H-VPLS N-PE Redundancy for MPLS Access

The H-VPLS N-PE Redundancy for MPLS Access feature enables two network provider edge (N-PE) devices to provide failover services to a user provider edge (U-PE) device in a hierarchical virtual private LAN service (H-VPLS). Having redundant N-PE devices provides improved stability and reliability against link and node failures.

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 https://cfnng.cisco.com/. An account on Cisco.com is not required.

Prerequisites for H-VPLS N-PE Redundancy for MPLS Access

- Before configuring this feature, configure your hierarchical virtual private LAN service (H-VPLS) network and make sure it is operating correctly.
- To provide faster convergence, you can enable the MPLS Traffic Engineering—Fast Reroute feature in the Multiprotocol Label Switching (MPLS) core.
- Enable the L2VPN Pseudowire Redundancy feature on the user provider edge (U-PE) devices for MPLS access.

Restrictions for H-VPLS N-PE Redundancy for MPLS Access

- This feature cannot be used with the VPLS Autodiscovery feature on pseudowires that attach to user provider edge (U-PE) devices. When you create the virtual private LAN service (VPLS), you can manually create the virtual forwarding interface (VFI).
- You cannot configure more than one pseudowire to carry the bridge protocol data unit (BPDU) information between the network provider edge (N-PE) devices.
- You cannot configure a local loopback address as a neighbor when you configure the H-VPLS N-PE Redundancy feature on N-PE devices.
- Only two N-PE devices can be connected to each U-PE device.

Information About H-VPLS N-PE Redundancy for MPLS Access

How H-VPLS N-PE Redundancy for MPLS Access

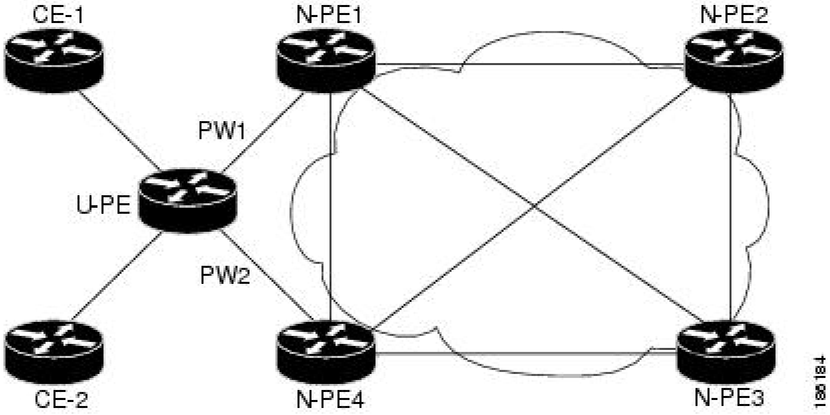
In a network configured with the H-VPLS N-PE Redundancy feature, the user provider edge (U-PE) device is connected to two network provider edge (N-PE) devices. This feature provides a level of redundancy that can tolerate both link and device faults. If a failure occurs in the network that disables one N-PE device from transmitting data, the other N-PE device takes over.

H-VPLS N-PE Redundancy with MPLS Access Based on Pseudowire Redundancy

For the H-VPLS Redundancy with MPLS Access feature based on pseudowire redundancy, the Multiprotocol Label Switching (MPLS) network has pseudowires to the virtual private LAN service (VPLS) core network provider edge (N-PE) devices.

As shown in the figure below, one pseudowire transports data between the user provider edge (U-PE) device and its peer N-PE devices. When a failure occurs along the path of the U-PE device, the backup pseudowire and the redundant N-PE device become active and start transporting data.

Figure 1: H-VPLS N-PE Redundancy for MPLS Access Based on Pseudowire Redundancy



How to Configure H-VPLS N-PE Redundancy for MPLS Access

Specifying the Devices in the Layer 2 VPN VFI

Repeat this task on each N-PE device that is part of the pseudowire redundancy.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **l2vpn vfi context** *name*
4. **vpn id** *vpn id*
5. **member** *ip-address* **encapsulation mpls**
6. **exit**
7. **bridge-domain** *bridge-id*
8. **member vfi** *vfi-name*
9. **member** *ip-address* [*vc-id*] **encapsulation mpls**
10. **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.

	Command or Action	Purpose
Step 3	**l2vpn vfi context** *name* **Example:** `Device(config)# l2vpn vfi context VPLS-10`	Establishes a L2VPN VFI between two or more separate networks, and enters L2VFI configuration mode.
Step 4	**vpn id** *vpn id* **Example:** `Device(config-vfi)# vpn id 10`	Sets a VPN ID on the Virtual Private LAN Services (VPLS) instance. • Use the same VPN ID for the PE devices that belong to the same VPN. • Make sure the VPN ID is unique for each VPN in the service provider network. The range is from 1 to 4294967295.
Step 5	**member** *ip-address* **encapsulation mpls** **Example:** `Device(config-vfi)# member 102.102.102.102 encapsulation mpls`	Specifies the device that forms a point-to-point L2VPN VFI connection. • *ip-address*—IP address of the VFI neighbor (the N-PE device). • **encapsulation mpls**—Specifies Multiprotocol Label Switching (MPLS) as the data encapsulation method.
Step 6	**exit** **Example:** `Device(config-vfi)# exit`	Returns to global configuration mode.
Step 7	**bridge-domain** *bridge-id* **Example:** `Device(config)# bridge-domain 10`	Configures components on a bridge domain, and enters bridge-domain configuration mode.
Step 8	**member vfi** *vfi-name* **Example:** `Device(config-bdomain)# member vfi VPLS-10`	Configures the VFI member in the bridge-domain.
Step 9	**member** *ip-address* [*vc-id*] **encapsulation mpls** **Example:** `Device(config-vfi)# member 105.105.105.105 10 encapsulation mpls`	Specifies the device that forms a point-to-point Layer 2 VPN (L2VPN) VFI connection. • *ip-address*—IP address of the VFI neighbor (U-PE device). • *vc-id*—Virtual circuit identifier. • **encapsulation mpls**—Specifies MPLS as the data encapsulation method.

Step 10	**end**
	Example:
	`Device(config-bdomain)# end`
		Returns to privileged EXEC mode.

Specifying the N-PE Devices That Form the Layer 2 VPN Cross Connection With the U-PE

Perform this task on the U-PE device.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **service instance** *id* **ethernet**
5. **encapsulation dot1q** *vlan-id*
6. **exit**
7. **exit**
8. **l2vpn xconnect context** *context-name*
9. **member gigabitethernet** *interface-number* [**service-instance** *id*]
10. **member** *ip-address vc-id* **encapsulation mpls** [**group** *group-name* [**priority** *number*]]
11. **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	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet0/1/0`	Specifies the interface to configure, and enters interface configuration mode.
Step 4	**service instance** *id* **ethernet** **Example:** `Device(config-if)# service instance 10 ethernet`	Configures an Ethernet service instance on theinterface, and enters Ethernet service configuration mode.
Step 5	**encapsulation dot1q** *vlan-id* **Example:** `Device(config-if-srv)# encapsulation dot1q 10`	Defines the matching criteria to map 802.1Q frames ingress on the interface to the appropriate service instance.
Step 6	**exit** **Example:** `Device(config-if-srv)# exit`	Returns to interface configuration mode.

	Command or Action	Purpose
Step 7	**exit** **Example:** `Device(config-if)# exit`	Returns to global configuration mode.
Step 8	**l2vpn xconnect context** *context-name* **Example:** `Device(config)# l2vpn xconnect context XC-10`	Creates a Layer 2 VPN (L2VPN) cross-connect context, and enters xconnect configuration mode.
Step 9	**member gigabitethernet** *interface-number* [**service-instance** *id*] **Example:** `Device(config-xconnect)# member GigabitEthernet0/1/0 service-instance 10`	Specifies devices that form a Layer 2 VPN (L2VPN) cross connect. • **service-instance** *id*—(Optional) Specifies the service instance identifier.

Step 10	**member** *ip-address vc-id* **encapsulation mpls** [**group** *group-name* [**priority** *number*]]
	Example:
	`Device(config-xconnect)# member 101.101.101.101 10 encapsulation mpls group pwred priority 9`
	`Device(config-xconnect)# member 102.102.102.102 10 encapsulation mpls group pwred priority 10`
		Specifies devices that form a Layer 2 VPN (L2VPN) cross connect.
		• *ip-address*—IP address of the peer N-PE device.
		• *vc-id*—Virtual circuit identifier.
		• **encapsulation mpls**—Specifies Multiprotocol Label Switching (MPLS) as the data encapsulation method.
		• **group** *group-name*—Specifies the cross-connect member redundancy group name.
		• **priority** *number*—Specifies the cross-connect member priority. The range is from 0 to 16. The highest priority is 0. Lowest priority is 16.

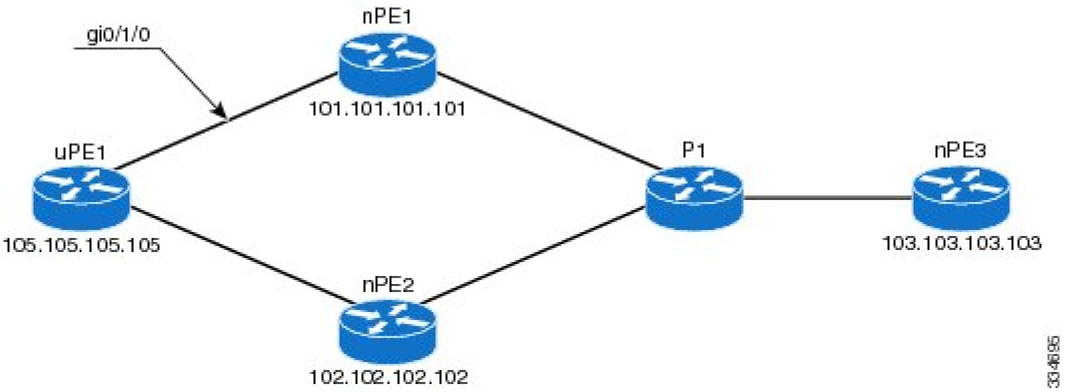
Step 11	**end**
	Example:
	`Device(config-xconnect)# end`
		Returns to privileged EXEC mode.

Configuration Examples for H-VPLS N-PE Redundancy for MPLS Access

Example: H-VPLS N-PE Redundancy for MPLS Access

The figure below shows a configuration that is set up for the H-VPLS N-PE Redundancy with MPLS Access feature. Since there is no option to configure multihoming on access VPLS, the **xconnect** command is used with priority on uPE1. Please let me know if you need any other info.

Figure 2: H-VPLS N-PE Redundancy with MPLS Access Topology



nPE1 Configuration

```
l2vpn vfi context VPLS-10
 vpn id 10
 member 102.102.102.102 encapsulation mpls
 member 103.103.103.103 encapsulation mpls
!
bridge-domain 10
 member vfi VPLS-10
 member 105.105.105.105 10 encapsulation mpls
```

nPE2 Configuration

```
l2vpn vfi context VPLS-10
 vpn id 10
 member 101.101.101.101 encapsulation mpls
 member 103.103.103.103 encapsulation mpls
!
bridge-domain 10
 member vfi VPLS-10
 member 105.105.105.105 10 encapsulation mpls
```

nPE3 Configuration

```
l2vpn vfi context VPLS-10
 vpn id 10
 member 101.101.101.101 encapsulation mpls
 member 102.102.102.102 encapsulation mpls
!
bridge-domain 10
 member vfi VPLS-10
```

uPE1 Configuration

```
interface GigabitEthernet0/1/0
 service instance 10 ethernet
 encapsulation dot1q 10
!
l2vpn xconnect context XC-10
 member GigabitEthernet0/1/0 service-instance 10
 member 101.101.101.101 10 encapsulation mpls group pwred priority 9
 member 102.102.102.102 10 encapsulation mpls group pwred priority 10
```

Sample Output on uPE1

```
Device# show xconnect peer 101.101.101.101 vcid 10

Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down            AD=Admin Down      IA=Inactive
  SB=Standby  HS=Hot Standby     RV=Recovering      NH=No Hardware

XC ST  Segment 1                         S1 Segment 2                         S2
------+---------------------------------+--+---------------------------------+--
UP pri   ac Gi0/1/0:10(Eth VLAN)         UP mpls 101.101.101.101:10           UP

Device# show xconnect peer 102.102.102.102 vcid 10

Legend:    XC ST=Xconnect State  S1=Segment1 State  S2=Segment2 State
  UP=Up       DN=Down            AD=Admin Down      IA=Inactive
  SB=Standby  HS=Hot Standby     RV=Recovering      NH=No Hardware

XC ST  Segment 1                         S1 Segment 2                         S2
------+---------------------------------+--+---------------------------------+--
IA pri   ac Gi0/1/0:10(Eth VLAN)         UP mpls 102.102.102.102:10           SB
Device#
```

Additional References for L2VPN VPLS Inter-AS Option B

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Command List, All Releases
MPLS commands	Cisco IOS Multiprotocol Label Switching Command Reference
IP Routing (BGP) commands	Cisco IOS IP Routing: BGP Command Reference
Concepts and tasks related to configuring the VPLS Autodiscovery: BGP Based feature.	*VPLS Autodiscovery BGP Based*
BGP support for the L2VPN address family	*BGP Support for the L2VPN Address Family*
VPLS	"VPLS Overview" section in the *Configuring Multiprotocol Label Switching on the Optical Services Modules* document
L2VPN multisegment pseudowires, MPLS OAM support for L2VPN multisegment pseudowires, MPLS OAM support for L2VPN inter-AS option B	*L2VPN Multisegment Pseudowires*

Standards

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

MIBs

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

RFCs

RFC	Title
RFC 4360	*BGP Extended Communities Attribute*
RFC 4364	*BGP/MPLS IP Virtual Private Networks (VPNs)*

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 H-VPLS N-PE Redundancy for MPLS Access

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 H-VPLS N-PE Redundancy for MPLS Access

Feature Name	Releases	Feature Information
H-VPLS N-PE Redundancy for MPLS Access	Cisco IOS XE Release 3.6S	The H-VPLS N-PE Redundancy for MPLS Access feature enables two network provider edge (N-PE) devices to provide redundancy to a user provider edge (U-PE) device in a hierarchical virtual private LAN service (H-VPLS). Having redundant N-PE devices provides improved stability and reliability against link and node failures. In Cisco IOS XE Release 3.6S, support was added for the Cisco ASR 903 Router. The following commands were introduced or modified: **forward permit l2protocol**, **show mpls l2transport vc**.

Glossary

CE device—customer edge device. A device that belongs to a customer network, which connects to a PE device to utilize MPLS VPN network services.

LAN—local-area network. High-speed, low-error data network covering a relatively small geographic area. LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited areas.

MPLS—Multiprotocol Label Switching. A packet-forwarding technology, used in the network core, that applies data link layer labels to tell switching nodes how to forward data, resulting in faster and more scalable forwarding than network layer routing normally can do.

MSTP—Multiple Spanning Tree Protocol. MSTP enables multiple VLANs to be mapped to the same spanning-tree instance, reducing the number of spanning-tree instances needed to support a large number of VLANs.

N-PE—network provider edge device. This device acts as a gateway between the MPLS core and edge domains.

PE device—provider edge device. The PE device is the entry point into the service provider network. The PE device is typically deployed on the edge of the network and is administered by the service provider.

pseudowire—A pseudowire is a virtual connection that, in the context of VPLS, connects two SVIs. It is a mechanism that carries the elements of an emulated service from one PE device to one or more PE devices over a packet switched network (PSN). A pseudowire is bidirectional and consists of a pair of unidirectional MPLS virtual circuits (VCs). A pseudowire can be used to connect a point-to-point circuit.

QinQ—An IEEE 802.1Q VLAN tunnel. A mechanism for constructing multipoint Layer 2 VPN using Ethernet switches.

redundancy—The duplication of devices, services, or connections so that, in the event of a failure, they can perform the work of those that failed.

router—A network layer device that uses one or more metrics to determine the optimal path along which network traffic should be forwarded. Routers forward packets from one network to another based on network layer information.

spanning tree—Loop-free subset of a network topology.

U-PE—user provider edge device. This device connects CE devices to the service.

VFI—virtual forwarding instance. A VFI is a collection of data structures used by the data plane, software-based or hardware-based, to forward packets to one or more VCs.

VLAN—Virtual LAN. Group of devices on one or more LANs that are configured (using management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments.

VPLS—Virtual Private LAN Service. VPLS describes an architecture that delivers Layer 2 service that emulates an Ethernet LAN across a wide-area network (WAN) and inherits the scaling characteristics of a LAN.

VPLS redundancy—Also called N-PE redundancy. Allows U-PEs to be dual-honed (to their N-PEs) in a loop-free topology with MPLS or QinQ as the access or aggregation domain.

VPN—Virtual Private Network. Allows IP traffic to travel securely over public TCP/IP networks and the Internet by encapsulating and encrypting all IP packets. VPN uses a tunnel to encrypt all information at the IP level.