CHAPTER 4

Provider Edge-Customer Edge Design Options

The domain creating the MPLS L2VPN service consisting of provider and provider edge routers remains the same regardless of access technologies. The technologies and designs used to connect the provider edge-to-customer edge device vary considerably based on technology preference, installed base, and operational expertise.

Common characteristics exist for each of the options. Each design needs to consider the following:

- Topology implemented, either hub-and-spoke or rings;
- How redundancy is configured; and,
- QoS implementation.

Network availability is critical for enterprises in order to prevent revenue loss. To improve network reliability, branch routers, campus routers, and Data Centers are multi-housed on provider edge devices using one of the various access topologies to achieve provider edge node redundancy. Each topology needs reliability and resilience to provide seamless connectivity. This chapter describes how to achieve seamless connectivity.

Inter-Chassis Communication Protocol

The provider edge nodes connecting to the dual-homed customer edge work in active or standby mode. The active provider edge forwards traffic while the standby provider edge monitors the active provider edge status. The standby provider edge takes over forwarding if the active provider edge fails. The nodes require a mechanism to communicate local connectivity failure to the customer edge; and, a mechanism to detect peer-node failure in order to move traffic to the standby provider edge. Inter-Chassis Communication Protocol (ICCP) provides the control channel to communicate this information.

ICCP allows active and standby provider edges, connecting to dual-homed CPE, to exchange information regarding local link failure to CPE and detect peer node failure or it's Core Isolation. This critical information helps to move forwarding from active to standby provider edge within milliseconds. The provider edges can be co-located or geo-redundant. ICCP communication occurs between provider edges either using dedicated link between provider edges or using the core network. ICCP configuration includes configuring redundancy group (RG) on both of the premise equipment devices with each other's address for ICCP communication. Using this information, provider edges set up ICCP control connection and different applications like Multi-Chassis Link Aggregation Group (MC-LAG) and Network Virtualization (nV) described in the next sections use this control connection to share state information.

Table 4-1 shows how to configure ICCP.

Table 4-1 ICCP Configuration

ICCP Configuration	Description
`redundancy`	Adds an ICCP redundancy group with mentioned group-id.
`iccp`	
`group group-id`	
`member`	This is the ICCP peer for this redundancy group. Only one neighbor can be configured per redundancy group. The IP address is the LDP router-ID of the neighbor. This configuration is required for ICCP to function.
`neighbor neighbor-ip-address`	
`!`	
`backbone`	Configures ICCP backbone interfaces to detect isolation from the network core, and triggers switchover to the peer provider edge if the provider edge on which the failure is occurring is active. Multiple backbone interfaces can be configured for each redundancy group. When all backbone interfaces are not UP, this is an indication of core isolation.
`backbone interface interface-type-id`	
`!`	

The next section discusses various access topologies that can be implemented between branch, campus, or Data Center devices in an Enterprise L2VPN network. Each topology ensures redundancy and fast failure detection and convergence mechanisms to provide seamless last mile connectivity.

Ethernet Access

The following sections describe how Ethernet access is implemented in hub-and-spoke or ring access.

Hub and Spoke Using MC-LAG Active/Active

In hub-and-spoke access topology, the customer edge device is dual homed to provider edge devices in the MPLS VPN network. The MC-LAG feature provides an end-to-end inter-chassis redundancy solution for Enterprise. MC-LAG involves provider edge devices collaborating through ICCP connection to act as a single Link Aggregation Group (LAG) from the perspective of customer edge device, thus providing device-level and link-level redundancy. To achieve this, provider edge devices use the ICCP connection to coordinate with each other to present a single LACP bundle (spanning the two devices) to the customer edge device. In addition, service multi-homing enables both provider edge nodes to load share traffic based on VLAN ranges. The provider edge nodes negotiate their active or standby role for a specific VLAN using the ICCP-SM protocol. Negotiation is based on locally-defined priority.

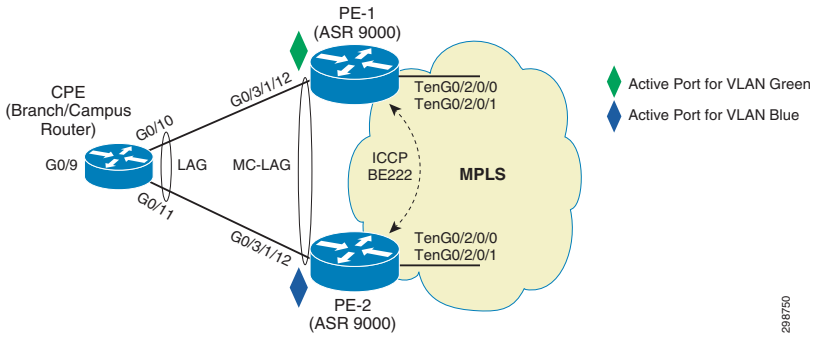
While the two ASR 9000 provider edge nodes share a common Bundle interface, the access node uplinks are grouped together on a per-provider edge-node basis only, or they can be unbundled in the case only a single uplink per provider edge exists.

The provider edge nodes enable the L2VPN functionality, mapping the inter-chassis bundle sub-interface to the VFI/Edge Bridge associated to the core VPLS/PBB-EVPN service.

Once MAC learning has completed only the active provider edge node for a specific VLAN will receive traffic. L2VPN service is configured on this bundle interface or sub-interface on provider edge. provider edge devices coordinate through the ICCP connection to perform a switchover while presenting an unchanged bundle interface to the customer edge for the following failure events:

- Link failure—A port or link between the customer edge and one of the provider edges fails.
- Device failure-Meltdown or reload of one of the provider edges, with total loss of connectivity to the customer edge, the core and the other provider edge.
- Core isolation—A provider edge loses its connectivity to the core network and therefore is of no value, being unable to forward traffic to or from the customer edge.

Figure 4-1 Hub and Spoke access with MLACP



When a loss of connectivity between the provider edges, both devices may assume that the other has failed. This will cause both devices to attempt to take on the Active role resulting in a loop. The customer edge device can mitigate this situation by limiting number of links so that those links are connected to one, active provider edge at a time. Hub and Spoke access configuration is described in Table 4-2, Table 4-3, and Table 4-4.

Note PE-1 is configured active for VLAN 100 and PE-2 is configured active for VLAN 102.

Table 4-2 Customer Edge Configuration

Customer Edge Configuration	Description
`interface GigabitEthernet0/9`	Interface connected to local LAN.
`switchport trunk allowed vlan 100-101`	
`switchport mode trunk`	
`spanning-tree portfast trunk`	
`load-interval 30`	
`interface GigabitEthernet0/10`	Interface connected to PE1.
`port-type nni`	
`switchport mode trunk`	
`interface GigabitEthernet0/11`	Interface connected to PE2.
`port-type nni`	
`switchport mode trunk`	

Table 4-3 Provider Edge-1 Configuration

Provider Edge-1 Configuration	Description
interface GigabitEthernet0/3/1/12	Configures customer edge connecting interface in bundle1.
description Bundle-Ether1	
bundle id 1 mode on	
cdp	
load-interval 30	
transceiver permit pid all	
!	
interface bundle-ether1	Configures Bundle interface.
!	
interface bundle-ether1.100 l2transport	Configures bundle sub-interface with specific VLAN.
encapsulation dot1q 100	
!	
interface bundle-ether1.101 l2transport	Configures bundle sub-interface with specific VLAN.
encapsulation dot1q 101	
!	
redundancy	Adds an ICCP redundancy group 1
iccp	
group 1	
member	
neighbor 100.111.3.2	Configures ICCP members as PE-2
!	
backbone	Configures ICCP backbone interfaces.
interface Ten0/2/0/0	
interface Ten0/2/0/1	
!	
l2vpn	
bridge group L2VPN	
bridge-domain CE-EPLAN-100	Bridge domain configuration for C-VLAN 100
!	
interface bundle-ether1.100	Adds attachment circuit for VLAN 100 to BD
!	
vfi CE-EPLAN-100	Creates VFI instance with VPLS neighbors
neighbor 100.111.3.2 pw-id 100	
!	
neighbor 100.111.11.1 pw-id 100	
!	
neighbor 100.111.11.2 pw-id 100	
!	

Table 4-3 Provider Edge-1 Configuration (continued)

Provider Edge-1 Configuration	Description
!	
bridge-domain CE-EPLAN-101	Bridge domain configuration for C-VLAN 101
interface Bundle-Ether1.101	Adds attachment circuit for VLAN 101 to BD
!	
vfi CE-EPLAN-101	Creates virtual fragment interface (VFI) instance with VPLS neighbors
neighbor 100.111.3.2 pw-id 101	
!	
neighbor 100.111.11.1 pw-id 101	
!	
neighbor 100.111.11.2 pw-id 101	
!	
!	
!	
redundancy	Enables L2VPN redundancy mode and enters redundancy configuration sub-mode. Adds an ICCP redundancy group.
iccp group 1	
multi-homing node-id 1	Enter the pseudo MLACP node ID. Enables the ICCP based multi-homing service. The node-ID is used for ICCP signaling arbitration.
interface Bundle-Ether1	Specifies the bundle interface
primary vlan 100	Configures the list of VLANs under the bundle port, which default to active (forwarding) when there are no faults detected.
secondary vlan 101	Configures the list of VLANs under the bundle port, which default to standby (blocked) when there are no faults detected.
recovery delay 60	Recovery delay timer is started once the core isolation condition has cleared. When the timer expires, the can take over as the active provider edge.

Table 4-4 Provider Edge-2 Configuration

Provider Edge-2 Configuration	Description
interface GigabitEthernet0/3/1/12	Configures customer edge connecting interface in bundle1.
description Bundle-Ether1	
bundle id 1 mode on	
cdp	
load-interval 30	
transceiver permit pid all	
!	
interface Bundle-Ether1	Configures Bundle interface.
!	
interface Bundle-Ether1.100 l2transport	Configures bundle sub-interface with specific VLAN.
encapsulation dot1q 100	

Table 4-4 Provider Edge-2 Configuration (continued)

Provider Edge-2 Configuration	Description
!	
interface Bundle-Ether1.101 l2transport	Configured bundle sub-interface with specific VLAN.
encapsulation dot1q 101	
!	
redundancy	Adds an ICCP redundancy group 1.
iccp	
group 1	
member	
neighbor 100.111.3.1	Configures ICCP members as Provider Edge-1.
!	
backbone	Configures ICCP backbone interfaces.
interface TenGigE0/2/0/0	
interface TenGigE0/2/0/1	
!	
!	
!	
l2vpn	
bridge group L2VPN	
bridge-domain CE-EPLAN-100	Bridge domain configuration for C-VLAN 100.
!	
interface Bundle-Ether1.100	Adds attachment circuit for VLAN 100 to BD.
!	
vfi CE-EPLAN-100	Creates VFI instance with VPLS neighbors.
neighbor 100.111.3.1 pw-id 100	
!	
neighbor 100.111.11.1 pw-id 100	
!	
neighbor 100.111.11.2 pw-id 100	
!	
!	
!	
bridge-domain CE-EPLAN-101	Bridge domain configuration for C-VLAN 101.
!	
interface Bundle-Ether1.101	Adds attachment circuit for VLAN 101 to BD.
!	

Table 4-4 Provider Edge-2 Configuration (continued)

Provider Edge-2 Configuration	Description
vfi CE-EPLAN-101	Creates VFI instance with VPLS neighbors.
neighbor 100.111.3.1 pw-id 101	
!	
neighbor 100.111.11.1 pw-id 101	
!	
neighbor 100.111.11.2 pw-id 101	
!	
!	
!	
l2vpn	
redundancy	Enables L2VPN redundancy mode and enters redundancy configuration sub-mode. Adds an ICCP redundancy group.
iccp group 1	
multi-homing node-id 2	
interface Bundle-Ether1	Enter the pseudo MLACP node ID. Enables the ICCP based multi-homing service. The node-ID is used for ICCP signaling arbitration.
primary vlan 101	Specifies the bundle interface.
secondary vlan 100	Configures the list of VLANs under the bundle port, which default to active (forwarding) when there are no faults detected.
!	Configures the list of VLANs under the bundle port, which default to standby (blocked) when there are no faults detected.
	Recovery delay timer is started once the core isolation condition has cleared. When the timer expires, the can take over as the active provider edge.

Note The model above can be implemented by configuring interfaces Bundle-Ether1.100 and Bundle-Ether1.101 for point-to-point E-line or multipoint E-LAN/E-TREE service using VPLS or PBB-EVPN core.

MC-LAG provides inter-chassis redundancy based on Hub and Spoke provider edge model. For Ring based topologies G.8032 access method is deployed as described below.

G.8032 Ring Access

In this access topology, provider edges are connected to a G.8032 Ethernet ring formed by connecting Ethernet access nodes to each other in a ring form. The G.8032 Ethernet ring protection switching protocol elects a specific link to protect the entire ring from loops. Such a link, which is called the Ring Protection Link (RPL), is typically maintained in disabled state by the protocol to prevent loops. The device connecting to the RPL link is called the RPL owner responsible for blocking RPL link. Upon a node or a link failure in the ring, the RPL link is activated allowing forwarding to resume over the ring. G.8032 uses Ring Automatic Protection Switching (R-APS) messages to coordinate the activities of switching the RPL on and off using a specified VLAN for the APS channel.

The G.8032 protocol also allows superimposing multiple logical rings over the same physical topology by using different instances. Each instance contains an inclusion list of VLAN IDs and defines different RPL links. In this guide, we are using two G.8032 instances with odd-numbered and even-numbered VLANs. ASR9000's provider edges also participate in the ring and act as the RPL owner. One provider edge acts as RPL owner for RPL for even-numbered VLAN's instance and the other provider edge as RPL owner for RPL for odd-numbered VLAN's instance so one provider edge remains in blocking state for one instance and other provider edge for other instance. Hence, load balancing and redundancy are achieved by making use of two RPLs, each RPL serving one instance. Additionally, each instance will have one VLAN dedicated to carry the automatic protection switching (APS) traffic.

In the G.8032 configuration, provider edge devices, which are configured as RPL owner nodes for one of the two instances, are specified with the interface connected to the ring. Two instances are configured for odd and even VLANs. provider edges are configured as RPL owner for one of the instances each to achieve load balancing and redundancy. Both instances are configured with dot1q sub-interface for the respective APS channel communication.

Figure 4-2 Ethernet Access with G.8032 Ring

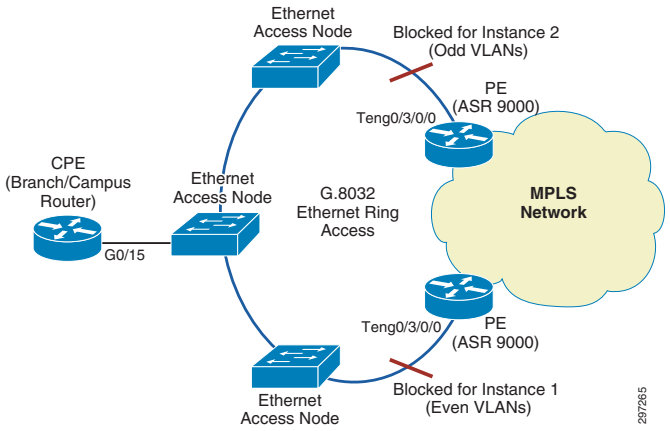


Table 4-5 details customer edge configuration.

Table 4-5 Customer Edge Configuration

Customer Edge Configuration	Description
`interface GigabitEthernet0/7`	Customer edge Interface.
`switchport trunk allowed vlan 118-119`	Allows VLAN 118 and 119 on the trunk port.
`switchport mode trunk`	Configures interface as trunk port.
`load-interval 30`	
`!`	

Table 4-6 details E-Access node customer edge-facing interface configuration (UNI).

Table 4-6 Ethernet Access Node Customer Edge-Facing Interface Configuration (UNI)

E-Access Node CE-Facing Interface Configuration (UNI)	Description
`interface GigabitEthernet0/1`	Customer edge connecting interface on Ethernet access node.
`switchport trunk allowed vlan none`	

Table 4-6 Ethernet Access Node Customer Edge-Facing Interface Configuration (UNI) (continued)

E-Access Node CE-Facing Interface Configuration (UNI)	Description
switchport mode trunk	
load-interval 30	
service instance 118 ethernet EVC-118	Configures EVC for VLAN 118.
encapsulation dot1q 118	
!	
service instance 119 ethernet EVC-119	Configures EVC for VLAN 119.
encapsulation dot1q 119	

Table 4-7 details Ethernet access node configuration.

Table 4-7 Ethernet Access Node Configuration

Ethernet Access Node Configuration	Description
ethernet ring g8032 profile ring_profile	Configures Ethernet Ring profile.
timer wtr 10	Configures G.8032 WTR timer.
timer guard 100	Configures Guard timer.
!	
ethernet ring g8032 ring_test	Configures G.8032 ring named ring_test.
open-ring	Configures ring as G.8032 ring as open ring.
exclusion-list vlan-ids 1000	Excludes VLAN 100.
port0 interface TenGigabitEthernet0/0/0	Mentions port0 as ten 0/0/0/0 for ring.
port1 interface TenGigabitEthernet0/1/0	Mentions port1 as ten 0/0/0/0 for ring.
instance 1	Configures Instance 1.
profile ring_profile	Configures instance with ring profile.
inclusion-list vlan-ids 99,106,108,118,301-302,310-311,1001-2000	Configures VLANs included in Instance 1.
aps-channel	Configures aps channel.
port0 service instance 99	Assigns service instance for APS messages on port0 and Port 1.
port1 service instance 99	
!	
!	
instance 2	Configures Instance 2.
profile ring_profile	Configures instance with ring profile.
rpl port1 next-neighbor	Configures Device interface as next neighbor to RPL link owner.
inclusion-list vlan-ids 107,109,119,199,351,2001-3000	Configures VLANs included in Instance 2.
aps-channel	Configures aps channel.
port0 service instance 199	Assigns service instance for APS messages on port0 and Port 1.
port1 service instance 199	

Table 4-7 Ethernet Access Node Configuration (continued)

Ethernet Access Node Configuration	Description
!	
!	
!	
interface TenGigabitEthernet0/0/0	Configures interface connected to ring.
!	
service instance 99 ethernet	Configures service instance used for APS messages on G.8032 ring for both instances.
encapsulation dot1q 99	
rewrite ingress tag pop 1 symmetric	
bridge-domain 99	
!	
service instance 199 ethernet	
encapsulation dot1q 199	
rewrite ingress tag pop 1 symmetric	
bridge-domain 199	
!	
interface TenGigabitEthernet0/1/0	Configures interface connected to ring.
service instance 99 ethernet	Configures service instance used for APS messages on G.8032 ring for both instances.
encapsulation dot1q 99	
rewrite ingress tag pop 1 symmetric	
bridge-domain 99	
!	
service instance 199 ethernet	
encapsulation dot1q 199	
rewrite ingress tag pop 1 symmetric	
bridge-domain 199	
!	
!	

Table 4-8 details provider edge configuration.

Table 4-8 Provider Edge Configuration

Provider edge Configuration	Description
interface TenGigE0/3/0/0.118 l2transport	L2 Customer Attachment Circuit.
encapsulation dot1q 118	Matching specific customer VLAN 118.
!	
interface TenGigE0/3/0/0.119 l2transport	L2 Customer Attachment Circuit.
encapsulation dot1q 119	Matching specific customer VLAN 119.
!	
ethernet ring g8032 profile ring_profile	Configures Ethernet Ring profile

Table 4-8 Provider Edge Configuration (continued)

Provider edge Configuration	Description
`timer wtr 10`	Configures G.8032 WTR timer.
`timer guard 100`	Configures Guard timer.
`timer hold-off 0`	Configures hold-off timer.
`!`	
`l2vpn`	Enters L2VPN Configuration mode
`bridge group L2VPN`	Configures bridge group named L2VPN.
`bridge-domain CE-L3VPN-118`	Configures bridge domain named customer edge-L3VPN-118.
`interface TenGigE0/3/0/0.118`	Enables sub-interface connected to ring towards customer edge under bridge domain CE-L3VPN-118.
`neighbor 100.111.3.2 pw-id 118`	Configures pseudo-wire to neighbor provider edge in the same bridge domain.
`bridge-domain CE-L3VPN-119`	Configures another bridge domain customer edge-L3VPN-119.
`interface TenGigE0/3/0/0.119`	Enables sub-interface connected to ring towards customer edge under same bridge domain customer edge-L3VPN-119
`neighbor 100.111.3.2 pw-id 119`	Configures pseudo-wire to neighbor provider edge in the same bridge domain customer edge-L3VPN-119.
`!`	
`ethernet ring g8032 ring_test`	Configures G.8032 ring named ring_test.
`port0 interface TenGigE0/3/0/0`	Configures port0 for g.8032 ring.
`!`	
`port1 none`	Mentions port 1 as none and G.8032 ring as open ring.
`open-ring`	
`Instance 1`	Enter instance 1 configuration.
`Inclusion-list vlan-ids 99,106,108,118,500,64,604,1001-2000`	Configures VLANs in the inclusion list of instance 1.
`aps-channel`	Enters APS channel configuration mode.
`port0 interface TenGigE0/3/0/0.99`	Configures sub-interface used for APS channel communication.
`port1 none`	
`!`	
`!`	
`instance 2`	Enter instance 2 configuration.
`profile ring_profile`	Configures instance with ring profile.
`rpl port0 owner`	Configures provider edge as RPL owner on port0 for instance 2.
`inclusion-list vlan-ids 199,107,109,109,119,501,2001-3000`	Configures VLANs in the inclusion list of instance 1.
`aps-channel`	Enters aps channel configuration mode
`port0 interface TenGigE0/3/0/0.199`	Configures sub-interface used for APS channel communication.
`port1 none`	

Note The model above can be implemented by configuring interfaces TenGigE0/3/0/0.118 and TenGigE0/3/0/0.199 for point-to-point E-line or multipoint E-LAN/E-TREE service using VPLS or PBB-EVPN core.

nV Access

The nV Satellite enables a system-wide solution in which one or more remotely-located devices or "satellites" complement a pair of host provider edge devices to collectively realize a single virtual switching entity in which the satellites act under the management and control of the host provider edge devices. Satellites and Hosts provider edges communicate using a Cisco proprietary protocol that offers discovery and remote management functions, thus turning the satellites from standalone devices into distributed logical line cards of the host.

The technology allows enterprises to virtualize access devices to which branch or campus the routers terminate, converting them into nV Satellite devices, and to manage them through provider edge nodes that operate as nV hosts. By doing so, the access devices transform from standalone devices with separate management and control planes into low profile devices that simply move user traffic from a port connecting branch or campus router towards a virtual counterpart at the host, where all network control plane protocols and advanced features are applied. The satellite only provides simple functions such as local connectivity and limited (and optional) local intelligence that includes ingress QoS, EOAM, performance measurements, and timing synchronization.

The satellites and the hosts exchange data and control traffic over point-to-point virtual connections known as Fabric Links. Branch or Campus Ethernet traffic carried over the fabric links is specially encapsulated using 802.1ah. A per-Satellite-Access-Port derived ISID value is used to map a given satellite node physical port to its virtual counterpart at the host for traffic flowing in the upstream and downstream direction. Satellite access ports are mapped as local ports at the host using the following naming convention:

```
<port type><Satellite-ID>/<satellite-slot>/<satellite-bay>/<satellite-port>
```

Where:

- **<port type>**—is GigabitEthernet for all existing Satellite models.
- **<Satellite-ID>**—is the satellite number as defined at the Host.
- **<satellite-slot>/<satellite-bay>/ <satellite-port>**—is the access port information as known at the Satellite node.

These satellite virtual interfaces on the Host provider edges are configured with L2VPN service.

The satellite architecture encompasses multiple connectivity models between the host and the satellite nodes. The guide discusses release support for:

- nV Satellite Simple Rings
- nV Satellite L2 Fabric

In all nV access topologies, host nodes load share traffic on a per-satellite basis. The active/standby role of a host node for a specific satellite is determined by a locally-defined priority and negotiated between the hosts via ICCP.

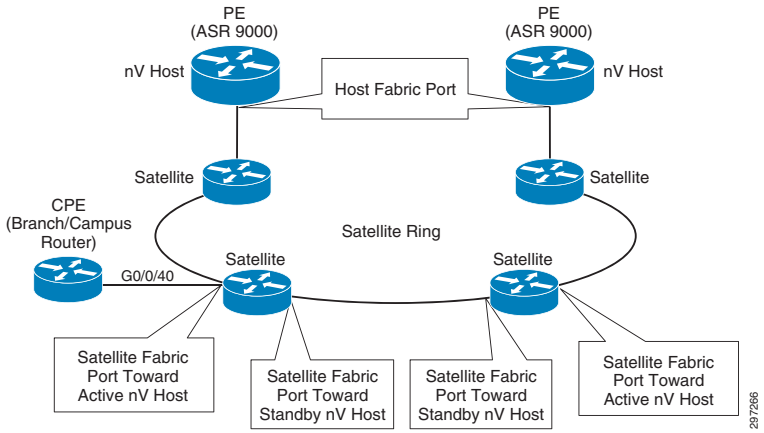
ASR 9000v and ASR 901 are implemented as a Satellite Devices:

- ASR 9000v has four 10 GbE ports that can be used as ICL.
- ASR901 has two GbE ports that can be used as ICL and that can be used as ICL and ASR 903 can have up to two 10 GbE ports can be used as ICL.

nV Satellite Simple Rings

In this topology, satellite access nodes connecting branch or campus are connected in an open ring topology terminating at the provider edge host devices as shown in Figure 4-3.

Figure 4-3 nV with L1 Fabric access



The provider edge device advertises multicast discovery messages periodically over a dedicated VLAN over fabric links. Each satellite access device in the ring listens for discovery messages on all its ports and dynamically detects the Fabric link port toward the host.

The satellite uses this auto-discovered port for the establishment of a management session and for the exchange of all the upstream and the downstream traffic with each of the hosts (data and control). At the host, incoming and outgoing traffic is associated to the corresponding satellite node using the satellite mac address, which was also dynamically learned during the discovery process. Discovery messages are propagated from one satellite node to another and from either side of the ring so that all nodes can establish a management session with both hosts. The is described below.

Table 4-9 details nV L1 fabric access configuration.

Table 4-9 nV L1 Fabric Configuration

nV L1 Fabric Configuration	Description
`interface TenGigE0/2/0/3`	Interface acting as Fabric link connecting to nV ring.
`ipv4 point-to-point`	
`ipv4 unnumbered Loopback10`	
`nv`	Enters nV configuration mode under interface.
`satellite-fabric-link network`	Defines fabric link connectivity to simple ring using keyword “Network.”
`redundancy`	Enters Redundancy configuration mode for ICP group 210.
`iccp-group 210`	
`!`	

Table 4-9 nV L1 Fabric Configuration (continued)

nV L1 Fabric Configuration	Description
satellite 100	Defines the Access ports of satellite ID 100.
remote-ports GigabitEthernet 0/0/0-30,31-43	
!	
satellite 101	Defines the Access ports of satellite ID 101.
remote-ports GigabitEthernet 0/0/0-43	
!	
satellite 102	Defines the Access ports of satellite ID 101.
remote-ports GigabitEthernet 0/0/0-43	
!	
!	
!	
!	
interface GigabitEthernet100/0/0/40	Virtual Interface configuration corresponding to satellite 100. This interface can be configured in L2VPN service (E-Line, E-LAN, or E-Tree).
negotiation auto	
load-interval 30	
!	
interface GigabitEthernet100/0/0/40.502 l2transport	
encapsulation dot1q 49	
!	
!	
redundancy	Configures ICCP redundancy group 210 and defines peer provider edge address in the redundancy group.
iccp	
group 210	
member	
neighbor 100.111.11.2	
!	
nv satellite	Configures system mac for nV communication.
system-mac cccc.cccc.cccc	
!	
!	
!	
!	
nv	Enters nV configuration mode to define satellites.
satellite 100	Defines the Satellite ID.
type asr9000v	Defines ASR 9000v device as satellite device.
ipv4 address 100.100.1.10	Configures satellite address used for Communication.

Table 4-9 nV L1 Fabric Configuration (continued)

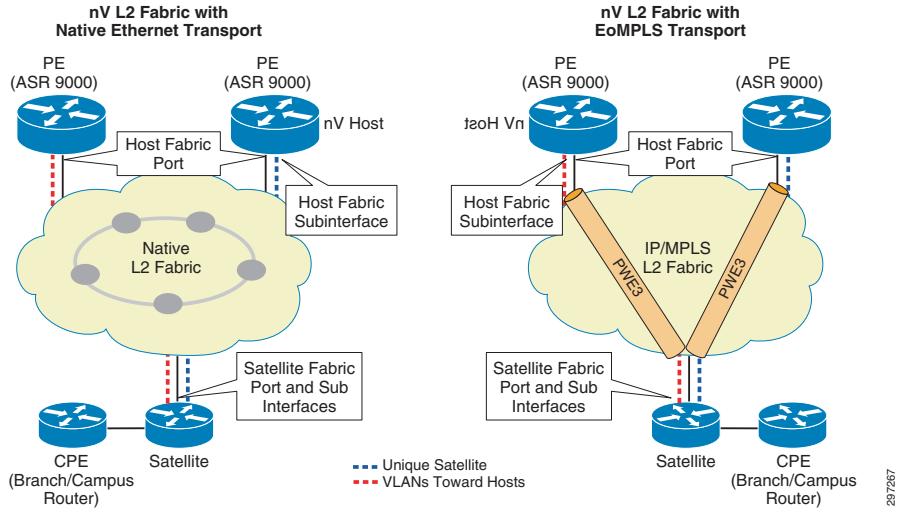
nV L1 Fabric Configuration	Description
redundancy	
Host-priority 20	Defines the priority for the Host provider edge.
!	
serial-number CAT1729U3BF	Satellite chassis serial number to identify satellite.
!	
!	
satellite 101	Defines the Satellite ID.
type asr9000v	Defines ASR 9000v device as satellite device.
ipv4 address 100.100.1.3	Configures satellite address used for Communication.
redundancy	
host-priority 20	Defines the priority for the Host provider edge.
!	
serial-number CAT1729U3BB	Satellite chassis serial number to identify satellite.
!	
satellite 102	Defines the Satellite ID.
type asr9000v	Defines ASR 9000v device as satellite device.
ipv4 address 100.100.1.20	Configures satellite address used for Communication.
redundancy	
Host-priority 20	Defines the priority for the Host provider edge.
!	
serial-number CAT1729U3AU	Satellite chassis serial number to identify satellite.
!	

Note The model above can be implemented by configuring interface GigabitEthernet100/0/0/40.502 for point-to-point E-line or multipoint E-LAN/E-TREE service using VPLS or PBB-EVPN core.

nV Satellite L2 Fabric

In this model, satellite nodes connecting to branch or campus are connected to the host(s) over any L2 Ethernet network. Such a network can be implemented as a native or as an overlay Ethernet transport to fit enterprise access network designs.

Figure 4-4 nV with L2 Fabric Access using Native or Overlay Transport



In the case of L2 Fabric, a unique VLAN is allocated for the point-to-point emulated connection between the Host and each Satellite device. The host uses such VLAN for the advertisement of multicast discovery messages.

Satellite devices listen for discovery messages on all the ports and dynamically create a sub-interface based on the port and VLAN pair on which the discovery messages were received. VLAN configuration at the satellite is not required.

The satellite uses this auto-discovered sub-interface for the establishment of a management session and for the exchange of all upstream and downstream traffic with each of the hosts (data and control). At the host, incoming and outgoing traffic is associated to the corresponding satellite node based on VLAN assignment.

Table 4-9 details nV L2 fabric access configuration.

Table 4-10 nV L2 Fabric Configuration

Network Virtualization L2 Fabric Configuration	Description
`interface TenGigE0/1/1/3`	Interface acting as Fabric link connecting to nV ring.
`load-interval 30`	
`transceiver permit pid all`	
`!`	
`interface TenGigE0/1/1/3.210`	Interface acting as Fabric link connecting to nV ring.
`ipv4 point-to-point`	
`ipv4 unnumbered Loopback200`	
`encapsulation dot1q 210`	
`nv`	Enters nV configuration mode under interface.
`satellite-fabric-link satellite 210`	Defines fabric link connectivity to satellite 210.
`ethernet cfm`	Configures Ethernet cfm to detect connectivity failure to the fabric link.
`continuity-check interval 10ms`	
`!`	

Table 4-10 nV L2 Fabric Configuration

Network Virtualization L2 Fabric Configuration	Description
redundancy	Enters redundancy configuration mode for ICP group 210.
iccp-group 210	
!	
remote-ports GigabitEthernet 0/0/0-9	Defines the Access ports of satellite ID 100.
!	
!	
!	
interface GigabitEthernet210/0/0/0	Virtual Interface configuration corresponding to satellite 100 . This interface can be configured in L2VPN service (E-Line, E-LAN or E-Tree).
negotiation auto	
load-interval 30	
!	
interface GigabitEthernet210/0/0/0.49 l2transport	
encapsulation dot1q 49	
!	
redundancy	Configures ICCP redundancy group 210 and defines peer provider edge address in the redundancy group.
iccp	
group 210	
member	
neighbor 100.111.11.2	
!	
nv satellite	Configures system mac for nV communication.
system-mac cccc.cccc.cccc	
!	
!	
!	
!	
nV	Enters nV configuration mode to define satellites.
satellite 210	Define the Satellite ID 210 and type of platform ASR 901
type asr901	
ipv4 address 27.27.27.40	
redundancy	
host-priority 17	Defines the priority for the Host provider edge.
!	
serial-number CAT1650U00D	Satellite chassis serial number to identify satellite.
!	
!	

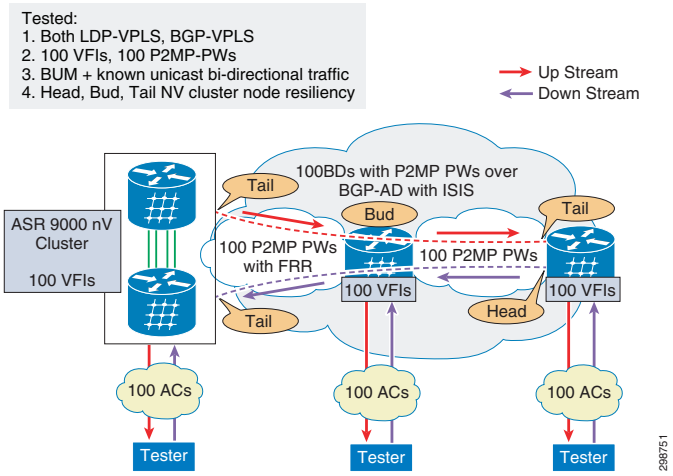
Note The model above can be implemented by configuring interface GigabitEthernet210/0/0/0.49 for point-to-point E-line or multipoint E-LAN/E-TREE service using VPLS or PBB-EVPN core.

nV Cluster

In this physical topology, we tested and measured fast convergence of VPLS-BGP LSM using P2MP-TE with ASR 9000 nV cluster technology and compared it against MC-LAG for dual-homing redundancy use cases.

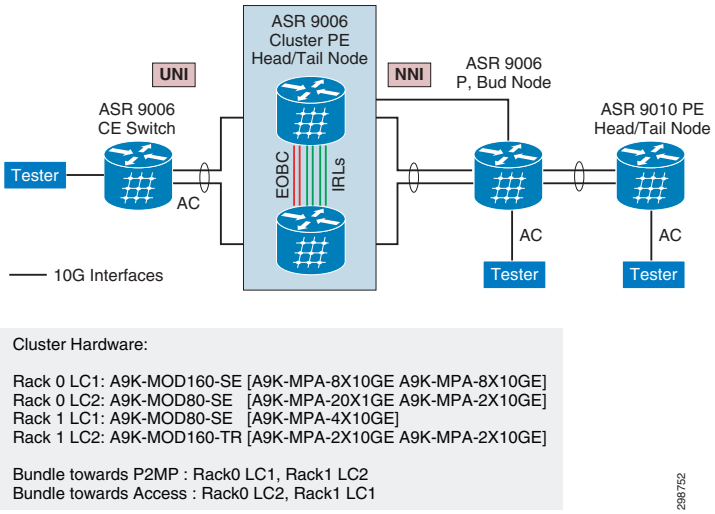
The UNI customer edge switch (left side) has normal LAG running LACP connected to an nV cluster ASR 9000 system for dual-homing redundancy instead of MC-LAG. The nV cluster acts as a single VPLS provider edge with 1 control plane and 1 data plane. VPLS-BGP LSM service is provisioned to the remote ASR9k VPLS provider edge. The provider router (BUD node) has dual-roles as a VPLS-BGP LSM provider edge and provider transit node connected to the nV cluster VPLS provider edge. MC-LAG convergence numbers were separately in this topology for comparison without nV cluster configuration.

Figure 4-5 VPLS-BGP LSM Cluster Convergence Test Topology



The logical VPLS service configuration and scale is described in Figure 14. We configured 100 VFIs with 100 P2MP-TEs to carry BUM + known unicast bi-directional traffic. The nV cluster provider edge is both Head-end and Tail-end provider edge of VPLS-BGP LSM and we tested and validated Head, Tail and Bud nV cluster node resiliency.

Figure 4-6 VPLS-BGP LSM Logical Configuration and Traffic Path

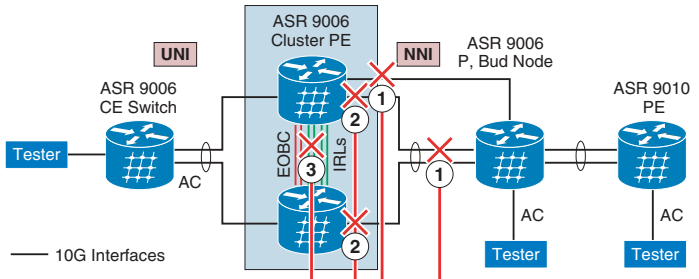


The convergence results of VPLS-BGP LSM nV cluster system Vs MC-LAG are summarized in Figure 4-7 and Figure 4-8, respectively. The 6 types of failure tests listed below. Note, each test is repeated 3 times and the worst case numbers of 3 trials are reported.

1. Core FRR failure between Head and Bud node: test 1-4
2. Core isolation failure: test 5-8
3. IRL link failure: test 9-12
4. EOBC link failure: test 13-16
5. DSC and RP redundancy switchover: test 17-18
6. Power off Primary DSC failover: test 21-24

For nV cluster deployment of L2VPN, the XR 5.2.2 release or above for deployments is recommended.

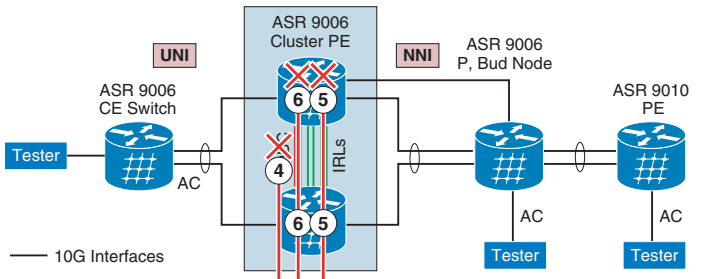
Figure 4-7 VPLS-BGP LSM Convergence Results Part 1



Failure	Test #	Trigger	Upstream Convergence	Downstream Convergence	MC-LAG Convergence
Core FRR failure between: Head and Bud node	1	Cluster core facing LAG LOS	12 msec	21 msec	N/A
	2	Cluster core facing link LOS	4 msec	12 msec	N/A
Core FRR failure between: Head and Bud node	3	Cluster core facing LAG repair	12 msec	0.4 msec	N/A
	4	Cluster core facing link repair	24 msec	4 msec	N/A
Core isolation failure: Force all traffic over IRL to rack 0 or rack 1	5	Rack 0: Remove LC with all core facing link and LAG member (ie. LOS)	85 msec	16 msec	6 sec/5 sec
	6	Rack 1: Remove LC with all core facing and LAG member (ie. LOS)	216 msec	17 msec	5 sec/7 sec
Core isolation recovery: Repair core links to force all traffic off IRLs on rack 0 or rack 1	7	Rack 0: Insert LC with all core facing link and LAG member	0.6 msec	0.36 msec	0/0
	8	Rack 1: Insert LC with all core facing LAG member	30 mec	66 msec	0/0
IRL Link failure with traffic	9	Remove IRLs 1 by 1 manually	0	0	N/A
	10	Remove LC with all IRLs	236 msec	163 msec	N/A
IRL Link addition with traffic	11	Add IRLs 1 by 1 manually	0	0	N/A
	12	Add LC with all IRLs manually	0.5 msec	42 msec	N/A

298753

Figure 4-8 VPLS-BGP LSM Convergence Results Part 2



Failure	Test #	Trigger	Upstream Convergence	Downstream Convergence	MC-LAG Convergence
EOBC redundancy link down	13	Pull out EOBC link on Primary-DSC	0	0	N/A
	14	Pull out EOBC link on Backup-DSC	0	0	N/A
EOBC redundancy link up	15	Insert EOBC link on Primary-DSC	0	0	N/A
	16	Insert EOBC link on Backup-DSC	0	0	N/A
DSC redundancy switchover	17	Rack 0: Primary DSCs RP failover	0	0	0/0
	18	Rack 1: Primary DSCs RP failover	0	0	0/0
DSC RP reload	19	Rack 0: Reload RP of Primary DSC	30 msec	90 msec	5 sec/4 sec
	20	Rack 1: Reload RP of Primary DSC	27 msec	46 msec	3 sec/8.5 sec
Power Off: Primary DSC	21	Rack 0 = Primary DSC, Rack 1 = Backup DSC	45 sec (ddts filed) 200 msec (w/. fix)	60 msec 120 msec	6 sec/3 sec
	22	Rack 1 = Primary DSC, Rack 0 = Backup DSC	43 sec (ddts filed) 204 msec (w/fix)	80 msec 170 msec	7 sec/4.5 sec
Power On: Primary DSC	23	Rack 0 = Primary DSC, Rack 1 = Backup DSC	40 msec	60 msec	0/0
	24	Rack 1 = Primary DSC, Rack 0 = Backup DSC	45 msec	10 msec	0/0

298754

MPLS Access Using Pseudo-wire Head-end (PWHE)

In MPLS Access, enterprise-access devices are connected to the ASR 9000 provider edge devices with the MPLS-enabled network. The branch or campus router is connected to the access device via an Ethernet 802.1Q-tagged interface. The access device is configured with a pseudo-wire terminating on the provider edge device on a pseudo-wire head-end interface.

The pseudo-wire head-end (PWHE) is a technology that allows termination of access pseudo-wires into an L3 (VRF or global) domain, therefore eliminating the requirement of keeping separate interfaces for terminating pseudo-wire and L3VPN service. PWHE introduces the construct of a "pseudo-wire-ether" interface on the provider edge device. This virtual pseudo-wire-ether interface terminates the pseudo-wires carrying traffic from the CPE device and maps directly to an MPLS VPN VRF on the provider edge device. Any QoS and ACLs are applied to the pseudo-wire-ether interface.

All traffic between the customer edge router and provider edge router is tunneled in this pseudo-wire. Access network runs its LDP/IGP domain along with Labeled BGP, as mentioned in the Large Scale Network Design and Implementation, page 2-10, and learns provider edge loopback address accordingly for pseudo-wire connectivity. The access device can initiate this pseudo-wire using two methods:

- Per access node method in which all customer edge-facing ports share a common bridge domain and a pseudo-wire is configured using an Xconnect statement under the switched virtual interface (SVI) associated to the bridge domain VLAN. The bridge domain VLAN is called service VLAN (S-VLAN) and is pushed as a second VLAN on the top of customer VLAN (C-VLAN) received from the enterprise CPE. On the ASR9000 provider edge device the pseudo-wire terminates on PWHE main interface and individual PWHE sub-interfaces terminate the combination of common S-VLAN and distinct C-VLAN.
- Per Access Port method in which a pseudo-wire is directly configured on the interface connecting to the CPE. No VLAN manipulation is required at the customer edge interface. Similar to the Per Access Node Method, on the ASR 9000 node the pseudo-wire is terminated on a PWHE main interface while a dedicated PWHE sub-interface terminates the specific VLANs.

The PWHE sub-interfaces are then mapped to the VPLS VFI or PBB-EVPN EVI associated to the corresponding L2VPN service.

Figure 4-9 shows the PWHE configuration.

Figure 4-9 MPLS Access Using Pseudo-wire Head-End

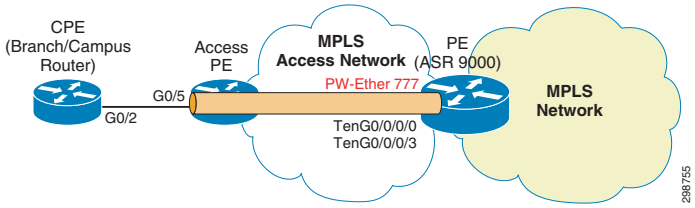


Table 4-11 and Table 4-12 details the MPLS access implementation with per access port method.

Table 4-11 Access Provider Edge Configuration

Access Provider Edge Configuration	Description
`interface GigabitEthernet0/5`	Customer-facing interface.
`mtu 1500`	
`no ip address`	

Table 4-11 Access Provider Edge Configuration (continued)

Access Provider Edge Configuration	Description
service instance 555 ethernet	Xconnect with the provider edge device on the EVC.
encapsulation 555	
xconnect 100.111.11.1 15 encapsulation mpls	

Table 4-12 Provider Edge Configuration

Provider Edge Configuration	Description
interface PW-Ether777	Configured PWHE main interface.
attach generic-interface-list pwhe_mux	Attaches interface list to the PWHE interface.
!	
generic-interface-list pwhe_mux	Creates generic-interface list.
interface TenGigE0/0/0/0	Assigns interfaces to the list.
interface TenGigE0/0/0/3	
!	
interface PW-Ether777.555 l2transport	PWHE L2 sub-interface.
encapsulation dot1q 555	Matching the customer VLAN C-VLAN.
rewrite ingress tag pop 1 symmetric	Symmetric Pop Operation before associating with VFI.
!	
l2vpn	Enters L2VPN configuration mode.
xconnect group pwhe_mux	Enters the name of the cross-connect group.
p2p pwhe_mux	Enters a name for the point-to-point cross-connect.
interface PW-Ether777	Specifies the attachment circuit.
neighbor ipv4 100.111.13.9 pw-id 15	Pseudo-wire to access node.
!	
bridge group pwhemux	Configures bridge group named pwhemux.
bridge-domain pwhemux	Configures Bridge-domain named pwhemux.
interface PW-Ether777.555	Enables PWHE sub-interface connected towards CPE.
!	
vfi pwhemux	Creates VFI instance with VPLS neighbors.
neighbor 100.111.3.2 pw-id 777	
!	
neighbor 100.111.5.5 pw-id 777	
!	
!	

Table 4-13 and Table 4-14 details the MPLS access implementation with per access node method.

Table 4-13 Access Provider Edge Configuration

Access Provider Edge Configuration	Description
`interface GigabitEthernet0/15`	Customer-connecting interface.
`switchport trunk allowed vlan none`	
`switchport mode trunk`	
`service instance 555 ethernet`	
`encapsulation dot1q 555`	Matching customer VLAN C-VLAN 555.
`rewrite ingress tag push dot1q 15 symmetric`	Pushing service VLAN S-VLAN 15.
`bridge-domain 15`	Associating to common Bridge-domain 15.
`!`	
`interface VLAN15`	Configured VLAN associated to the Bridge domain 15.
`no ip address`	
`xconnect 100.111.5.5 15 encapsulation mpls`	SVI based Xconnect to SE Node

Table 4-14 Provider Edge Configuration

Provider Edge Configuration	Description
`interface PW-Ether777`	Configured PWHE main interface.
`attach generic-interface-list pwhe_mux`	Attaches interface list to the PWHE interface.
`!`	
`generic-interface-list pwhe_mux`	Creates generic-interface list.
`interface TenGigE0/0/0/1`	Assigns interfaces to the list.
`interface TenGigE0/0/0/2`	
`!`	
`interface PW-Ether777.555 l2transport`	PWHE L2 sub-interface.
`encapsulation dot1q 15 second-dot1q 555`	Matching for outer S-Tag and inner C-Tag.
`rewrite ingress tag pop 2 symmetric`	Symmetric Pop Operation before associating with VFI.
`!`	
`l2vpn`	Enters L2VPN configuration mode.
`xconnect group pwhe_mux`	Enters the name of the cross-connect group.
`p2p pwhe_mux`	Enters a name for the point-to-point cross-connect.
`interface PW-Ether777`	Specifies the attachment circuit.
`neighbor ipv4 100.111.7.3 pw-id 15`	Pseudo-wire to access node.
`!`	
`bridge group pwhemux`	Configures bridge-group named pwhemux.
`bridge-domain pwhemux`	Configures bridge-domain named pwhemux.
`interface PW-Ether777.555`	Enables PWHE sub-interface connected towards CPE.
`!`	

Table 4-14 Provider Edge Configuration

Provider Edge Configuration	Description
`vfi pwhemux`	Creates VFI instance with VPLS neighbors.
`neighbor 100.111.3.2 pw-id 777`	
`!`	
`neighbor 100.111.11.1 pw-id 777`	

Note The model above can be implemented by configuring interface PW-Ether777.555 for point-to-point E-line or multipoint E-LAN/E-TREE service using VPLS or PBB-EVPN core.