BGP Support for the L2VPN Address Family

First Published: February 23, 2007
Last Updated: February 23, 2007

BGP support for the L2VPN address family introduces a BGP-based autodiscovery mechanism to distribute Layer 2 Virtual Private Network (L2VPN) endpoint provisioning information. BGP uses a separate L2VPN routing information base (RIB) to store endpoint provisioning information, which is updated each time any Layer 2 virtual forwarding instance (VFI) is configured. When BGP distributes the endpoint provisioning information in an update message to all its BGP neighbors, the endpoint information is used to set up a pseudowire mesh to support L2VPN-based services.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the "Feature Information for BGP Support for the L2VPN Address Family" section on page 22.

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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

Contents

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for BGP Support for the L2VPN Address Family

This feature assumes prior knowledge of Virtual Private Network (VPN), Virtual Private LAN Service (VPLS), and Multiprotocol Layer Switching (MPLS) technologies.

Restrictions for BGP Support for the L2VPN Address Family

- For route maps used within BGP, all commands related to prefix processing, tag processing, and automated tag processing are ignored when used under L2VPN address family configuration. All other route map commands are supported.
- BGP multipaths and confederations are not supported under the L2VPN address family.

Information About BGP Support for the L2VPN Address Family

To configure BGP support for the L2VPN address family, you should understand the following concept.

L2VPN Address Family

In Cisco IOS Release 12.2(33)SRB and later releases, support for the L2VPN address family is introduced. L2VPN is defined as a secure network that operates inside an unsecured network by using an encryption technology such as IP security (IPsec) or Generic Routing Encapsulation (GRE). The L2VPN address family is configured under BGP routing configuration mode, and within the L2VPN address family the VPLS subsequent address family identifier (SAFI) is supported.

BGP support for the L2VPN address family introduces a BGP-based autodiscovery mechanism to distribute L2VPN endpoint provisioning information. BGP uses a separate L2VPN routing information base (RIB) to store endpoint provisioning information, which is updated each time any Layer 2 VFI is configured. Prefix and path information is stored in the L2VPN database, allowing BGP to make best-path decisions. When BGP distributes the endpoint provisioning information in an update message to all its BGP neighbors, the endpoint information is used to set up a pseudowire mesh to support L2VPN-based services.

The BGP autodiscovery mechanism facilitates the setting up of L2VPN services, which are an integral part of the Cisco IOS Virtual Private LAN Service (VPLS) feature. VPLS enables flexibility in deploying services by connecting geographically dispersed sites as a large LAN over high-speed Ethernet in a robust and scalable IP MPLS network. For more details about VPLS, see the VPLS Autodiscovery: BGP Based feature.

Under L2VPN address family, the following BGP command-line interface (CLI) commands are supported:

- **bgp nexthop**
- **bgp scan-time**

- **neighbor activate**
- **neighbor advertisement-interval**
- **neighbor allowas-in**
- **neighbor capability**
- **neighbor inherit**
- **neighbor maximum-prefix**
- **neighbor next-hop-self**
- **neighbor next-hop-unchanged**
- **neighbor peer-group**
- **neighbor remove-private-as**
- **neighbor route-map**
- **neighbor route-reflector-client**
- **neighbor send-community**
- **neighbor soft-reconfiguration**
- **neighbor soo**
- **neighbor weight**

Note For route reflectors using L2VPNs, the **neighbor next-hop-self** and **neighbor next-hop-unchanged** commands are not supported.

For route maps used within BGP, all commands related to prefix processing, tag processing, and automated tag processing are ignored when used under L2VPN address family configuration. All other route map commands are supported.

BGP multipaths and confederations are not supported under the L2VPN address family.

How to Configure BGP Support for the L2VPN Address Family

This section contains the following task:

- Configuring VPLS Autodiscovery Using BGP and the L2VPN Address Family, page 3

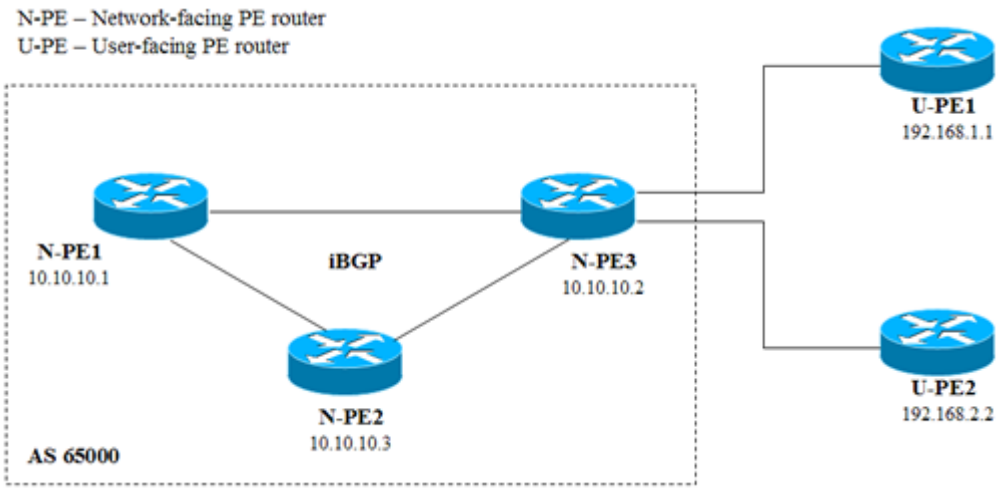
Configuring VPLS Autodiscovery Using BGP and the L2VPN Address Family

Perform this task to implement VPLS autodiscovery of each provider edge (PE) router that is a member of a specific VPLS. In Cisco IOS Release 12.2(33)SRB, the BGP L2VPN address family was introduced with a separate L2VPN routing information base (RIB) that contains endpoint provisioning information. BGP learns the endpoint provisioning information from the L2VPN database, which is updated each time any Layer 2 (L2) virtual forwarding instance (VFI) is configured. When BGP distributes the endpoint provisioning information in an update message to all its BGP neighbors, the endpoint information is used to set up a pseudowire (PW) mesh to support L2VPN-based services.

BGP-based VPLS autodiscovery eliminates the need to manually provision a VPLS neighbor. After a PE router configures itself to be a member of a particular VPLS, information needed to set up connections to remote routers in the same VPLS is distributed by a discovery process. When the discovery process is complete, each member of the VPLS will have the information needed to set up VPLS PWs to form the full mesh of PWs needed for the VPLS.

This task is configured at router N-PE3 in Figure 1 and must be repeated at routers N-PE1 and N-PE2 with the appropriate changes such as different IP addresses. For a full configuration of these routers, see the "Configuring VPLS Autodiscovery Using BGP and the L2VPN Address Family: Example" section on page 9.

Figure 1 Network Diagram for BGP Autodiscovery Using the L2VPN Address Family



In this task, the PE router N-PE3 in Figure 1 is configured with a Layer 2 router ID, a VPN ID, a VPLS ID, and enabled to automatically discover other PE routers that are part of the same VPLS domain. A BGP session is created to activate BGP neighbors under the L2VPN address family. Finally, two optional **show** commands are entered to verify the steps in the task.

VPLS ID

A VPLS ID is a BGP extended community value that identifies the VPLS domain. Manual configuration of this ID is optional because a default VPLS ID is generated using the BGP autonomous system number and the configured VPN ID. A VPLS ID can be composed in one of two ways: with an autonomous system number and an arbitrary number or with an IP address and an arbitrary number.

You can enter a VPLS ID in either of these formats:

- Enter a 16-bit autonomous system number, a colon, and a 32-bit number. For example:

  45000:3

- Enter a 32-bit IP address, a colon, and a 16-bit number. For example:

  192.168.10.15:1

Prerequisites

This task assumes that MPLS is configured with VPLS options. For more details, see the VPLS Autodiscovery: BGP Based feature.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **l2 router-id** *ip-address*
4. **l2 vfi** *vfi-name* **autodiscovery**
5. **vpn id** *vpn-id*
6. **vpls-id** *vpls-id*
7. **exit**
8. Repeat Step 4 through Step 6 to configure other L2 VFIs and associated VPN and VPLS IDs.
9. **router bgp** *autonomous-system-number*
10. **no bgp default ipv4-unicast**
11. **bgp log-neighbor-changes**
12. **bgp update-delay** *seconds*
13. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
14. **neighbor** {*ip-address* | *peer-group-name*} **update-source** *interface-type interface-number*
15. Repeat Step 13 and Step 14 to configure other BGP neighbors.
16. **address-family l2vpn** [**vpls**]
17. **neighbor** {*ip-address* | *peer-group-name*} **activate**
18. **neighbor** {*ip-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**]
19. Repeat Step 17 and Step 18 to activate other BGP neighbors under L2VPN address family.
20. **end**
21. **show vfi**
22. **show ip bgp l2vpn vpls** {**all** | **rd** *vpn-rd*}

DETAILED STEPS

	Command or Action	Purpose

Step 1	`enable`
	
	Example:
	`Router> enable`
		Enables privileged EXEC mode.
		• Enter your password if prompted.

Step 2	`configure terminal`
	
	Example:
	`Router# configure terminal`
		Enters global configuration mode.

Step 3	`l2 router-id` *ip-address* **Example:** `Router(config)# l2 router-id 10.1.1.3`	Specifies a router ID (in IP address format) for the provider edge (PE) router to use with Virtual Private LAN Services (VPLS) autodiscovery pseudowires. • In this example, the L2 router ID is defined as 10.1.1.3.

	Command or Action	Purpose
Step 4	**l2 vfi** *vfi-name* **autodiscovery** **Example:** `Router(config)# l2 vfi customerA autodiscovery`	Creates an L2 VFI, enables the VPLS PE router to automatically discover other PE routers that are part of the same VPLS domain, and enters L2 VFI autodiscovery configuration mode. • In this example, the L2 VFI named customerA is created.
Step 5	**vpn id** *vpn-id* **Example:** `Router(config-vfi)# vpn id 100`	Specifies a VPN ID. • Use the same VPN ID for the PE routers that belong to the same VPN. Make sure that the VPN ID is unique for each VPN in the service provider network. • Use the *vpn-id* argument to specify a number in the range from 1 to 4294967295. • In this example, a VPN ID of 100 is specified.
Step 6	**vpls-id** *vpls-id* **Example:** `Router(config-vfi)# vpls-id 65000:100`	(Optional) Specifies a VPLS ID. • The VPLS ID is an identifier that is used to identify the VPLS domain. This command is optional because a default VPLS ID is automatically generated using the BGP autonomous-system number and the VPN ID configured for the VFI. Only one VPLS ID can be configured per VFI, and the same VPLS ID cannot be configured in multiple VFIs on the same router. • In this example, a VPLS ID of 65000:100 is specified.
Step 7	**exit** **Example:** `Router(config-vfi)# exit`	Exits L2 VFI autodiscovery configuration mode and returns to global configuration mode.
Step 8	Repeat Step 4 through Step 6 to configure other L2 VFIs and associated VPN and VPLS IDs.	—
Step 9	**router bgp** *autonomous-system-number* **Example:** `Router(config)# router bgp 65000`	Enters router configuration mode for the specified routing process.
Step 10	**no bgp default ipv4-unicast** **Example:** `Router(config-router)# no bgp default ipv4-unicast`	Disables the IPv4 unicast address family for the BGP routing process. **Note** Routing information for the IPv4 unicast address family is advertised by default for each BGP routing session configured with the **neighbor remote-as** router configuration command unless you configure the **no bgp default ipv4-unicast** router configuration command before configuring the **neighbor remote-as** command. Existing neighbor configurations are not affected.

	Command or Action	Purpose
Step 11	**bgp log-neighbor-changes** **Example:** `Router(config-router)# bgp log-neighbor-changes`	Enables logging of BGP neighbor resets.
Step 12	**bgp update-delay** *seconds* **Example:** `Router(config-router)# bgp update-delay 1`	Sets the maximum initial delay period before a BGP-speaking networking device sends its first updates. • Use the *seconds* argument to set the delay period.
Step 13	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* **Example:** `Router(config-router)# neighbor 10.10.10.1 remote-as 65000`	Adds the IP address or peer group name of the neighbor in the specified autonomous system to the IPv4 multiprotocol BGP neighbor table of the local router. • If the *autonomous-system-number* argument matches the autonomous system number specified in the **router bgp** command, the neighbor is an internal neighbor. • If the *autonomous-system-number* argument does not match the autonomous system number specified in the **router bgp** command, the neighbor is an external neighbor. • In this example, the neighbor at 10.10.10.1 is an internal BGP neighbor.
Step 14	**neighbor** {*ip-address* | *peer-group-name*} **update-source** *interface-type interface-number* **Example:** `Router(config-router)# neighbor 10.10.10.1 update-source loopback1`	(Optional) Configures a router to select a specific source or interface to receive routing table updates. • This example uses a loopback interface. The advantage to this configuration is that the loopback interface is not as susceptible to the effects of a flapping interface.
Step 15	Repeat Step 13 and Step 14 to configure other BGP neighbors.	—
Step 16	**address-family l2vpn** [**vpls**] **Example:** `Router(config-router)# address-family l2vpn vpls`	Specifies the L2VPN address family and enters address family configuration mode. • The optional **vpls** keyword specifies that VPLS endpoint provisioning information is to be distributed to BGP peers. • In this example, an L2VPN VPLS address family session is created.
Step 17	**neighbor** *ip-address* **activate** **Example:** `Router(config-router-af)# neighbor 10.10.10.1 activate`	Enables the neighbor to exchange information for the L2VPN VPLS address family with the local router. **Note** If you have configured a BGP peer group as a neighbor, you do not use this step. BGP peer groups are activated when a BGP parameter is configured. For example, the **neighbor send-community** command in the next step will automatically activate a peer group.

	Command or Action	Purpose
Step 18	**neighbor** {*ip-address* | *peer-group-name*} **send-community** [**both** | **standard** | **extended**] **Example:** `Router(config-router-af)# neighbor 10.10.10.1 send-community extended`	Specifies that a communities attribute should be sent to a BGP neighbor. • In this example, an extended communities attribute is sent to the neighbor at 10.10.10.1.
Step 19	Repeat Step 17 and Step 18 to activate other BGP neighbors under L2VPN address family.	—
Step 20	**end** **Example:** `Router(config-router-af)# end`	Exits address family configuration mode and returns to privileged EXEC mode.
Step 21	**show vfi** **Example:** `Router# show vfi`	(Optional) Displays information about the configured VFI instances.
Step 22	**show ip bgp l2vpn vpls** {**all** | **rd** *vpn-rd*} **Example:** `Router# show ip bgp l2vpn vpls all`	(Optional) Displays information about the L2 VPN VPLS address family.

Examples

The following is example output from the **show vfi** command that shows two VFIs, CustomerA and CustomerB, with their associated VPN and VPLS IDs:

```
Router# show vfi

Legend: RT=Route-target, S=Split-horizon, Y=Yes, N=No

VFI name: customerA, state: down, type: multipoint
  VPN ID: 100, VPLS-ID: 65000:100
  RD: 65000:100, RT: 65000:100
  Local attachment circuits:
  Neighbors connected via pseudowires:
  Peer Address     VC ID        Discovered Router ID    S
  10.10.10.1         100        10.10.10.99             Y

VFI name: customerB, state: down, type: multipoint
  VPN ID: 200, VPLS-ID: 65000:200
  RD: 65000:200, RT: 65000:200
  Local attachment circuits:
  Neighbors connected via pseudowires:
  Peer Address     VC ID        Discovered Router ID    S
  10.10.10.3         200                10.10.10.98    Y
```

The following is example output from the **show ip bgp l2vpn vpls all** command that shows two VFIs identified by their VPN route distinguisher:

```
Router# show ip bgp l2vpn vpls all

BGP table version is 5, local router ID is 10.10.10.2
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
```

```
             r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 65000:100
*> 65000:100:10.10.10.1/96
                     0.0.0.0                              32768 ?
*>i65000:100:192.168.1.1/96
                     10.10.10.2               0    100      0 ?
Route Distinguisher: 65000:200
*> 65000:200:10.10.10.3/96
                     0.0.0.0                              32768 ?
*>i65000:200:192.168.2.2/96
                     10.10.10.2               0    100      0 ?
```

What to Do Next

To configure more VPLS features, see the main VPLS documentation in the VPLS Autodiscovery: BGP Based feature.

Configuration Examples for BGP Support for the L2VPN Address Family

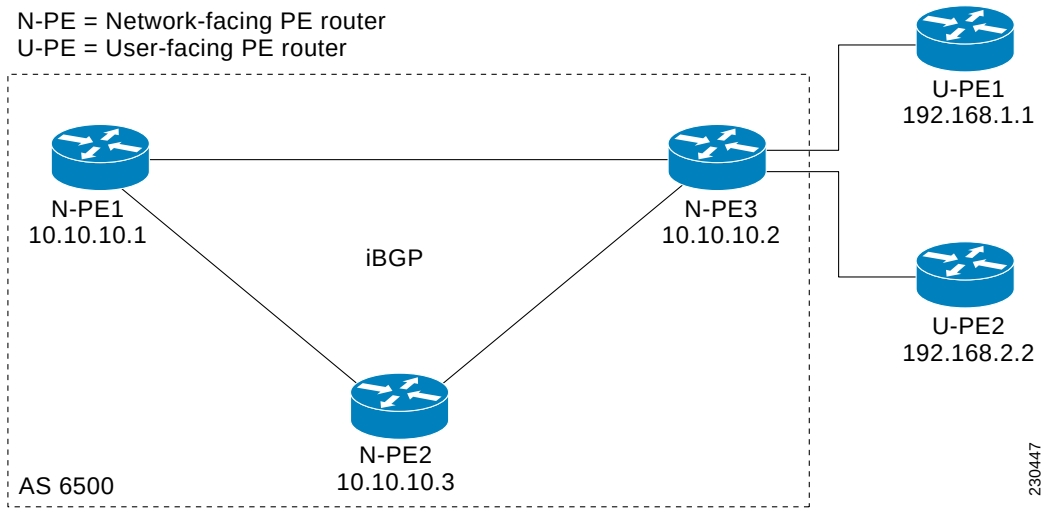
This section contains the following configuration example:

- Configuring VPLS Autodiscovery Using BGP and the L2VPN Address Family: Example, page 9

Configuring VPLS Autodiscovery Using BGP and the L2VPN Address Family: Example

In this configuration example, all the routers in autonomous system 65000 in Figure 2 are configured to provide BGP support for the L2VPN address family. VPLS autodiscovery is enabled and L2 VFI and VPN IDs are configured. BGP neighbors are configured and activated under L2VPN address family to ensure that the VPLS endpoint provisioning information is saved to a separate L2VPN RIB and then distributed to the other BGP peers in BGP update messages. When the endpoint information is received by the BGP peers, a pseudowire mesh is set up to support L2VPN-based services.

Figure 2 Network Diagram for VPLS Autodiscovery Using BGP and the L2VPN Address Family



Router N-PE1

```
ip subnet-zero
ip cef
no ip dhcp use vrf connected
!
no mpls traffic-eng auto-bw timers frequency 0
mpls label range 1000 2000
mpls label protocol ldp
l2 router-id 10.1.1.1
l2 vfi auto autodiscovery
 vpn id 100
!
pseudowire-class mpls
 encapsulation mpls
!
interface Loopback1
 ip address 10.1.1.1 255.255.255.255
!
interface Ethernet0/0
 description Backbone interface
 ip address 10.0.0.1 255.255.255.0
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 10.10.1.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.0.255 area 0
!
router bgp 65000
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp update-delay 1
 neighbor 10.10.10.2 remote-as 65000
 neighbor 10.10.10.2 update-source Loopback1
 neighbor 10.10.10.3 remote-as 65000
 neighbor 10.10.10.3 update-source Loopback1
!
 address-family l2vpn vpls
 neighbor 10.10.10.2 activate
 neighbor 10.10.10.2 send-community extended
 neighbor 10.10.10.3 activate
```

```
 neighbor 10.10.10.3 send-community extended
 exit-address-family
!
ip classless
```

Router N-PE2

```
ip subnet-zero
ip cef
no ip dhcp use vrf connected
!
no mpls traffic-eng auto-bw timers frequency 0
mpls label range 2000 3000
mpls label protocol ldp
l2 router-id 10.1.1.2
l2 vfi auto autodiscovery
 vpn id 100
!
pseudowire-class mpls
 encapsulation mpls
!
interface Loopback1
 ip address 10.1.1.2 255.255.255.255
!
interface Ethernet0/0
 description Backbone interface
 ip address 10.0.0.2 255.255.255.0
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 10.10.1.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.0.255 area 0
!
router bgp 65000
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp update-delay 1
 neighbor 10.10.10.1 remote-as 65000
 neighbor 10.10.10.1 update-source Loopback1
 neighbor 10.10.10.3 remote-as 65000
 neighbor 10.10.10.3 update-source Loopback1
!
 address-family l2vpn vpls
 neighbor 10.10.10.1 activate
 neighbor 10.10.10.1 send-community extended
 neighbor 10.10.10.3 activate
 neighbor 10.10.10.3 send-community extended
 exit-address-family
!
ip classless
```

Router N-PE3

```
ip subnet-zero
ip cef
no ip dhcp use vrf connected
!
no mpls traffic-eng auto-bw timers frequency 0
mpls label range 2000 3000
mpls label protocol ldp
l2 router-id 10.1.1.3
l2 vfi auto autodiscovery
 vpn id 100
```

```
!
pseudowire-class mpls
 encapsulation mpls
!
interface Loopback1
 ip address 10.1.1.3 255.255.255.255
!
interface Ethernet0/0
 description Backbone interface
 ip address 10.0.0.3 255.255.255.0
 mpls ip
!
router ospf 1
 log-adjacency-changes
 network 10.10.1.0 0.0.0.255 area 0
 network 192.168.0.0 0.0.0.255 area 0
!
router bgp 65000
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp update-delay 1
 neighbor 10.10.10.1 remote-as 65000
 neighbor 10.10.10.1 update-source Loopback1
 neighbor 10.10.10.2 remote-as 65000
 neighbor 10.10.10.2 update-source Loopback1
!
 address-family l2vpn vpls
 neighbor 10.10.10.1 activate
 neighbor 10.10.10.1 send-community extended
 neighbor 10.10.10.2 activate
 neighbor 10.10.10.2 send-community extended
 exit-address-family
!
ip classless
```

Where to Go Next

For more details about configuring VPLS autodiscovery, see the VPLS Autodiscovery: BGP Based feature.

Additional References

The following sections provide references related to the BGP Support for the L2VPN Address Family feature.

Related Documents

Related Topic	Document Title
BGP commands: complete command syntax, command mode, defaults, command history, usage guidelines, and examples	*Cisco IOS IP Routing Protocols Command Reference*, Release 12.2SR
BGP overview	"Cisco BGP Overview" module
Configuring basic BGP tasks	"Configuring a Basic BGP Network" module

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	—

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	—

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register on Cisco.com.	http://www.cisco.com/techsupport

Command Reference

This section documents only commands that are new or modified.

- **address-family l2vpn**
- **clear ip bgp l2vpn**
- **show ip bgp l2vpn**

address-family l2vpn

To enter address family configuration mode to configure a routing session using Layer 2 Virtual Private Network (L2VPN) endpoint provisioning address information, use the **address-family l2vpn** command in router configuration mode. To remove the L2VPN address family configuration from the running configuration, use the **no** form of this command.

address-family l2vpn [**vpls**]

no address-family l2vpn [**vpls**]

Syntax Description

vpls	(Optional) Specifies L2VPN Virtual Private LAN Service (VPLS) endpoint provisioning address information.

Command Default

No L2VPN endpoint provisioning support is enabled.

Command Modes

Router configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

The **address-family l2vpn** command places the router in address family configuration mode (prompt: `config-router-af`), from which you can configure routing sessions that support L2VPN endpoint provisioning.

BGP support for the L2VPN address family introduces a BGP-based autodiscovery mechanism to distribute L2VPN endpoint provisioning information. BGP uses a separate L2VPN routing information base (RIB) to store endpoint provisioning information, which is updated each time any Layer 2 (L2) virtual forwarding instance (VFI) is configured. Prefix and path information is stored in the L2VPN database, allowing BGP to make best-path decisions. When BGP distributes the endpoint provisioning information in an update message to all its BGP neighbors, the endpoint information is used to set up a pseudowire mesh to support L2VPN-based services.

The BGP autodiscovery mechanism facilitates the setting up of L2VPN services, which are an integral part of the Cisco IOS Virtual Private LAN Service (VPLS) feature. VPLS enables flexibility in deploying services by connecting geographically dispersed sites as a large LAN over high-speed Ethernet in a robust and scalable IP MPLS network.

Note Routing information for address family IPv4 is advertised by default for each BGP routing session configured with the **neighbor remote-as** command unless you configure the **no bgp default ipv4-unicast** command before configuring the **neighbor remote-as** command.

Examples

In this example, two provider edge (PE) routers are configured with VPLS endpoint provisioning information that includes L2 VFI, VPN, and VPLS IDs. BGP neighbors are configured and activated under L2VPN address family to ensure that the VPLS endpoint provisioning information is saved to a separate L2VPN RIB and then distributed to other BGP peers in BGP update messages. When the endpoint information is received by the BGP peers, a pseudowire mesh is set up to support L2VPN-based services.

Router A

```
enable
configure terminal
l2 vfi customerA autodiscovery
 vpn id 100
 vpls-id 45000:100
 exit
l2 vfi customerB autodiscovery
 vpn id 200
 vpls-id 45000:200
 exit
router bgp 45000
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 172.16.1.2 remote-as 45000
 neighbor 172.21.1.2 remote-as 45000
 address-family l2vpn vpls
 neighbor 172.16.1.2 activate
 neighbor 172.16.1.2 send-community extended
 neighbor 172.21.1.2 activate
 neighbor 172.21.1.2 send-community extended
 end
```

Router B

```
enable
configure terminal
l2 vfi customerA autodiscovery
 vpn id 100
 vpls-id 45000:100
 exit
l2 vfi customerB autodiscovery
 vpn id 200
 vpls-id 45000:200
 exit
router bgp 45000
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 neighbor 172.16.1.1 remote-as 45000
 neighbor 172.22.1.1 remote-as 45000
 address-family l2vpn vpls
 neighbor 172.16.1.1 activate
 neighbor 172.16.1.1 send-community extended
 neighbor 172.22.1.1 activate
 neighbor 172.22.1.1 send-community extended
 end
```

Related Commands

Command	Description
neighbor activate	Enables the exchange of information with a BGP neighboring router.
show ip bgp l2vpn	Displays L2VPN address family information.

clear ip bgp l2vpn

To reset Border Gateway Protocol (BGP) neighbor session information for Layer 2 Virtual Private Network (L2VPN) address family, use the **clear ip bgp l2vpn** command in privileged EXEC mode.

clear ip bgp l2vpn vpls {*autonomous-system-number* | **peer-group** *peer-group-name* | **update-group** [*number* | *ip-address*]} [**in** [**prefix-filter**] | **out** | **soft** [**in** [**prefix-filter**] | **out**]]

Syntax Description

vpls	Specifies that Virtual Private LAN Service (VPLS) subsequent address family identifier (SAFI) information will be cleared.
autonomous-system-number	Autonomous system number in which peers are reset.
peer-group *peer-group-name*	Clears peer group information for the peer group specified with the *peer-group-name* argument.
update-group	Clears update group session information.
number	(Optional) Clears update-group session information for the specified update group number.
ip-address	(Optional) Clears update-group session information for the peer specified with the *ip-address* argument.
in	(Optional) Initiates inbound reconfiguration. If neither the **in** keyword nor **out** keyword is specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Clears the inbound prefix filter.
out	(Optional) Initiates outbound reconfiguration. If neither the **in** keyword nor **out** keyword is specified, both inbound and outbound sessions are reset.
soft	(Optional) Initiates a soft reset. Does not tear down the session.

Command Default

If no arguments or keywords are specified, all BGP L2VPN VPLS neighbor session information is cleared.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

The **clear ip bgp l2vpn** command clears BGP session information for the L2VPN address family and VPLS SAFI. This command can be used to initiate a hard reset or soft reconfiguration. A hard reset tears down and rebuilds the specified peering sessions and rebuilds the BGP routing tables. A soft reconfiguration uses stored prefix information to reconfigure and activate BGP routing tables without tearing down existing peering sessions. Soft reconfiguration uses stored update information, at the cost of additional memory for storing the updates, to allow you to apply new BGP policy without disrupting the network. Soft reconfiguration can be configured for inbound or outbound sessions.

Generating Updates from Stored Information

To generate new inbound updates from stored update information (rather than dynamically) without resetting the BGP session, you must preconfigure the local BGP router using the **neighbor soft-reconfiguration inbound** command. This preconfiguration causes the software to store all received updates without modification regardless of whether an update is accepted by the inbound policy. Storing updates is memory intensive and should be avoided if possible.

Outbound BGP soft configuration has no memory overhead and does not require any preconfiguration. You can trigger an outbound reconfiguration on the other side of the BGP session to make the new inbound policy take effect.

Use the **clear ip bgp l2vpn** command whenever any of the following changes occur:

- Additions or changes to the BGP-related access lists
- Changes to BGP-related weights
- Changes to BGP-related distribution lists
- Changes to BGP-related route maps

Dynamic Inbound Soft Reset

The route refresh capability, as defined in RFC 2918, allows the local router to reset inbound routing tables dynamically by exchanging route refresh requests to supporting peers. The route refresh capability does not store update information locally for non-disruptive policy changes. It instead relies on dynamic exchange with supporting peers. Route refresh is advertised through BGP capability negotiation. All BGP routers must support the route refresh capability.

To determine if a BGP router supports this capability, use the **show ip bgp neighbors** command. The following message is displayed in the output when the router supports the route refresh capability:

```
Received route refresh capability from peer.
```

If all BGP routers support the route refresh capability, use the **clear ip bgp l2vpn vpls** {*autonomous-system-number* | **peer-group** *peer-group-name* | **update-group** [*number* | *ip-address*]} **in** command. You need not use the **soft** keyword, because soft reset is automatically assumed when the route refresh capability is supported.

Note After a soft reset (inbound or outbound) is configured, it is normal for the BGP routing process to hold memory. The amount of memory that is held depends on the size of the routing tables and the percentage of memory chunks that are utilized. Partially used memory chunks will be used or released before more memory is allocated from the global router memory pool.

Examples

The following example configures soft reconfiguration for the inbound session with BGP L2VPN peers in the 45000 autonomous system. The outbound session is unaffected:

```
Router# clear ip bgp l2vpn vpls 45000 soft in
```

Related Commands

Command	Description
address-family l2vpn	Enters address family configuration mode to configure a routing session using L2VPN endpoint provisioning information.
neighbor soft-reconfiguration	Configures the Cisco IOS software to start storing updates.

show ip bgp l2vpn

To display Layer 2 Virtual Private Network (L2VPN) address family information from the Border Gateway Protocol (BGP) table, use the **show ip bgp l2vpn** command in user EXEC or privileged EXEC mode.

With BGP show Command Argument

show ip bgp l2vp vpls {**all** | **rd** *route-distinguisher*} [*bgp-keyword*]

With IP Prefix and Mask Length Syntax

show ip bgp l2vp vpls {**all** | **rd** *route-distinguisher*} [*ip-prefix/length* [**bestpath**] [**longer-prefixes** [**injected**]] [**multipaths**] [**shorter-prefixes** [*mask-length*]] [**subnets**]]

With Network Address Syntax

show ip bgp l2vp vpls {**all** | **rd** *route-distinguisher*} [*network-address* [*mask* | **bestpath** | **multipaths**] [**bestpath**] [**longer-prefixes** [**injected**]] [**multipaths**] [**shorter-prefixes** [*mask-length*]] [**subnets**]]

Syntax Description

vpls	Displays L2VPN address family database information for the Virtual Private LAN Service (VPLS) subsequent address family identifier (SAFI).
all	Displays the complete L2VPN database.
rd *route-distinguisher*	Displays prefixes that match the specified route distinguisher.
bgp-keyword	(Optional) Argument representing a **show ip bgp** command keyword that can be added to this command. See Table 1.
ip-prefix/length	(Optional) The IP prefix address (in dotted decimal format) and the length of the mask (0 to 32). The slash mark must be included.
network-address	(Optional) The IP address of a network in the BGP routing table.
mask	(Optional) The mask of the network address, in dotted decimal format.
bestpath	(Optional) Displays the best path for the specified prefix.
longer-prefixes	(Optional) Displays the route and more specific routes.
injected	(Optional) Displays more specific routes that were injected because of the specified prefix.
multipaths	(Optional) Displays the multipaths for the specified prefix.
shorter-prefixes	(Optional) Displays the less specific routes.
mask-length	(Optional) The length of the mask as a number in the range from 0 to 32. Prefixes longer than the specified mask length are displayed.
subnets	(Optional) Displays the subnet routes for the specified prefix.

Command Default

If no arguments or keywords are specified, this command displays the complete L2VPN database.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(33)SRB	This command was introduced.

Usage Guidelines

Table 1 displays optional **show ip bgp** command keywords that can be configured with the **show ip bgp l2vpn** command. Replace the *bgp-keyword* argument with the appropriate keyword from the table. For more details about each command in its **show ip bgp** *bgp-keyword* form, see the *Cisco IOS IP Routing Protocols Command Reference*, Release 12.2SR.

Table 1 Optional show ip bgp Command Keywords and Descriptions

Keyword	Description
community	Displays routes that match a specified community
community-list	Displays routes that match a specified community list.
dampening	Displays paths suppressed because of dampening (BGP route from peer is up and down).
extcommunity-list	Displays routes that match a specified extcommunity list.
filter-list	Displays routes that conform to the filter list.
inconsistent-as	Displays only routes that have inconsistent autonomous systems of origin.
neighbors	Displays details about TCP and BGP neighbor connections.
oer-paths	Displays all OER-managed path information.
paths [*regexp*]	Displays autonomous system path information. If the optional *regexp* argument is entered, the autonomous system paths that are displayed match the autonomous system path regular expression.
peer-group	Displays information about peer groups.
pending-prefixes	Displays prefixes that are pending deletion.
prefix-list	Displays routes that match a specified prefix list.
quote-regexp	Displays routes that match the quoted autonomous system path regular expression.
regexp	Displays routes that match the autonomous system path regular expression.
replication	Displays the replication status update groups.
route-map	Displays routes that match the specified route map.
rt-filter-list	Displays the specified inbound route target filter list.
summary	Displays a summary of BGP neighbor status.
update-group	Displays information on update groups.

Examples

The following example shows output for the **show ip bgp l2vpn** command when the **vpls** and **all** keywords are used to display the complete L2VPN database:

```
Router# show ip bgp l2vpn vpls all

BGP table version is 5, local router ID is 192.168.3.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 45000:100
*> 45000:100:172.17.1.1/96
                    0.0.0.0                            32768 ?
*>i45000:100:172.18.2.2/96
                    172.16.1.2               0    100      0 ?
Route Distinguisher: 45000:200
*> 45000:200:172.17.1.1/96
                    0.0.0.0                            32768 ?
*>i45000:200:172.18.2.2/96
                    172.16.1.2               0    100      0 ?
```

Table 2 describes the significant fields shown in the display.

Table 2 show ip bgp l2vpn vpls all Field Descriptions

Field	Description
BGP table version	Internal version number of the table. This number is incremented whenever the table changes.
local router ID	IP address of the router.
Status codes	Status of the table entry. The status is displayed at the beginning of each line in the table. It can be one of the following values: • s—The table entry is suppressed. • d—The table entry is dampened. • h—The table entry is a historical entry. • *—The table entry is valid. • >—The table entry is the best entry to use for that network. • i—The table entry was learned via an internal BGP (iBGP) session. • r—The table entry failed to install in the routing information base (RIB) table. • S—The table entry is Stale (old). This entry is useful in BGP graceful restart situations.

Table 2 show ip bgp l2vpn vpls all Field Descriptions (continued)

Field	Description
Origin codes	Origin of the entry. The origin code is displayed at the end of each line in the table. It can be one of the following values: • i—Entry originated from an Interior Gateway Protocol (IGP) and was advertised with a network router configuration command. • e—Entry originated from an Exterior Gateway Protocol (EGP). • ?—Origin of the path is not clear. Usually, this is a router that is redistributed into BGP from an IGP.
Network	IP address of a network entity.
Next Hop	IP address of the next system that is used when forwarding a packet to the destination network. An entry of 0.0.0.0 indicates that the router has some non-BGP routes to this network.
Metric	If shown, the value of the interautonomous system metric.
LocPrf	Local preference value as set with the set local-preference route-map configuration command. The default value is 100.
Weight	Weight of the route as set via autonomous system filters.
Path	Autonomous system paths to the destination network. There can be one entry in this field for each autonomous system in the path.
Route Distinguisher	Route distinguisher that identifies a set of routing and forwarding tables used in virtual private networks.

The following example shows output for the **show ip bgp l2vpn** command when the **vpls** and **rd** keywords are used to display the L2VPN information that matches the route distinguisher 45000:100. Note that the information displayed is a subset of the information displayed using the **all** keyword.

```
Router# show ip bgp l2vpn vpls rd 45000:100

BGP table version is 5, local router ID is 192.168.3.1
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 45000:100
*> 45000:100:172.17.1.1/96
                    0.0.0.0                              32768 ?
*>i45000:100:172.18.2.2/96
                    172.16.1.2               0    100      0 ?
```

Related Commands

Command	Description
address-family l2vpn	Enters address family configuration mode to configure a routing session using L2VPN endpoint provisioning information.

Feature Information for BGP Support for the L2VPN Address Family

Table 3 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Note Table 3 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 3 Feature Information for BGP Support for the L2VPN Address Family

Feature Name	Releases	Feature Information
BGP Support for the L2VPN Address Family	12.2(33)SRB	BGP support for the L2VPN address family introduces a BGP-based autodiscovery mechanism to distribute L2VPN endpoint provisioning information. BGP uses a separate L2VPN routing information base (RIB) to store endpoint provisioning information, which is updated each time any Layer 2 VFI is configured. When BGP distributes the endpoint provisioning information in an update message to all its BGP neighbors, the endpoint information is used to set up a pseudowire mesh to support L2VPN-based services. In 12.2(33)SRB, this feature was introduced on the Cisco 7600 platform. The following commands were introduced or modified by this feature: **address-family l2vpn**, **clear ip bgp l2vpn**, **show ip bgp l2vpn**.