes and MPLS labels:

The following figure shows the configuration for the peering with directly connected interfaces between CSC-PE and CSC-CE routers. This configuration is used as the example in the tasks that follow.

Figure 7: Configuration for Peering with Directly Connected Interfaces Between CSC-PE and CSC-CE Routers

Configuring a Static Route to a Peer

Perform this task to configure a static route to an Inter-AS or CSC-CE peer.

When you configure an Inter-AS or CSC peer, BGP allocates a label for a /32 route to that peer and performs a NULL label rewrite. When forwarding a labeled packet to the peer, the router removes the top label from the label stack; however, in such an instance, BGP expects a /32 route to the peer. This task ensures that there is, in fact, a /32 route to the peer.

Please be aware of the following facts before performing this task:

- A /32 route is not required to establish BGP peering. A route using a shorter prefix length will also work.
- A shorter prefix length route is not associated with the allocated label; even though the BGP session comes up between the peers, without the static route, forwarding will not work.

Note To configure a static route on a CSC-PE, you must configure the router under the VRF (as noted in the detailed steps).

SUMMARY STEPS

1. **configure**
2. **router static**
3. **address-family ipv4 unicast**
4. **A.B.C.D/length** *next-hop*

5. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

Step 1 **configure**

Example:

```
RP/0/RSP0/CPU0:router# configure
```

Enters the Global Configuration mode.

Step 2 **router static**

Example:

```
RP/0/RSP0/CPU0:router(config)# router static
```

Enters router static configuration mode.

Step 3 **address-family ipv4 unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-static)# address-family ipv4 unicast
```

Enables an IPv4 address family.

Note
To configure a static route on a CSC-PE, you must first configure the VRF using the **vrf** command before **address-family**.

Step 4 **A.B.C.D/length** *next-hop*

Example:

```
RP/0/RSP0/CPU0:router(config-static-afi)# 10.10.10.10/32 10.9.9.9
```

Enters the address of the destination router (including IPv4 subnet mask).

Step 5 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Verifying the MPLS Layer 3 VPN Configuration

Perform this task to verify the MPLS Layer 3 VPN configuration.

SUMMARY STEPS

1. **show running-config router bgp** *as-number* **vrf** *vrf-name*
2. **show running-config routes**
3. **show ospf vrf** *vrf-name* **database**
4. **show running-config router bgp** *as-number* **vrf** *vrf-name* **neighbor** *ip-address*
5. **show bgp vrf** *vrf-name* **summary**
6. **show bgp vrf** *vrf-name* **neighbors** *ip-address*
7. **show bgp vrf** *vrf-name*
8. **show route vrf** *vrf-name ip-address*
9. **show bgp vpn unicast summary**
10. **show running-config router isis**
11. **show running-config mpls**
12. **show isis adjacency**
13. **show mpls ldp forwarding**
14. **show bgp vpnv4 unicast** or **show bgp vrf** *vrf-name*
15. **show bgp vrf** *vrf-name* **imported-routes**
16. **show route vrf** *vrf-name ip-address*
17. **show cef vrf** *vrf-name ip-address*
18. **show cef vrf** *vrf-name ip-address* **location** *node-id*
19. **show bgp vrf** *vrf-name ip-address*
20. **show ospf vrf** *vrf-name* **database**

DETAILED STEPS

Procedure

Step 1 **show running-config router bgp** *as-number* **vrf** *vrf-name*

Example:

```
RP/0/RSP0/CPU0:router# show running-config router bgp 3 vrf vrf_A
```

Displays the specified VPN routing and forwarding (VRF) content of the currently running configuration.

Step 2 **show running-config routes**

Example:

```
RP/0/RSP0/CPU0:router# show running-config routes
```

Displays the Open Shortest Path First (OSPF) routes table in the currently running configuration.

Step 3 **show ospf vrf** *vrf-name* **database**

Example:

```
RP/0/RSP0/CPU0:router# show ospf vrf vrf_A database
```

Displays lists of information related to the OSPF database for a specified VRF.

Step 4 **show running-config router bgp** *as-number* **vrf** *vrf-name* **neighbor** *ip-address*

Example:

```
RP/0/RSP0/CPU0:router# show running-config router bgp 3 vrf vrf_A neighbor 172.168.40.24
```

Displays the Border Gateway Protocol (BGP) VRF neighbor content of the currently running configuration.

Step 5 **show bgp vrf** *vrf-name* **summary**

Example:

```
RP/0/RSP0/CPU0:router# show bgp vrf vrf_A summary
```

Displays the status of the specified BGP VRF connections.

Step 6 **show bgp vrf** *vrf-name* **neighbors** *ip-address*

Example:

```
RP/0/RSP0/CPU0:router# show bgp vrf vrf_A neighbors 172.168.40.24
```

Displays information about BGP VRF connections to the specified neighbors.

Step 7 **show bgp vrf** *vrf-name*

Example:

```
RP/0/RSP0/CPU0:router# show bgp vrf vrf_A
```

Displays information about a specified BGP VRF.

Step 8 **show route vrf** *vrf-name ip-address*

Example:

```
RP/0/RSP0/CPU0:router# show route vrf vrf_A 10.0.0.0
```

Displays the current routes in the Routing Information Base (RIB) for a specified VRF.

Step 9 **show bgp vpn unicast summary**

Example:

```
RP/0/RSP0/CPU0:router# show bgp vpn unicast summary
```

Displays the status of all BGP VPN unicast connections.

Step 10 **show running-config router isis**

Example:

```
RP/0/RSP0/CPU0:router# show running-config router isis
```

Displays the Intermediate System-to-Intermediate System (IS-IS) content of the currently running configuration.

Step 11 **show running-config mpls**

Example:

```
RP/0/RSP0/CPU0:router# show running-config mpls
```

Displays the MPLS content of the currently running-configuration.

Step 12 **show isis adjacency**

Example:

```
RP/0/RSP0/CPU0:router# show isis adjacency
```

Displays IS-IS adjacency information.

Step 13 **show mpls ldp forwarding**

Example:

```
RP/0/RSP0/CPU0:router# show mpls ldp forwarding
```

Displays the Label Distribution Protocol (LDP) forwarding state installed in MPLS forwarding.

Step 14 **show bgp vpnv4 unicast** or **show bgp vrf** *vrf-name*

Example:

```
RP/0/RSP0/CPU0:router# show bgp vpnv4 unicast
```

Displays entries in the BGP routing table for VPNv4 or VPNv6 unicast addresses.

Step 15 **show bgp vrf** *vrf-name* **imported-routes**

Example:

```
RP/0/RSP0/CPU0:router# show bgp vrf vrf_A imported-routes
```

Displays BGP information for routes imported into specified VRF instances.

Step 16 **show route vrf** *vrf-name ip-address*

Example:

```
RP/0/RSP0/CPU0:router# show route vrf vrf_A 10.0.0.0
```

Displays the current specified VRF routes in the RIB.

Step 17 **show cef vrf** *vrf-name ip-address*

Example:

```
RP/0/RSP0/CPU0:router# show cef vrf vrf_A 10.0.0.1
```

Displays the IPv4 Cisco Express Forwarding (CEF) table for a specified VRF.

Step 18 **show cef vrf** *vrf-name ip-address* **location** *node-id*

Example:

```
RP/0/RSP0/CPU0:router# show cef vrf vrf_A 10.0.0.1 location 0/1/cpu0
```

Displays the IPv4 CEF table for a specified VRF and location.

Step 19 **show bgp vrf** *vrf-name ip-address*

Example:

```
RP/0/RSP0/CPU0:router# show bgp vrf vrf_A 10.0.0.0
```

Displays entries in the BGP routing table for VRF vrf_A.

Step 20 **show ospf vrf** *vrf-name* **database**

Example:

```
RP/0/RSP0/CPU0:router# show ospf vrf vrf_A database
```

Displays lists of information related to the OSPF database for a specified VRF.

Configuring L3VPN over GRE

Perform the following tasks to configure L3VPN over GRE:

Creating a GRE Tunnel between Provider Edge Routers

Perform this task to configure a GRE tunnel between provider edge routers.

SUMMARY STEPS

1. **configure**
2. **interface tunnel-ip** *number*
3. **ipv4 address** *ipv4-address subnet-mask*
4. **ipv6 address** *ipv6-prefix/prefix-length*
5. **tunnel mode gre ipv4**
6. **tunnel source** *type path-id*
7. **tunnel destination** *ip-address*
8. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

Step 1 **configure**

Example:

```
RP/0/RSP0/CPU0:router# configure
```

Enters the Global Configuration mode.

Step 2 **interface tunnel-ip** *number*

Example:

```
RP/0/RSP0/CPU0:router(config)# interface tunnel-ip 4000
```

Enters tunnel interface configuration mode.

- number is the number associated with the tunnel interface.

Step 3 **ipv4 address** *ipv4-address subnet-mask*

Example:

```
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 10.0.0.1 255.0.0.0
```

Specifies the IPv4 address and subnet mask for the interface.

- ipv4-address specifies the IP address of the interface.
- subnet-mask specifies the subnet mask of the interface.

Step 4 **ipv6 address** *ipv6-prefix/prefix-length*

Example:

```
RP/0/RSP0/CPU0:router(config-if)# ipv6 address 100:1:1:1::1/64
```

Specifies an IPv6 network assigned to the interface.

Step 5 **tunnel mode gre ipv4**

Example:

```
RP/0/RSP0/CPU0:router(config-if)# tunnel mode gre ipv4
```

Sets the encapsulation mode of the tunnel interface to GRE.

Step 6 **tunnel source** *type path-id*

Example:

```
RP/0/RSP0/CPU0:router(config-if)# tunnel source TenGigE0/2/0/1
```

Specifies the source of the tunnel interface.

Step 7 **tunnel destination** *ip-address*

Example:

```
RP/0/RSP0/CPU0:router(config-if)# tunnel destination 145.12.5.2
```

Defines the tunnel destination.

Step 8 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Configuring IGP between Provider Edge Routers

Perform this task to configure IGP between provider edge routers.

SUMMARY STEPS

1. **configure**
2. **router ospf** *process-name*
3. **nsr**
4. **router-id** { *router-id* }
5. **mpls ldp sync**
6. **dead-interval** *seconds*
7. **hello-interval** *seconds*
8. **area** *area-id*
9. **interface tunnel-ip** *number*
10. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

Step 1 **configure**

Example:

```
RP/0/RSP0/CPU0:router# configure
```

Enters the Global Configuration mode.

Step 2 **router ospf** *process-name*

Example:

```
RP/0/RSP0/CPU0:router(config)# router ospf 1
```

Enables OSPF routing for the specified routing process and places the router in router configuration mode.

Step 3 **nsr**

Example:

```
RP/0/RSP0/CPU0:router(config-ospf)# nsr
```

Activates BGP NSR.

Step 4 **router-id** { *router-id* }

Example:

```
RP/0/RSP0/CPU0:router(config-ospf)# router-id 10.0.0.1
```

Configures a router ID for the OSPF process.

Note
We recommend using a stable IP address as the router ID.

Step 5 **mpls ldp sync**

Example:

```
RP/0/RSP0/CPU0:router(config-ospf)# mpls ldp sync
```

Enables MPLS LDP synchronization.

Step 6 **dead-interval** *seconds*

Example:

```
RP/0/RSP0/CPU0:router(config-ospf)# dead-interval 60
```

Sets the time to wait for a hello packet from a neighbor before declaring the neighbor down.

Step 7 **hello-interval** *seconds*

Example:

```
RP/0/RSP0/CPU0:router(config-ospf)# hello-interval 15
```

Specifies the interval between hello packets that OSPF sends on the interface.

Step 8 **area** *area-id*

Example:

```
RP/0/RSP0/CPU0:router(config-ospf)# area 0
```

Enters area configuration mode and configures an area for the OSPF process.

Step 9 **interface tunnel-ip** *number*

Example:

```
RP/0/RSP0/CPU0:router(config-ospf)# interface tunnel-ip 4
```

Enters tunnel interface configuration mode.

- number is the number associated with the tunnel interface.

Step 10 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Configuring LDP/GRE on the Provider Edge Routers

Perform this task to configure LDP/GRE on the provider edge routers.

SUMMARY STEPS

1. **configure**
2. **mpls ldp**
3. **router-id** { *router-id* }
4. **discovery hello holdtime** *seconds*
5. **discovery hello interval** *seconds*
6. **nsr**
7. **graceful-restart**
8. **graceful-restart reconnect-timeout** *seconds*
9. **graceful-restart forwarding-state-holdtime** *seconds*
10. **holdtime** *seconds*
11. **neighbor** *ip-address*
12. **interface tunnel-ip** *number*
13. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

Step 1 **configure**

Example:

```
RP/0/RSP0/CPU0:router# configure
```

Enters the Global Configuration mode.

Step 2 **mpls ldp**

Example:

```
RP/0/RSP0/CPU0:router(config)# mpls ldp
```

Enables MPLS LDP configuration mode.

Step 3 **router-id** { *router-id* }

Example:

```
RP/0/RSP0/CPU0:router(config-ldp)# router-id 10.0.0.1
```

Configures a router ID for the OSPF process.

Note
We recommend using a stable IP address as the router ID.

Step 4 **discovery hello holdtime** *seconds*

Example:

```
RP/0/RSP0/CPU0:router(config-ldp)# discovery hello holdtime 40
```

Defines the period of time a discovered LDP neighbor is remembered without receipt of an LDP Hello message from the neighbor.

Note
We recommend using a stable IP address as the router ID.

Step 5 **discovery hello interval** *seconds*

Example:

```
RP/0/RSP0/CPU0:router(config-ldp)# discovery hello holdtime 20
```

Defines the period of time between the sending of consecutive Hello messages.

Step 6 **nsr**

Example:

```
RP/0/RSP0/CPU0:router(config-ldp)# nsr
```

Activates BGP NSR.

Step 7 **graceful-restart**

Example:

```
RP/0/RSP0/CPU0:router(config-ldp)# graceful-restart
```

Enables graceful restart on the router.

Step 8 **graceful-restart reconnect-timeout** *seconds*

Example:

```
RP/0/RSP0/CPU0:router(config-ldp)# graceful-restart recoonect-timeout 180
```

Defines the time for which the neighbor should wait for a reconnection if the LDP session is lost.

Step 9 **graceful-restart forwarding-state-holdtime** *seconds*

Example:

```
RP/0/RSP0/CPU0:router(config-ldp)# graceful-restart forwarding-state-holdtime 300
```

Defines the time that the neighbor should retain the MPLS forwarding state during a recovery.

Step 10 **holdtime** *seconds*

Example:

```
RP/0/RSP0/CPU0:router(config-ldp)# holdtime 90
```

Configures the hold time for an interface.

Step 11 **neighbor** *ip-address*

Example:

```
RP/0/RSP0/CPU0:router(config-ldp)# neighbor 10.1.1.0
```

Defines a neighboring router.

Step 12 **interface tunnel-ip** *number*

Example:

```
RP/0/RSP0/CPU0:router(config-ldp)# interface tunnel-ip 4
```

Enters tunnel interface configuration mode.

- number is the number associated with the tunnel interface.

Step 13 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Configuring L3VPN

Perform this task to configure L3VPN.

SUMMARY STEPS

1. **configure**
2. **vrf** *vrf-name*

3. **address-family { ipv4 | ipv6 } unicast**
4. **import route-target** [*as-number:nn* | *ip-address:nn*]
5. **export route-target** [*as-number:nn* | *ip-address:nn*]
6. **interface** *type interface-path-id*
7. **vrf** *vrf-name*
8. **ipv4 address** *ipv4-address subnet-mask*
9. **dot1q native vlan** *vlan-id*
10. **router bgp** *as-number*
11. **nsr**
12. **bgp router-id** *ip-address*
13. **address-family {vpnv4 | vpnv6} unicast**
14. **neighbor** *ip-address*
15. **remote-as** *as-number*
16. **update-source** *type interface-path-id*
17. **address-family { vpnv4 | vpnv6 } unicast**
18. **route-policy** *route-policy-name* **in**
19. **route-policy** *route-policy-name* **out**
20. **vrf** *vrf-name*
21. **rd { as-number:nn | ip-address:nn | auto }**
22. **address-family { ipv4 | ipv6 } unicast**
23. **redistribute connected** [**metric** *metric-value*] [*route-policy route-policy-name*]
24. **redistribute static** [**metric** *metric-value*] [*route-policy route-policy-name*]
25. **neighbor** *ip-address*
26. **remote-as** *as-number*
27. **ebg-multihop** *ttl-value*
28. **address-family { ipv4 | ipv6 } unicast**
29. **route-policy** *route-policy-name* **in**
30. **route-policy** *route-policy-name* **out**
31. Use the **commit** or **end** command.

DETAILED STEPS

Procedure

Step 1 **configure**

Example:

```
RP/0/RSP0/CPU0:router# configure
```

Enters the Global Configuration mode.

Step 2 **vrf** *vrf-name*

Example:

```
RP/0/RSP0/CPU0:router(config)# vrf vpn1
```

Configures a VRF instance.

Step 3 **address-family { ipv4 | ipv6 } unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-vrf)# address-family { ipv4 | ipv6 } unicast
```

Specifies either the IPv4 or IPv6 address family and enters address family configuration submode.

Step 4 **import route-target** [*as-number:nn* | *ip-address:nn*]

Example:

```
RP/0/RSP0/CPU0:router(config-vrf)# import route-target 2:1
```

Specifies a list of route target (RT) extended communities. Only prefixes that are associated with the specified import route target extended communities are imported into the VRF.

Step 5 **export route-target** [*as-number:nn* | *ip-address:nn*]

Example:

```
RP/0/RSP0/CPU0:router(config-vrf)# export route-target 1:1
```

Specifies a list of route target extended communities. Export route target communities are associated with prefixes when they are advertised to remote PEs. The remote PEs import them into VRFs which have import RTs that match these exported route target communities.

Step 6 **interface** *type interface-path-id*

Example:

```
RP/0/RSP0/CPU0:router(config)# interface TenGigE0/2/0/0.1
```

Enters interface configuration mode and configures an interface.

Step 7 **vrf** *vrf-name*

Example:

```
RP/0/RSP0/CPU0:router(config-if)# vrf vpn1
```

Configures a VRF instance.

Step 8 **ipv4 address** *ipv4-address subnet-mask*

Example:

```
RP/0/RSP0/CPU0:router(config-if)# ipv4 address 172.16.0.1 255.240.0.0
```

Specifies the IPv4 address and subnet mask for the interface.

- ipv4-address specifies the IP address of the interface.
- subnet-mask specifies the subnet mask of the interface.

Step 9 **dot1q native vlan** *vlan-id*

Example:

```
RP/0/RSP0/CPU0:router(config-if)# dot1q native
vlan 1
```

Assigns the native VLAN ID of a physical interface trunking 802.1Q VLAN traffic.

Step 10 **router bgp** *as-number*

Example:

```
RP/0/RSP0/CPU0:router(config)# router bgp 1
```

Specifies the autonomous system number and enters the BGP configuration mode, allowing you to configure the BGP routing process.

Step 11 **nsr**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp)# nsr
```

Activates BGP NSR.

Step 12 **bgp router-id** *ip-address*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp)# bgp router-id 10.0.0.1
```

Configures the local router with a specified router ID.

Step 13 **address-family {vpnv4 | vpnv6} unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp)# address-family vpnv4 unicast
```

Enters address family configuration submode for the specified address family.

Step 14 **neighbor** *ip-address*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp)# neighbor 192.168.0.1
```

Places the router in neighbor configuration mode for BGP routing and configures the neighbor IP address as a BGP peer.

Step 15 **remote-as** *as-number*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)#remote-as 1
```

Creates a neighbor and assigns a remote autonomous system number to it..

Step 16 **update-source** *type interface-path-id*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)#update-source Loopback0
```

Allows sessions to use the primary IP address from a specific interface as the local address when forming a session with a neighbor.

Step 17 **address-family { vpnv4 | vpnv6 } unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family vpnv4 unicast
```

Enters address family configuration submode for the specified address family.

Step 18 **route-policy** *route-policy-name* **in**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)#route-policy pass-all in
```

Defines a route policy and enters route policy configuration mode.

Step 19 **route-policy** *route-policy-name* **out**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)#route-policy pass-all out
```

Defines a route policy and enters route policy configuration mode.

Step 20 **vrf** *vrf-name*

Example:

```
RP/0/RSP0/CPU0:router(config)# vrf vpn1
```

Configures a VRF instance.

Step 21 **rd { as-number:nn | ip-address:nn | auto }**

Example:

```
RP/0/RSP0/CPU0:router(config-vrf)#rd 1:1
```

Configures the route distinguisher.

Step 22 **address-family { ipv4 | ipv6 } unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-vrf)# address-family ipv4 unicast
```

Specifies either the IPv4 or IPv6 address family and enters address family configuration submode.

Step 23 **redistribute connected** [**metric** *metric-value*] [*route-policy route-policy-name*]

Example:

```
RP/0/RSP0/CPU0:router(config-vrf-af)#
redistribute connected
```

Configures the local router with a specified router ID.

Step 24 **redistribute static** [**metric** *metric-value*] [*route-policy route-policy-name*]

Example:

```
RP/0/RSP0/CPU0:router(config-vrf-af)#
redistribute static
```

Causes routes from the specified instance to be redistributed into BGP.

Step 25 **neighbor** *ip-address*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp)# neighbor 172.16.0.2
```

Places the router in neighbor configuration mode for BGP routing and configures the neighbor IP address as a BGP peer.

Step 26 **remote-as** *as-number*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)#remote-as 7501
```

Creates a neighbor and assigns a remote autonomous system number to it..

Step 27 **ebg-multihop** *ttl-value*

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)
#ebgp-multihop 10
```

Configures the CE neighbor to accept and attempt BGP connections to external peers residing on networks that are not directly connected.

Step 28 **address-family { ipv4 | ipv6 } unicast**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr)# address-family ipv4 unicast
```

Specifies either the IPv4 or IPv6 address family and enters address family configuration submode.

Step 29 **route-policy** *route-policy-name* **in**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)#route-policy
BGP_pass_all in
```

Configures the local router with a specified router.

Step 30 **route-policy** *route-policy-name* **out**

Example:

```
RP/0/RSP0/CPU0:router(config-bgp-nbr-af)#route-policy BGP_pass_all out
```

Defines a route policy and enters route policy configuration mode.

Step 31 Use the **commit** or **end** command.

commit - Saves the configuration changes and remains within the configuration session.

end - Prompts user to take one of these actions:

- **Yes** - Saves configuration changes and exits the configuration session.
- **No** - Exits the configuration session without committing the configuration changes.
- **Cancel** - Remains in the configuration mode, without committing the configuration changes.

Configuration Examples for Implementing MPLS Layer 3 VPNs

The following section provides sample configurations for MPLS L3VPN features:

Configuring an MPLS VPN Using BGP: Example

The following example shows the configuration for an MPLS VPN using BGP on “vrf vpn1”:

```
address-family ipv4 unicast
    import route-target
      100:1
    !
    export route-target
      100:1
    !
  !
!
route-policy pass-all
  pass
end-policy
!
interface Loopback0
  ipv4 address 10.0.0.1 255.255.255.255
!
interface TenGigE 0/1/0/0
  vrf vpn1
  ipv4 address 10.0.0.2 255.0.0.0
!
interface TenGigE 0/1/0/1
  ipv4 address 10.0.0.1 255.0.0.0
!
router ospf 100
  area 100
    interface loopback0
    interface TenGigE 0/1/0/1
  !
!
router bgp 100
  address-family vpnv4 unicast
  retain route-target route-policy policy1
  neighbor 10.0.0.3
    remote-as 100
    update-source Loopback0
    address-family vpnv4 unicast
  !
```

```
  vrf vpn1
    rd 100:1
    address-family ipv4 unicast
      redistribute connected
    !
    neighbor 10.0.0.1
      remote-as 200
      address-family ipv4 unicast
        as-override
        route-policy pass-all in
        route-policy pass-all out
      !
      advertisement-interval 5
    !
  !
!
mpls ldp
  route-id looback0
  interface TenGigE 0/1/0/1
!
```

Configuring the Routing Information Protocol on the PE Router: Example

The following example shows the configuration for the RIP on the PE router:

```
vrf vpn1
  address-family ipv4 unicast
    import route-target
      100:1
    !
    export route-target
      100:1
    !
  !
!
route-policy pass-all
  pass
end-policy
!

interface TenGigE 0/1/0/0
  vrf vpn1
  ipv4 address 10.0.0.2 255.0.0.0
!

router rip
 vrf vpn1
  interface TenGigE 0/1/0/0
  !
  timers basic 30 90 90 120
  redistribute bgp 100
  default-metric 3
  route-policy pass-all in
 !
```

Configuring the PE Router Using EIGRP: Example

The following example shows the configuration for the Enhanced Interior Gateway Routing Protocol (EIGRP) on the PE router:

```
Router eigrp 10
 vrf VRF1
  address-family ipv4
   router-id 10.1.1.2
   default-metric 100000 2000 255 1 1500
   as 62
   redistribute bgp 2000
   interface Loopback0
   !
   interface TenGigE 0/6/0/0
```

Configuration Examples for MPLS VPN CSC

Configuration examples for the MPLS VPN CSC include:

Configuring the Backbone Carrier Core: Examples

Configuration examples for the backbone carrier core included in this section are as follows:

Configuring VRFs for CSC-PE Routers: Example

The following example shows how to configure a VPN routing and forwarding instance (VRF) for a CSC-PE router:

```
config
  vrf vpn1
   address-family ipv4 unicast
    import route-target 100:1
    export route-target 100:1
   end
```

Configuring the Links Between CSC-PE and CSC-CE Routers: Examples

This section contains the following examples:

Configuring a CSC-PE: Example

In this example, a CSC-PE router peers with a PE router, 10.1.0.2, in its own AS. It also has a labeled unicast peering with a CSC-CE router, 10.0.0.1.

```
config
 router bgp 2
  address-family vpnv4 unicast
  neighbor 10.1.0.2
      remote-as 2
     update-source loopback0
     address-family vpnv4 unicast
    vrf customer-carrier
     rd 1:100
     address-family ipv4 unicast
      allocate-label all
      redistribute static
    neighbor 10.0.0.1
     remote-as 1
     address-family ipv4 labeled-unicast
      route-policy pass-all in
      route-policy pass-all out
      as-override
```

```
end
```

Configuring a CSC-CE: Example

The following example shows how to configure a CSC-CE router. In this example, the CSC-CE router peers CSC-PE router 10.0.0.2 in AS 2.

```
config
 router bgp 1
  address-family ipv4 unicast
     redistribute ospf 200
     allocate-label all
    neighbor 10.0.0.2
     remote-as 2
     address-family ipv4 labeled-unicast
     route-policy pass-all in
     route-policy pass-all out
end
```

Configuring a Static Route to a Peer: Example

The following example shows how to configure a static route to an Inter-AS or CSC-CE peer:

```
config
 router static
  address-family ipv4 unicast
  10.0.0.2/32 172.16.0.1
end
```

Configuring a Static Route to a Peer: Example

This example shows how to configure a static route to an Inter-AS or CSC-CE peer:

```
config
 router static
  address-family ipv4 unicast
  10.0.0.2/32 40.1.1.1
end
```

Configuring L3VPN over GRE: Example

The following example shows how to configure L3VPN over GRE:

Sample configuration to create a GRE tunnel between PE1 and PE2:

```
RP/0/RSP0/CPU0:PE1#sh run int tunnel-ip 1
interface tunnel-ip1
 ipv4 address 172.16.0.1 255.240.0.0
 ipv6 address 100:1:1:1::1/64
 tunnel mode gre ipv4
 tunnel source TenGigE0/2/0/1
 tunnel destination 145.12.5.2
!
RP/0/RSP0/CPU0:PE2#sh run int tunnel-ip 1
interface tunnel-ip1
```

```
 ipv4 address 172.16.0.2 255.240.0.0
 ipv6 address 100:1:1:1::2/64
 tunnel mode gre ipv4
 tunnel source TenGigE0/1/0/2
 tunnel destination 192.168.0.1
```

Configure IGP between PE1 and PE2:

Sample configuration for PE1 is given below. PE2 will also have a similar configuration.

```
RP/0/RSP0/CPU0:PE1#sh run router ospf 1
router ospf 1
 nsr
 router-id 10.0.0.1 <=== Loopback0
 mpls ldp sync
 mtu-ignore enable
 dead-interval 60
 hello-interval 15
 area 0
  interface TenGigE0/2/0/1
  !
 RP/0/RSP0/CPU0:PE1#sh run router ospf 0
router ospf 0
 nsr
 router-id 10.0.0.1
 mpls ldp sync
 dead-interval 60
 hello-interval 15
 area 0
  interface Loopback0
  !
  interface tunnel-ip1
  !

* Check for OSPF neighbors

RP/0/RSP0/CPU0:PE1#sh ospf neighbor

Neighbors for OSPF 0

Neighbor ID     Pri   State           Dead Time   Address         Interface
4.4.4.4         1     FULL/  -        00:00:47    172.16.0.2       tunnel-ip1      <==
Neighbor PE2
    Neighbor is up for 00:13:40
Neighbors for OSPF 1

Neighbor ID     Pri   State           Dead Time   Address         Interface
2.2.2.2         1     FULL/DR         00:00:50    192.168.0.1      TenGigE0/2/0/1  <==
Neighbor P1
    Neighbor is up for 00:13:43
```

Configure LDP/GRE on PE1 and PE2:

```
RP/0/RSP0/CPU0:PE1#sh run mpls ldp
mpls ldp
 router-id 10.0.0.1 <=== Loopback0
 discovery hello holdtime 45
 discovery hello interval 15
 nsr
```

```
 graceful-restart
 graceful-restart reconnect-timeout 180
 graceful-restart forwarding-state-holdtime 300
 holdtime 90
 log
  neighbor
 !
 interface tunnel-ip1
 !

*Check for mpls forwarding

RP/0/RSP0/CPU0:PE1#sh mpls forwarding prefix 10.0.0.2/8
Local  Outgoing    Prefix             Outgoing     Next Hop        Bytes
Label  Label       or ID              Interface                    Switched
---- ------- -------------- -------- ----------- ----------
16003  Pop         10.0.0.2/8         ti1          172.16.0.2       0
```

Configure L3VPN

```
RP/0/RSP0/CPU0:PE1#sh run vrf vpn1
vrf vpn1
 address-family ipv4 unicast
  import route-target
   2:1
  !
  export route-target
   1:1
  !
RP/0/RSP0/CPU0:PE1#sh run int tenGigE 0/2/0/0.1
interface TenGigE0/2/0/0.1
 vrf vpn1
 ipv4 address 172.16.0.1 255.255.255.0
 encapsulation dot1q 1
!

RP/0/RSP0/CPU0:PE1#sh run router bgp
router bgp 1
 nsr
 bgp router-id 10.0.0.1 <===Loopback0
 address-family vpnv4 unicast
 !
 neighbor 192.168.0.1      <===iBGP session with PE2
  remote-as 1
  update-source Loopback0
  address-family vpnv4 unicast
   route-policy pass-all in
   route-policy pass-all out
  !
 !
 vrf vpn1
  rd 1:1
  address-family ipv4 unicast
   redistribute connected
   redistribute static
  !
  neighbor 172.16.0.2   <=== VRF neighbor
   remote-as 7501
   ebgp-multihop 10
   address-family ipv4 unicast
    route-policy BGP_pass_all in
    route-policy BGP_pass_all out
```

```
   !

* Check vrf ping to the 172.16.0.2

RP/0/RSP0/CPU0:PE1#ping vrf vpn1 172.16.0.2
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.0.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/3 ms

* Send traffic to vrf routes adverstised and verify that mpls counters increase in tunnel
interface accounting

RP/0/RSP0/CPU0:PE1#sh int tunnel-ip1 accounting
tunnel-ip1
  Protocol              Pkts In         Chars In     Pkts Out        Chars Out
  IPV4_MULTICAST              3              276            3              276
   MPLS                  697747         48842290            0                0
```

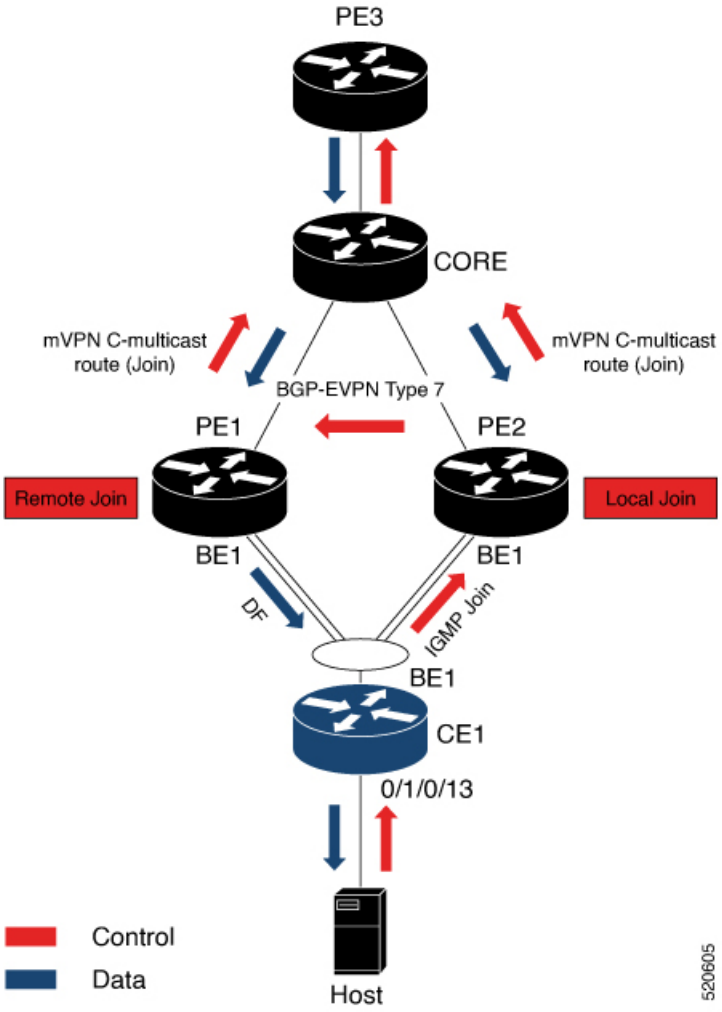
EVPN IGMP L3 Synchronization

The EVPN IGMP L3 Synchronization feature enables you to synchronize IGMPv2 and IGMPv3 reports on multihomed PEs over EVPN. The multihomed PEs synchronize IGMP JOIN using BGP EVPN route-type 7. The multihomed PEs synchronize IGMP LEAVE using BGP EVPN route-type 8. This feature provides better serviceability.

Restrictions

- This feature is supported on the Cisco ASR9000 3rd generation line cards.
- This feature is supported on the Cisco ASR 9000 4th generation line cards with the Cisco IOS XR 64-bit operating system.
- This feature only supports receivers behind multihomed PEs.
- This feature does not support multicast source behind multihomed PEs.
- This feature supports only EVPN multihoming active-active mode.
- This feature does not support the coexistence of L2 IGMP synchronization and L3 IGMP synchronization. You must configure only one mode at any point in time.

Topology



Consider a topology where CE1 is multihomed to PE1 and PE2. When the host sends IGMPv2 or IGMPv3 JOIN to CE1. CE1 hashes the JOIN to either PE2 or PE1. When CE1 hashes the JOIN to PE2. IGMP learns the group as local on PE2. IGMP notifies EVPN and updates MRIB on PE2. BGP advertises IGMP JOIN to PE1 using BGP EVPN route-type 7. Both PE1 and PE2 sends the mVPN C-multicast route (Join) to the source, which is PE3. Both PE1 and PE2 act as a designated router (DR) and receives traffic from PE3. Only one of the PE, either PE1 or PE2 which is the designated forwarder (DF), sends traffic to CE1.

In multihoming active-active mode, both PEs receive the traffic from the core. However, only one of the PEs forwards traffic to CE to avoid duplicate traffic. To enable this, bucket IDs are used. Bucket ID is allotted based on the evpn-route-sync id configured either under VRF or under EVPN. You must configure the same evpn-route-sync id under VRF on both the PEs.

Configure each VRF with a different evpn-route-sync id to enable load balancing. Each VRF is allocated with a different bucket ID. For example, if you configure VRF RED on PE1, and VRF BLUE on PE2, then the routes in VRF RED are allotted bucket ID 1, and routes in VRF BLUE are allotted bucket ID 2. PE1 becomes the DF for bucket ID 1, and PE2 becomes the DF for the bucket ID 2.

Configure EVPN IGMP L3 Synchronization

This section describes how to configure the EVPN IGMP L3 Synchronization feature.

Configuration Example

Peform this task to configure EVPN IGMP L3 Synchronization.

```
/* PE1 Configuration */
Router# configure
Router(config)#  interface Loopback0
Router(config-if)# ipv4 address 10.0.0.1 255.0.0.0
Router(config-if)# exit
Router(config)#  vrf vpn101 -> ESI on non-default VRF
Router(config-vrf)# evpn-route-sync 101
Router(config-vrf)# exit
Router(config)# lacp system mac 0004.0005.0006
Router(config)# commit

Router# configure
Router(config)# router bgp 100
Router(config-bgp)# bgp router-id 10.0.0.1
Router(config-bgp)# address-family l2vpn evpn
Router(config-bgp-af)# exit
Router(config-bgp)# neighbor 172.16.0.1
Router(config-bgp-nbr)#r remote-as 100
Router(config-bgp-nbr)# update-source Loopback0
Router(config-bgp-nbr)# address-family l2vpn evpn
Router(config-bgp-nbr-af)# commit

Router# configure
Router(config)# evpn
Router(config-evpn)# route-sync 2001 -> Associate EVI to default VRF
Router(config-evpn-instance)# vrf default
Router(config-evpn-instance)# exit
Router(config-evpn)# group 1
Router(config-evpn-group)# core interface TenGigE0/1/0/0/4
Router(config-evpn-group)# core interface TenGigE0/1/0/0/5
Router(config-evpn-group)# exit
Router(config-evpn)# interface Bundle-Ether1
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 00.01.00.ac.00.00.01.0a.00
Router(config-evpn-ac-es)# core-isolation-group 1
Router(config-evpn-ac)# commit

Router# configure
Router(config)# interface Bundle-Ether1
Router(config-if)# bundle wait-while 100
Router(config-if)# exit
Router(config)# interface bundle-ether 1.10
Router(config-subif)# vrf vpn101
Router(config-subif)# ipv4 address 192.168.0.1 255.255.0.0
Router(config-subif)# encapsulation dot1q 10
Router(config-subif)# exit
Router(config)# interface bundle-ether 1.20
Router(config-subif)# ipv4 address 192.168.1.1 255.255.0.0
Router(config-subif)# encapsulation dot1q 11
Router(config-subif)# commit


/* PE2 Configuration */
```

```
Router# configure
Router(config)#  interface Loopback0
Router(config-if)# ipv4 address 172.16.0.1 255.240.0.0
Router(config-if)# exit
Router(config)#  vrf vpn101 -> ESI on non-default VRF
Router(config-vrf)# evpn-route-sync 101
Router(config-vrf)# exit
Router(config)# lacp system mac 0004.0005.0006
Router(config)# commit

Router# configure
Router(config)# router bgp 100
Router(config-bgp)# bgp router-id 172.16.0.1
Router(config-bgp)# address-family l2vpn evpn
Router(config-bgp-af)# exit
Router(config-bgp)# neighbor 10.0.0.1
Router(config-bgp-nbr)#r remote-as 100
Router(config-bgp-nbr)# update-source Loopback0
Router(config-bgp-nbr)# address-family l2vpn evpn
Router(config-bgp-nbr-af)# commit

Router# configure
Router(config)# evpn
Router(config-evpn)# route-sync 2001 -> Associate EVI to default VRF
Router(config-evpn-instance)# vrf default
Router(config-evpn-instance)# exit
Router(config-evpn)# group 1
Router(config-evpn-group)# core interface TenGigE0/1/0/0/4
Router(config-evpn-group)# core interface TenGigE0/1/0/0/5
Router(config-evpn-group)# exit
Router(config-evpn)# interface Bundle-Ether1
Router(config-evpn-ac)# ethernet-segment
Router(config-evpn-ac-es)# identifier type 0 00.01.00.ac.00.00.01.0a.00
Router(config-evpn-ac-es)# core-isolation-group 1
Router(config-evpn-ac)# commit

Router# configure
Router(config)# interface Bundle-Ether1
Router(config-if)# bundle wait-while 100
Router(config-if)# exit
Router(config)# interface bundle-ether 1.10
Router(config-subif)# vrf vpn101
Router(config-subif)# ipv4 address 192.168.0.1 255.255.0.0
Router(config-subif)# encapsulation dot1q 10
Router(config-subif)# exit
Router(config)# interface bundle-ether 1.20
Router(config-subif)# ipv4 address 192.168.1.1 255.255.0.0
Router(config-subif)# encapsulation dot1q 11
Router(config-subif)# commit
```

Running Configuration

This section shows the EVPN IGMP L3 synchronization running configuration.

```
/* PE1 Configuratin */
interface Loopback0
 ipv4 address 10.0.0.1 255.0.0.0
!
vrf vpn101  -> ESI on non-default VRF
 evpn-route-sync 101
 !
```

```
lacp system mac 0004.0005.0006
 !
!

router bgp 100
bgp router-id 10.0.0.1
address-family l2vpn evpn
!
neighbor 172.16.0.1
 remote-as 100
 update-source Loopback0
 address-family l2vpn evpn
!
!

evpn
 route-sync 2001  -> Associate EVI to default VRF
  vrf default
!
 group 1
  core interface TenGigE0/1/0/0/4
  core interface TenGigE0/1/0/0/5
 !

 interface Bundle-Ether1
  ethernet-segment
   identifier type 0 00.01.00.ac.00.00.01.0a.00
  !
  core-isolation-group 1
!


interface Bundle-Ether1
 bundle wait-while 100
!
interface Bundle-Ether1.10
 vrf vpn101
 ipv4 address 192.168.0.1 255.255.0.0
 encapsulation dot1q 10
 !
interface Bundle-Ether1.20
 ipv4 address 192.168.1.1 255.255.0.0
 encapsulation dot1q 11
 !


/* PE2 Configuration */
interface Loopback0
 ipv4 address 172.16.0.1  255.240.0.0
!
vrf vpn101  -> ESI on non default VRF
 evpn-route-sync 101
 !
lacp system mac 0004.0005.0006
!

router bgp 100
bgp router-id 172.16.0.1
address-family l2vpn evpn
!
neighbor 10.0.0.1
 remote-as 100
 update-source Loopback0
 address-family l2vpn evpn
!
```

```
!

evpn
 route-sync 2001   -> Associate EVI to default VRF
  vrf default
!
group 1
  core interface TenGigE0/1/0/0/4
  core interface TenGigE0/1/0/0/5
 !

 interface Bundle-Ether1
  ethernet-segment
   identifier type 0 00.01.00.ac.00.00.01.0a.00
  !

  core-isolation-group 1
!
interface Bundle-Ether1
 bundle wait-while 100
!
interface Bundle-Ether1.10
 vrf vpn101
 ipv4 address 192.168.0.1 255.255.0.0
 encapsulation dot1q 10
 !
interface Bundle-Ether1.20
 ipv4 address 192.168.1.1 255.255.0.0
 encapsulation dot1q 11
 !
```

Verification

Verify that you have configured EVPN IGMP L3 synchronization successfully.

```
/* Verify EVPN ethernet-segment peers */
Router# show evpn ethernet-segment

Ethernet Segment Id      Interface                           Nexthops
------------------------ ----------------------------------- --------------------
0000.0100.ac00.0001.0a00 BE1                                 10.0.0.1
                                                             172.16.0.1
------------------------------------------------------------------------------

 /* Verify multihome interface is enabled in IGMP */

Router# show igmp vrf vpn101 interface bundle-ether 1.10
Bundle-Ether1.10 is up, line protocol is up
  Internet address is 192.168.0.1 255.255.0.0
  IGMP_AFD is enabled on interface
  Multihoming is enabled on interface [Stale : False].  -> multihome must be enabled
  Current IGMP version is 3


/* Verify bucket IDS in control plane and hardware */
Router# show mrib evpn bucket-db

EVPN Bucket Database
--------------------

IFName IFHandle BucketID State Uptime Delete In Progress
```

```
Bundle-Ether1 0x20008e0 0 Forward 3d17h N
Bundle-Ether1 0x20008e0 1 Blocked 3d17h N
Bundle-Ether1 0x20008e0 2 Forward 3d17h N
Bundle-Ether1 0x20008e0 3 Blocked 3d17h N
Bundle-Ether1 0x20008e0 4 Forward 3d17h N
Bundle-Ether1 0x20008e0 5 Blocked 3d17h N
Bundle-Ether1 0x20008e0 6 Forward 3d17h N
Bundle-Ether1 0x20008e0 7 Blocked 3d17h N
Bundle-Ether1 0x20008e0 8 Forward 3d17h N
Bundle-Ether1 0x20008e0 9 Blocked 3d17h N
Bundle-Ether1 0x20008e0 10 Forward 3d17h N
Bundle-Ether1 0x20008e0 11 Blocked 3d17h N

Router# show mfib platform evpn bucket location 0/1/CPU0
LC Type: A9K-4X100GE-TR
-------------------------------------------------------
ESI Interface        Handle     Bucket ID State Stale
-------------------------------------------------------
Bundle-Ether1        0x4000620          0       DF     F
Bundle-Ether1        0x4000620          1      NDF     F
Bundle-Ether1        0x4000620          2       DF     F
Bundle-Ether1        0x4000620          3      NDF     F
Bundle-Ether1        0x4000620          4       DF     F
Bundle-Ether1        0x4000620          5      NDF     F
Bundle-Ether1        0x4000620          6       DF     F
Bundle-Ether1        0x4000620          7      NDF     F
Bundle-Ether1        0x4000620          8       DF     F
Bundle-Ether1        0x4000620          9      NDF     F
Bundle-Ether1        0x4000620         10       DF     F
Bundle-Ether1        0x4000620         11      NDF     F
-------------------------------------------------------
If duplicate traffic is seen or one of the PEs is dropping traffic even though the routes
are present, it could be that bucket ID states are incorrect in hardware or control plane.
```

Verify IGMP report in IGMP, EVPN, and BGP.

```
Router:PE1#  show igmp vrf vpn101 groups 209.165.201.1 detail
Interface:      Bundle-Ether1.10
Group:          209.165.201.1
Uptime:         01:11:24
Router mode:    EXCLUDE (Expires: never)
Host mode:      INCLUDE
Last reporter:  10.0.0.2
Suppress:       0
EVPN Remote group: True (Stale: False)  -> Learnt over EVPN
Source list is empty


Router:PE1# show evpn igmp detail
EVI   Ethernet Segment         (S,G)                                                Source
Type
----- ----------------------- ---------------------------------------------- --------------
------
101   0000.0100.ac00.0001.0a00 (0.0.0.0,209.165.201.1)                          172.16.0.1
JOIN
  Ethernet Tag      : 10
  IGMP Version      : V3 [IS_EX]

Router#show bgp l2vpn evpn rd 172.16.0.1:101
[7][0000.0100.ac00.0001.0a00][10][32][0.0.0.0][32][[
209.165.201.1][32][172.16.0.1]/240
BGP routing table entry for
[7][0000.0100.ac00.0001.0a00][10][32][0.0.0.0][32][209.165.201.1][32][172.16.0.1]/240,
Route Distinguisher: 172.16.0.1:101
```

```
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker               6352        6352
Last Modified: Mar 31 00:09:50.666 for 01:42:22
Paths: (1 available, best #1)
  Not advertised to any peer
  Path #1: Received by speaker 0
  Not advertised to any peer
  Local
    172.16.0.1 (metric 3) from 172.16.0.1 (172.16.0.1)
      Origin IGP, localpref 100, valid, internal, best, group-best, import-candidate,
not-in-vrf
      Received Path ID 0, Local Path ID 1, version 6352
      Extended community: EVPN ES Import:0001.00ac.0000 EVI RT:0064.0000.0065
0x060e:0000.ffff.ffff
      IGMP Flags: 0xc

Router:PE2# show igmp vrf vpn101 groups 209.165.201.1 detail

Interface:      Bundle-Ether1.10
Group:          209.165.201.1
Uptime:         01:15:14
Router mode:    EXCLUDE (Expires: 00:02:09)
Host mode:      INCLUDE
Last reporter:  10.0.0.2
Suppress:       0
EVPN Remote group: False (Stale: False)    -> Learnt locally
Source list is empty


Router:PE2# show evpn igmp detail

EVI   Ethernet Segment         (S,G)                          Source             Type
----- ---------------------- ------------------------------ ------------------ ------
101   0000.0100.ac00.0001.0a00 (0.0.0.0,209.165.201.1)      Bundle-Ether1.10    JOIN
  Ethernet Tag      : 10

  IGMP Version      : V3 [IS_EX]

Router:PE2 #show bgp l2vpn evpn rd 172.16.0.1:101
[7][0000.0100.ac00.0001.0a00][10][32][0.0.0.0][32]
[209.165.201.1][32][172.16.0.1]/240
BGP routing table entry for
[7][0000.0100.ac00.0001.0a00][10][32][0.0.0.0][32][209.165.201.1][32][172.16.0.1]/240,
 Route Distinguisher: 172.16.0.1
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker               9328        9328
Last Modified: Mar 31 00:09:47.824 for 01:41:49
Paths: (1 available, best #1)
  Advertised to peers (in unique update groups):
    10.0.0.1
  Path #1: Received by speaker 0
  Advertised to peers (in unique update groups):
    10.0.0.1
  Local
    0.0.0.0 from 0.0.0.0 (172.16.0.1)
      Origin IGP, localpref 100, valid, redistributed, best, group-best, import-candidate,
 rib-install
      Received Path ID 0, Local Path ID 1, version 9328
      Extended community: EVPN ES Import:0001.00ac.0000 EVI RT:0064.0000.0065
0x060e:0000.ffff.ffff
      EVPN ESI: 0000.0000.0000.0000.0000
      IGMP Flags: 0xc
```

```
IGMPv2 report for group is local on PE2 and remote on PE.
```

Verify MRIB entries

For IGMPv2 hosts, only *,G OLEs have bucket IDs displayed in MRIB. The bucket IDs are not displayed for S,G OLE.

For IGMPv3 hosts, S,G OLE bucket IDs are displayed in MRIB.

```
Router:PE1# show mrib vrf vpn101 route 209.165.201.1
(*,209.165.201.1) RPF nbr: 10.0.0.5 Flags: C RPF
  Up: 02:23:51
  Incoming Interface List
    mdtvpn101 Flags: A NS MI, Up: 02:23:51
  Outgoing Interface List
    Bundle-Ether1.10 (0/1/CPU0) Flags: F NS LI MH, Up: 02:23:50

(192.168.0.4,209.165.201.1) RPF nbr: 10.0.0.5 Flags: RPF
  Up: 02:23:07
  Incoming Interface List
    mdtvpn101 Flags: A MI, Up: 02:23:07
  Outgoing Interface List
    Bundle-Ether1.10 (0/1/CPU0) Flags: F NS, Up: 02:23:07


Router:PE1# show mrib vrf vpn101 route 209.165.201.1 priv
Tue Mar 31 02:33:15.978 UTC
(*,209.165.201.1) RPF nbr: 10.0.0.5 Flags: C RPF
  Up: 02:26:22, Route node: 0x556459daff90, In PD retry list: N
  RPF-ID: 1, Encap-ID: 0, EPtr: 0x0, New EPtr: 0x0, New EID: 0, Hd: 0x0, Cts: 0, 0, 0, 0
  Acc: 1, Fwd: 10 (10), Encap-next: 0x0
  Incoming Interface List
   mdtvpn101 Flags: A NS MI, Up: 02:26:22, type 0, Ptrs: 0x556459e14a58, 0x0 0x0 0x0 0x0,
 Bundle Ptrs: 0x0(vp)
 , 0x0(vn) 0x0(pp) 0x0(pn)
   Outgoing Interface List
     Bundle-Ether1.10 (0/1/CPU0, 0x6004980) Flags: F NS LI MH, Up: 02:26:20, type 0, Ptrs:
0x55645a8ba750, 0x0
   0x0 0x0 0x00x55645a5397d8(l) , Bundle Ptrs: 0xf9b20000f8(vp), 0x47a00d37000400(vn)
0x2100000000000040(pp)
0xa19000000001504(pn)
       LI add redist count: 1
       Platform MH MRIB Annotation: ESI: 0x4000620 Bucket ID: 5
 (192.168.0.4,209.165.201.1) RPF nbr: 10.0.0.5 Flags: RPF
   Up: 02:25:37, Route node: 0x55645aabec00, In PD retry list: N
   RPF-ID: 1, Encap-ID: 0, EPtr: 0x0, New EPtr: 0x0, New EID: 0, Hd: 0x0, Cts: 0, 0, 0, 0
   Acc: 1, Fwd: 10 (10), Encap-next: 0x0
   Incoming Interface List
     mdtvpn101 Flags: A MI, Up: 02:25:37, type 0, Ptrs: 0x55645acf7450, 0x0 0x0 0x0 0x0,
 Bundle Ptrs: 0x100000020830000(vp)
 , 0x0(vn) 0x0(pp) 0x100000000000000(pn)
   Outgoing Interface List
     Bundle-Ether1.10 (0/1/CPU0, 0x6004940) Flags: F NS, Up: 02:25:37, type 0, Ptrs:
 0x55645aceb090, 0x0 0x0 0x0 0x00x55645
 a5397f8(l) , Bundle Ptrs: 0x0(vp), 0x0(vn) 0x0(pp) 0x0(pn)


Router:PE2# show mrib vrf vpn101 route 209.165.201.1

(*,209.165.201.1) RPF nbr: 10.0.0.5 Flags: C RPF
  Up: 02:16:24
  Incoming Interface List
```

```
    mdtvpn101 Flags: A NS MI, Up: 02:16:24
  Outgoing Interface List
    Bundle-Ether1.10 (0/0/CPU0) Flags: F NS LI MH, Up: 02:16:24

(192.168.0.4,209.165.201.1) RPF nbr: 10.0.0.5 Flags: RPF
  Up: 02:16:06
  Incoming Interface List
    mdtvpn101 Flags: A MI, Up: 02:16:06
  Outgoing Interface List
    Bundle-Ether1.10 (0/1/CPU0) Flags: F NS, Up: 02:16:06


Router:PE2# show mrib vrf vpn101 route 209.165.201.1 priv
Tue Mar 31 02:27:18.748 UTC
(*,209.165.201.1) RPF nbr: 10.0.0.5 Flags: C RPF
  Up: 02:17:38, Route node: 0x55bb45ca3948, In PD retry list: N
  RPF-ID: 1, Encap-ID: 0, EPtr: 0x0, New EPtr: 0x0, New EID: 0, Hd: 0x0, Cts: 0, 0, 0, 0
  Acc: 1, Fwd: 10 (10), Encap-next: 0x0
  Incoming Interface List
   mdtvpn101 Flags: A NS MI, Up: 02:17:38, type 0, Ptrs: 0x55bb463db210, 0x0 0x0 0x0 0x0,
 Bundle Ptrs: 0x0(vp), 0x0(vn) 0x0(pp) 0x0(pn)
  Outgoing Interface List
    Bundle-Ether1.10 (0/0/CPU0, 0x4d00) Flags: F NS LI MH, Up: 02:17:38, type 0, Ptrs:
 0x55bb45271ae8, 0x0 0x0 0x0 0x00x55bb459d3708(l) , Bundle Ptrs: 0x0(vp), 0x0(vn) 0x0(pp)
  0x0(pn)
      LI add redist count: 3
      Platform MH MRIB Annotation: ESI: 0x2000be0 Bucket ID: 5
 (192.168.0.4,209.165.201.1) RPF nbr: 10.0.0.5 Flags: RPF
   Up: 02:17:19, Route node: 0x55bb45e546b0, In PD retry list: N
   RPF-ID: 1, Encap-ID: 0, EPtr: 0x0, New EPtr: 0x0, New EID: 0, Hd: 0x0, Cts: 0, 0, 0, 0
   Acc: 1, Fwd: 10 (10), Encap-next: 0x0
Incoming Interface List
 mdtvpn101 Flags: A MI, Up: 02:17:19, type 0, Ptrs: 0x55bb4526a708, 0x0 0x0 0x0 0x0,
Bundle Ptrs: 0x0(vp), 0x0(vn) 0x0(pp) 0x0(pn)
 Outgoing Interface List
  Bundle-Ether1.10 (0/1/CPU0, 0x6009ac0) Flags: F NS, Up: 02:17:19, type 0, Ptrs:
0x55bb460068f0, 0x0 0x0 0x0 0x00x55bb459d36a8(l) , Bundle Ptrs: 0x0(vp), 0x0(vn) 0x0(pp)
  0x0(pn)
```

.