



MPLS VPN Support for EIGRP Between PE and CE

The MPLS VPN Support for EIGRP Between PE and CE feature allows service providers to configure the Enhanced Interior Gateway Routing Protocol (EIGRP) between provider edge (PE) and customer edge (CE) devices in a Multiprotocol Label Switching (MPLS) virtual private network (VPN) and offer MPLS VPN services to those customers that require native support for EIGRP. An MPLS VPN consists of a set of sites that are interconnected by an MPLS provider core network. At each customer site, one or more CE devices attach to one or more PE devices.

- [Finding Feature Information, on page 1](#)
- [Prerequisites for MPLS VPN Support for EIGRP Between PE and CE, on page 1](#)
- [Information About MPLS VPN Support for EIGRP Between PE and CE, on page 2](#)
- [How to Configure MPLS VPN Support for EIGRP Between PE and CE, on page 2](#)
- [Configuration Examples for MPLS VPN Support for EIGRP Between PE and CE, on page 8](#)
- [Additional References, on page 10](#)
- [Feature Information for MPLS VPN Support for EIGRP Between PE and CE, on page 10](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see [Bug Search Tool](#) and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for MPLS VPN Support for EIGRP Between PE and CE

- Configure MPLS Layer 3 VPNs.
- Configure the Border Gateway Protocol (BGP) in the network core.

Information About MPLS VPN Support for EIGRP Between PE and CE

Overview of MPLS VPN Support for EIGRP Between PE and CE

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

How to Configure MPLS VPN Support for EIGRP Between PE and CE

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

To configure PE-to-CE routing sessions that use EIGRP, perform this task.

Before you begin

Configure the PE device with the same routing protocol that the CE device uses.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router bgp <i>as-number</i> Example: Device(config)# router bgp 10	Enters router configuration mode, and creates a BGP routing process.
Step 4	no synchronization Example:	Configures BGP to send advertisements without waiting to synchronize with the IGP.

	Command or Action	Purpose
	Device(config-router)# no synchronization	
Step 5	neighbor ip-address remote-as as-number Example: Device(config-router)# neighbor 10.0.0.1 remote-as 10	Establishes peering with the specified neighbor or peer group. <ul style="list-style-type: none"> In this step, you are establishing an iBGP session with the PE device that is connected to the CE device at the other CE site.
Step 6	neighbor ip-address update-source loopback interface-number Example: Device(config-router)# neighbor 10.0.0.1 update-source loopback 0	Configures BGP to use any operational interface for TCP connections. <ul style="list-style-type: none"> This configuration step is not required. However, the BGP routing process will be less susceptible to the effects of interface or link flapping.
Step 7	address-family vpnv4 Example: Device(config-router)# address-family vpnv4	Enters address family configuration mode for configuring routing sessions that use standard IPv4 address prefixes, such as BGP, RIP, and static routing sessions.
Step 8	neighbor ip-address activate Example: Device(config-router-af)# neighbor 10.0.0.1 activate	Establishes peering with the specified neighbor or peer group. <ul style="list-style-type: none"> In this step, you are activating the exchange of VPNv4 routing information between the PE devices.
Step 9	neighbor ip-address send-community extended Example: Device(config-router-af)# neighbor 10.0.0.1 send-community extended	Configures the local device to send extended community attribute information to the specified neighbor. <ul style="list-style-type: none"> This step is required for the exchange of EIGRP extended community attributes.
Step 10	exit-address-family Example: Device(config-router-af)# exit-address-family	Exits address family configuration mode and enters router configuration mode.
Step 11	address-family ipv4 vrf vrf-name Example: Device(config-router)# address-family ipv4 vrf RED	Configures an IPv4 address family for the EIGRP VRF and enters address family configuration mode.

	Command or Action	Purpose
		<ul style="list-style-type: none"> An address-family VRF needs to be configured for each EIGRP VRF that runs between the PE and CE devices.
Step 12	redistribute eigrp <i>as-number</i> [metric <i>metric-value</i>] [route-map <i>map-name</i>] Example: <pre>Device(config-router-af)# redistribute eigrp 101</pre>	Redistributes the EIGRP VRF into BGP. <ul style="list-style-type: none"> The autonomous system number from the CE network is configured in this step.
Step 13	no synchronization Example: <pre>Device(config-router-af)# no synchronization</pre>	Configures BGP to send advertisements without waiting to synchronize with the IGP.
Step 14	exit-address-family Example: <pre>Device(config-router-af)# exit-address-family</pre>	Exits address family configuration mode and enters router configuration mode.
Step 15	end Example: <pre>Device(config-router)# end</pre>	Exits router configuration mode and enters privileged EXEC mode.

Configuring EIGRP Redistribution in the MPLS VPN

Perform this task on every PE device that provides VPN services to enable EIGRP redistribution in the MPLS VPN.

Before you begin

The metric must be configured for routes from external EIGRP autonomous systems and non-EIGRP networks before these routes can be redistributed into an EIGRP CE device. The metric can be configured in the redistribute statement using the **redistribute** (IP) command or can be configured with the **default-metric** (EIGRP) command. If an external route is received from another EIGRP autonomous system or a non-EIGRP network without a configured metric, the route will not be advertised to the CE device.



Note Redistribution between native EIGRP VRFs is not supported. This is designed behavior.

Procedure

	Command or Action	Purpose
Step 1	enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.
Step 2	configure terminal Example: Device# configure terminal	Enters global configuration mode.
Step 3	router eigrp <i>as-number</i> Example: Device(config)# router eigrp 1	Enters router configuration mode and creates an EIGRP routing process. <ul style="list-style-type: none"> • The EIGRP routing process for the PE device is created in this step.
Step 4	address-family ipv4 [multicast unicast vrf <i>vrf-name</i>] Example: Device(config-router)# address-family ipv4 vrf RED	Enters address-family configuration mode and creates a VRF. <ul style="list-style-type: none"> • The VRF name must match the VRF name that was created in the previous section.
Step 5	network <i>ip-address wildcard-mask</i> Example: Device(config-router-af)# network 172.16.0.0 0.0.255.255	Specifies the network for the VRF. <ul style="list-style-type: none"> • The network statement is used to identify which interfaces to include in EIGRP. The VRF must be configured with addresses that fall within the wildcard-mask range of the network statement.
Step 6	redistribute bgp {<i>as-number</i>} [metric <i>bandwidth delay reliability load mtu</i>] [route-map <i>map-name</i>] Example: Device(config-router-af)# redistribute bgp 10 metric 10000 100 255 1 1500	Redistributes BGP into the EIGRP. <ul style="list-style-type: none"> • The autonomous system number and metric of the BGP network are configured in this step. BGP must be redistributed into EIGRP for the CE site to accept the BGP routes that carry the EIGRP information. A metric must also be specified for the BGP network and is configured in this step.
Step 7	autonomous-system <i>as-number</i> Example: Device(config-router-af)# autonomous-system 101	Specifies the autonomous system number of the EIGRP network for the customer site.

	Command or Action	Purpose
Step 8	exit-address-family Example: <pre>Device(config-router-af)# exit-address-family</pre>	Exits address family configuration mode and enters router configuration mode.
Step 9	end Example: <pre>Device(config-router)# end</pre>	Exits router configuration mode and enters privileged EXEC mode.

Verifying Connectivity Between MPLS Virtual Private Network Sites

To verify that the local and remote customer edge (CE) devices can communicate across the Multiprotocol Label Switching (MPLS) core, perform the following tasks:

Verifying IP Connectivity from CE Device to CE Device Across the MPLS Core

Procedure

-
- Step 1** **enable**
Enables privileged EXEC mode.
- Step 2** **ping** [*protocol*] {*host-name* | *system-address*}
Diagnoses basic network connectivity on AppleTalk, Connectionless-mode Network Service (CLNS), IP, Novell, Apollo, Virtual Integrated Network Service (VINES), DECnet, or Xerox Network Service (XNS) networks. Use the **ping** command to verify the connectivity from one CE device to another.
- Step 3** **trace** [*protocol*] [*destination*]
Discovers the routes that packets take when traveling to their destination. The **trace** command can help isolate a trouble spot if two devices cannot communicate.
- Step 4** **show ip route** [*ip-address* [*mask*] [**longer-prefixes**]] | *protocol* [*process-id*] | [**list** [*access-list-name* | *access-list-number*]]
Displays the current state of the routing table. Use the *ip-address* argument to verify that CE1 has a route to CE2. Verify the routes learned by CE1. Make sure that the route for CE2 is listed.
-

Verifying That the Local and Remote CE Devices Are in the PE Routing Table

Procedure

- Step 1** **enable**
Enables privileged EXEC mode.
- Step 2** **show ip route vrf *vrf-name* [*prefix*]**
Displays the IP routing table associated with a virtual routing and forwarding (VRF) instance. Check that the loopback addresses of the local and remote customer edge (CE) devices are in the routing table of the provider edge (PE) devices.
- Step 3** **show ip cef vrf *vrf-name* [*ip-prefix*]**
Displays the Cisco Express Forwarding forwarding table associated with a VRF. Check that the prefix of the remote CE device is in the Cisco Express Forwarding table.
-

Configuration Examples for MPLS VPN Support for EIGRP Between PE and CE

Example: Configuring an MPLS VPN Using EIGRP

PE Configuration	CE Configuration
	<pre>ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0 ip address 10.0.0.9 255.255.255.255 ! interface FastEthernet0/0/0 ip address 34.0.0.1 255.0.0.0 no cdp enable ! router eigrp 1000 network 34.0.0.0 auto-summary</pre>

PE Configuration	CE Configuration
<pre> ip vrf vpn1 rd 100:1 route-target export 100:1 route-target import 100:1 ! ip cef mpls ldp router-id Loopback0 force mpls label protocol ldp ! interface Loopback0 ip address 10.0.0.1 255.255.255.255 interface FastEthernet0/0/0 ip vrf forwarding vpn1 ip address 34.0.0.2 255.0.0.0 no cdp enable interface FastEthernet1/1/0 ip address 30.0.0.1 255.0.0.0 mpls label protocol ldp mpls ip router eigrp 1000 auto-summary ! address-family ipv4 vrf vpn1 redistribute bgp 100 metric 10000 100 255 1 1500 network 34.0.0.0 distribute-list 20 in no auto-summary autonomous-system 1000 exit-address-family ! router bgp 100 no synchronization bgp log-neighbor changes neighbor 10.0.0.3 remote-as 100 neighbor 10.0.0.3 update-source Loopback0 no auto-summary ! address-family vpv4 neighbor 10.0.0.3 activate neighbor 10.0.0.3 send-community extended bgp scan-time import 5 exit-address-family ! address-family ipv4 vrf vpn1 redistribute connected redistribute eigrp no auto-summary no synchronization exit-address-family </pre>	

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco Master Command List, All Releases
MPLS and MPLS applications commands	Cisco IOS Multiprotocol Label Switching Command Reference

Standards and RFCs

Standard/RFC	Title
RFC 4576	<i>Using a Link State Advertisement (LSA) Options Bit to Prevent Looping in BGP/MPLS IP Virtual Private Networks (VPNs)</i>

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for MPLS VPN Support for EIGRP Between PE and CE

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for MPLS VPN Support for EIGRP Between PE and CE

Feature Name	Releases	Feature Information
MPLS VPN Support for EIGRP Between PE and CE	12.0(22)S 12.2(15)T 12.2(18)S 12.2(18)SXD 12.2(27)SBB 12.3(2)T Cisco IOS XE Release 2.1	<p>The MPLS VPN Support for EIGRP Between PE and CE feature allows service providers to configure the Enhanced Interior Gateway Routing Protocol (EIGRP) between provider edge (PE) and customer edge (CE) devices in a Multiprotocol Label Switching (MPLS) virtual private network (VPN) and offer MPLS VPN services to those customers that require native support for EIGRP.</p> <p>In Cisco IOS Release 12.0(22)S, this feature was introduced.</p> <p>In Cisco IOS Release 12.2(15)T, 12.2(18)S, 12.2(18)SXD, 12.2(27)SBB, and 12.3(2)T, this feature was integrated.</p> <p>In Cisco IOS XE Release 2.1, this feature was implemented on Cisco ASR 1000 Series Routers.</p> <p>No commands were introduced or modified.</p>

