VPLS BGP Signaling L2VPN Inter-AS Option A

The Virtual Private LAN Switching (VPLS) Border Gateway Protocol (BGP) Signaling Layer 2 Virtual Private Network (L2VPN) feature simplifies the auto-discovery and signaling of all known PE devices in a VPLS instance by using BGP.

- Finding Feature Information, on page 1
- Prerequisites for VPLS BGP Signaling L2VPN Inter-AS Option A, on page 1
- Information About VPLS BGP Signaling L2VPN Inter-AS Option A, on page 2
- How to Configure VPLS BGP Signaling L2VPN Inter-AS Option A, on page 3
- VPLS BGP Signaling L2VPN Inter-AS Option A: Example, on page 8
- Additional References for VPLS Autodiscovery BGP Based, on page 9
- Feature Information for VPLS BGP Signaling L2VPN Inter-AS Option A, 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 VPLS BGP Signaling L2VPN Inter-AS Option A

- The Control word must turned off for VPLS BGP signaling by using the **no control-word** command under a pseudowire class. For example:

```
Router> enable
Router# configure terminal
Router(config)# pseudowire-class my_pw_class
Router(config-pw-class)# no control-word
```

- The Route Distinguisher (RD) must match for all the virtual forwarding instances (VFIs) in a VPLS domain.

Information About VPLS BGP Signaling L2VPN Inter-AS Option A

BGP Auto-discovery and Signaling for VPLS

The Virtual Private LAN Switching (VPLS) control plane is used for auto-discovery and signaling. Auto-discovery involves locating all provider edge (PE) devices that participate in a particular VPLS instance. Signaling is accomplished by configuring pseudowires for a VPLS instance. Prior to the introduction of the VPLS BGP Signaling L2VPN Inter-AS Option B feature, Label Distribution Protocol (LDP) was used for signaling and Border Gateway Protocol (BGP) was used for auto-discovery, as specified in RFC 6074. With the introduction of the VPLS BGP Signaling L2VPN Inter-AS Option B feature, the VPLS BGP Signaling L2VPN feature supports RFC 4761 by simplifying the auto-discovery and signaling of all known PE devices in a VPLS instance by using BGP for both functions. Auto-discovery is defined per VPLS instance.

Internal BGP (IBGP) peers exchange update messages of the L2VPN Address Family Identifier (AFI) and the Subsequent Address Family Identifier (SAFI) numbers with L2VPN information to perform both auto-discovery and signaling, which includes the Network Layer Reachability Information (NLRI).

Both BGP standards (RFC 6074 and RFC 4761) for the auto-discovery protocol for VPLS use the same BGP AFI (25) and SAFI (65) but they have different Network Layer Reachability Information (NLRI) encoding, which makes them incompatible with each other. CLI configuration is needed to distinguish the two encoding types as they are mutually exclusive per neighbor. The difference between the two BGP standards is:

- RFC 6074 provides guidelines for specifying length encoding as bits.
- RFC 4761 provides guidelines for specifying length encoding as bytes.

To detect which NLRI encoding standard is supported, the length encoding needs to be determined.

BGP L2VPN Signaling with NLRI

Network Layer Reachability Information (NLRI) enables Border Gateway Protocol (BGP) to carry supernetting information, as well as perform aggregation. Each NLRI consists of block labels that follow the structure LB, LB+1, ... , LB+VBS-1. The NLRI is exchanged between BGP devices for BGP auto-discovery with BGP signaling. The following fields are configured or auto-generated for each Virtual Private LAN Switching (VPLS) instance:

- Length (2 Octets)
- Route distinguisher (RD) is usually an auto-generated 8-byte VPN ID that can also be configured. This value must be unique for a VPLS bridge-domain (or instance).
- VPLS Endpoint ID (VEID) (2 Octets). Each PE device is configured with a VEID value.
- VPLS Endpoint Block Offset (VBO) (2 Octets).
- VPLS Endpoint Block Size (VBS) (2 Octets).
- Label Base (LB) (3 Octets).

- Extended Community Type (2 Octets) - 0x800A attributes. The Route Target (RT) specified for a VPLS instance, next-hop and other Layer 2 information is carried in this encoding. An RT-based import and export mechanism similar to L3VPN is performed by BGP to perform filtering on the L2VPN NLRIs of a particular VPLS instance.
- Encapsulation Type (1 Octet) - VPLS = 19
- Control Flags (1 Octet)
- Layer 2 Maximum Transmission Unit (MTU) (2 Octets)
- Reserved (2 Octets)

How to Configure VPLS BGP Signaling L2VPN Inter-AS Option A

Enabling BGP Auto-discovery and BGP Signaling

Perform this task to enable Virtual Private LAN Service (VPLS) PE devices to discover other PE devices by BGP auto-discovery and BGP signaling functions announced through IBGP.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **l2vpn vfi context** *vfi-context-name*
4. **vpn id** *vpn-id*
5. **autodiscovery bgp signaling bgp**
6. **ve id** *ve-ID-number*
7. **ve range** *ve-range-number*
8. **end**

DETAILED STEPS

	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	**l2vpn vfi context** *vfi-context-name* **Example:**	Establishes a Layer 2 VPN (L2VPN) virtual forwarding interface (VFI) for specifying core-facing pseudowires in

	Command or Action	Purpose
	`Device(config)# l2vpn vfi context vfi1`	a Virtual Private LAN Services (VPLS) and enters L2VFI configuration mode. • The VFI represents an emulated LAN or a VPLS forwarder from the VPLS architectural model when using an emulated LAN interface.
Step 4	**vpn id** *vpn-id* **Example:** `Device(config-vfi)# vpn id 10`	Configures a VPN ID for the VPLS domain.
Step 5	**autodiscovery bgp signaling bgp** **Example:** `Device(config-vfi)# autodiscovery bgp signaling bgp`	Enables BGP auto-discovery and BGP signaling on the device.
Step 6	**ve id** *ve-ID-number* **Example:** `Device(config-vfi)# ve id 1`	Configures a VPLS Endpoint ID (VEID) for the NLRI exchanged between BGP devices for BGP auto-discovery with BGP signaling. • For example, VEID numbering sequences such as 1,2,3 or 501, 502, 503 are preferred because the VEIDs are contiguous. • Avoid a non-contiguous numbering scheme such as 100, 200, 300. Repeat this step to add more VEIDs. The VEID must be unique within the same VPLS domain for all PE devices. **Note** If you change the VEID, then the virtual circuit (VC) reprovisions and traffic is impacted as a result.
Step 7	**ve range** *ve-range-number* **Example:** `Device(config-vfi)# ve range 10`	Overrides the minimum size of VPLS edge (VE) blocks. • The VE range value should be approximately the same as the number of neighbors (up to 100). • The VE range can be configured based on the number of neighboring PE devices in the network. • For example, if 50 PE devices are in a VPLS domain, then a VE range of 50 is better than 10 because the number of NLRIs exchanged are less and the convergence time is reduced. **Note** If no VE range is configured or an existing VE range value is removed, then the default VE range of 10 is applied. The default VE range should not be used if the device has many PE neighbors. **Note** If you change the VE range, then the VC reprovisions and traffic is impacted as a result.

	Command or Action	Purpose
Step 8	**end** **Example:** `Device(config-vfi)# end`	Exits L2 VFI configuration mode and returns to privileged EXEC mode. **Note** Commands take effect after the device exits L2VFI configuration mode.

Configuring BGP Signaling for VPLS Autodiscovery

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router bgp** *autonomous-system-number*
4. **bgp graceful-restart**
5. **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number*
6. **address-family l2vpn vpls**
7. **neighbor** {*ip-address* | *peer-group-name*} **activate**
8. **neighbor** {*ip-address* | *peer-group-name*} **send-community extended**
9. **neighbor** {*ip-address* | *peer-group-name*} **suppress-signaling-protocol ldp**
10. **exit-address-family**
11. Repeat steps 1 to 10 to configure and activate other BGP neighbors in an L2VPN address family.
12. **end**
13. **show l2vpn vfi**
14. **show ip bgp l2vpn vpls** {**all** [**summary**] | **rd** *route-distinguisher*}

DETAILED STEPS

	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** *autonomous-system-number* **Example:** `Device(config)# router bgp 100`	Enters router configuration mode for the specified routing process.
Step 4	**bgp graceful-restart** **Example:** `Device(config-router)# bgp graceful-restart`	Enables the Border Gateway Protocol (BGP) graceful restart capability globally for all BGP neighbors.

	Command or Action	Purpose
Step 5	**neighbor** {*ip-address* | *peer-group-name*} **remote-as** *autonomous-system-number* **Example:** `Device(config-router)# neighbor 198.51.100.1 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 6	**address-family l2vpn vpls** **Example:** `Device(config-router)# address-family l2vpn vpls`	Specifies the L2VPN address family and enters address family configuration mode. • The **vpls** keyword specifies that the VPLS endpoint provisioning information is to be distributed to BGP peers and a L2VPN VPLS address family session is created.
Step 7	**neighbor** {*ip-address* | *peer-group-name*} **activate** **Example:** `Device(config-router-af)# neighbor 198.51.100.1 activate`	Enables the exchange of information with a BGP neighbor.
Step 8	**neighbor** {*ip-address* | *peer-group-name*} **send-community extended** **Example:** `Device(config-router-af)# neighbor 198.51.100.1 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 9	**neighbor** {*ip-address* | *peer-group-name*} **suppress-signaling-protocol ldp** **Example:** `Device(config-router-af)# neighbor 198.51.100.1 suppress-signaling protocol ldp`	Suppresses LDP signaling for a BGP neighbor so that BGP signaling for VPLS auto-discovery is used instead. • In this example, LDP signaling is suppressed for the neighbor at 10.10.10.1.
Step 10	**exit-address-family** **Example:** `Device(config-router-af)# exit-address-family`	Exits address family configuration mode and returns to router configuration mode.
Step 11	Repeat steps 1 to 10 to configure and activate other BGP neighbors in an L2VPN address family.	

	Command or Action	Purpose
Step 12	**end** **Example:** `Device(config-router)# end`	Exits router configuration mode and returns to privileged EXEC mode.

Step 13	**show l2vpn vfi**
	Example:
	`Device# show l2vpn vfi`
	
	`PE1-standby#sh l2vpn vfi`
	`Load for five secs: 0%/0%; one minute: 0%; five minutes: 0%`
	`Time source is hardware calendar, *20:50:52.526 GMT Wed Aug 29 2012`
	
	`Legend: RT=Route-target, S=Split-horizon, Y=Yes, N=No`
	
	`VFI name: VFI1, state: up, type: multipoint, signaling: BGP`
	`VPN ID: 1, VE-ID: 10, VE-SIZE: 10`
	`RD: 1:1, RT: 1:1`
	`Bridge-Domain 100 attachment circuits:`
	`Pseudo-port interface: pseudowire100001`
	`Interface Peer Address VE-ID Local Label Remote Label S`
	`pseudowire100003 198.51.100.2 11 1003 2002 Y`
	`pseudowire100005 198.51.100.3 12 1004 2002 Y`
	
	`VFI name: VFI2, state: up, type: multipoint, signaling: BGP`
	`VPN ID: 2, VE-ID: 20, VE-SIZE: 12`
	`RD: 1:2, RT: 1:2, import 3:3, export 4:4`
	`Bridge-Domain 200 attachment circuits:`
	`Pseudo-port interface: pseudowire100002`
	`Interface Peer Address VE-ID Local Label Remote Label S`
	`pseudowire100004 198.51.100.2 21 1021 2020 Y`
	`pseudowire100006 198.51.100.3 22 1022 2020 Y`
		Displays information about the configured VFI instances.

Step 14	**show ip bgp l2vpn vpls** {**all** [**summary**] | **rd** *route-distinguisher*}
	Example:
	`Device# show ip bgp l2vpn vpls all summary`
	
	`BGP router identifier 198.51.100.1, local AS number 65000`
	`BGP table version is 14743, main routing table version 14743`
	`6552 network entries using 1677312 bytes of memory`
	`6552 path entries using 838656 bytes of memory`
	`3276/3276 BGP path/bestpath attribute entries using 760032 bytes of memory`
	`1638 BGP extended community entries using 65520`
		Displays information about the L2VPN VPLS address family.

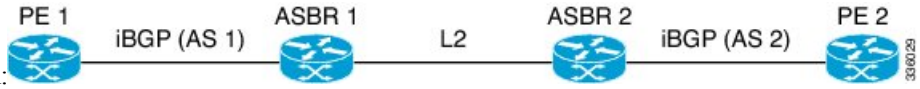
	Command or Action	Purpose
	bytes of memory 0 BGP route-map cache entries using 0 bytes of memory 0 BGP filter-list cache entries using 0 bytes of memory BGP using 3341520 total bytes of memory BGP activity 9828/3276 prefixes, 9828/3276 paths, scan interval 60 secs Neighbor V AS MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/PfxRcd 198.51.101.1 4 65000 90518 90507 14743 0 0 8w0d 1638 198.51.102.2 4 65000 4901 4895 14743 0 0 2d01h 1638 198.51.103.3 4 65000 4903 4895 14743 0 0 2d01h 1638	

VPLS BGP Signaling L2VPN Inter-AS Option A: Example

The following example configuration describes Inter-AS Option A for VPLS BGP signaling in an L2VPN. The Autonomous System Boundary Router (ASBR) 1 acts as the Provider Edge (PE) for all VPLS instances that span over Autonomous System (AS) 1 and ASBR 2 are viewed as the CE device. And for the other way around, for AS 2, ASBR 2 acts as the PE and ASBR 1 is viewed as the CE. MPLS is not required between ASBR 1 and ASBR 2 because VPLS is used for layer 2 linking. Each VPLS instance needs to be segregated so that it can be sent in the proper VPLS domain in ASBRs (for example, a switchport interface or Ethernet sub-interface).

Note From a BGP signaling perspective, there is no specific change within the AS. From the VPLS perspective, there is no BGP peering between ASBR1 and ASBR2.

The following figure shows a network diagram for the BGP signaling Inter-AS option A BGP configuration:



The following example shows the PE 1 BGP configuration for Inter-AS Option A:

```
router bgp 100
  neighbor 10.0.0.2 remote-as 100
   address-family l2vpn vpls
    neighbor 10.0.0.2 activate
    neighbor 10.0.0.2 send-community extended
    neighbor 10.0.0.2 suppress-signaling-protocol ldp
   exit-address-family
```

The following example shows the ASBR 1 BGP configuration for Inter-AS Option A:

```
router bgp 100
  neighbor 10.0.0.1 remote-as 100
   address-family l2vpn vpls
    neighbor 10.0.0.1 activate
    neighbor 10.0.0.1 send-community extended
```

```
    neighbor 10.0.0.1 suppress-signaling-protocol ldp
   exit-address-family
```

The following example shows the ASBR 2 BGP configuration for Inter-AS Option A:

```
router bgp 200
  neighbor 10.0.1.1 remote-as 100
   address-family l2vpn vpls
    neighbor 10.0.1.1 activate
    neighbor 10.0.1.1 send-community extended
    neighbor 10.0.1.1 suppress-signaling-protocol ldp
   exit-address-family
```

The following example shows the PE 2 BGP configuration for Inter-AS Option A:

```
router bgp 200
  neighbor 10.0.1.2 remote-as 100
   address-family l2vpn vpls
    neighbor 10.0.1.2 activate
    neighbor 10.0.1.2 send-community extended
    neighbor 10.0.1.2 suppress-signaling-protocol ldp
   exit-address-family
```

Additional References for VPLS Autodiscovery BGP Based

Related Documents

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

Standards and RFCs

Standard/RFC	Title
draft-ietf-l2vpn-signaling-08.txt	*Provisioning, Autodiscovery, and Signaling in L2VPNs*
draft-ietf-l2vpn-vpls-bgp-08.8	*Virtual Private LAN Service (VPLS) Using BGP for Autodiscovery and Signaling*
draft-ietf-mpls-lsp-ping-03.txt	*Detecting MPLS Data Plane Failures*
draft-ietf-pwe3-vccv-01.txt	*Pseudo-Wire (PW) Virtual Circuit Connection Verification (VCCV)*
RFC 3916	*Requirements for Pseudo-wire Emulation Edge-to-Edge (PWE3)*
RFC 3981	*Pseudo Wire Emulation Edge-to-Edge Architecture*
RFC 6074	Provisioning, Auto-Discovery, and Signaling in Layer 2 Virtual Private Networks (L2VPNs)
RFC 4761	Virtual Private LAN Service (VPLS) Using BGP for Auto-Discovery and Signaling

MIBs

MIB	MIBs Link
• CISCO-IETF-PW-ATM-MIB (PW-ATM-MIB) • CISCO-IETF-PW-ENET-MIB (PW-ENET-MIB) • CISCO-IETF-PW-FR-MIB (PW-FR-MIB) • CISCO-IETF-PW-MIB (PW-MIB) • CISCO-IETF-PW-MPLS-MIB (PW-MPLS-MIB)	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

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

Feature Information for VPLS BGP Signaling L2VPN Inter-AS Option A

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 VPLS BGP Signaling L2VPN

Feature Name	Releases	Feature Information
VPLS BGP Signaling L2VPN	Cisco IOS XE Release 3.8S	This feature simplifies the auto-discovery and signaling of all known provider edge (PE) devices in a VPLS instance by using BGP for both functions. The following commands were introduced or modified: **autodiscovery bgp signaling bgp**, **debug bgp l2vpn vpls updates**, **neighbor suppress-signaling-protocol ldp**, **ve id**, **ve range**, **show bgp l2vpn vpls**.