

9 VPN

Introduce the VPN protocols and features.

9.1 PWE3

PWE3 is an end-to-end Layer 2 service carrying technology and is a type of point-to-point L2VPN technology. PWE3 is proposed by the IETF PWE3 working group as one of the solutions for connecting the traditional communication network with the PSN network.

9.2 Native TDM

In Native TDM, TDM frames are directly encapsulated to GPON GEM frames. This mode features simple encapsulation, small network cost, and guaranteed link quality. TDMoGEM mode and TDMoETH mode are encapsulated to NativeTDM in access network at present, and the MA5800 supports TDMoETH mode.

9.3 VPLS

The Virtual Private LAN Service (VPLS), also called the Transparent LAN Service (TLS) or virtual private switched network service, is a Layer 2 VPN (L2VPN) technology that is based on Multi-Protocol Label Switching (MPLS) and Ethernet technologies.

9.4 VRF

Virtual route forwarding instance (VRF) is a mechanism in which a device works as multiple virtual routing devices. After the Layer 3 interfaces of the device are divided into different VRFs, multiple route forwarding instances can be emulated on the device.

9.5 BGP/MPLS IP VPN

9.6 GRE

9.1 PWE3

PWE3 is an end-to-end Layer 2 service carrying technology and is a type of point-to-point L2VPN technology. PWE3 is proposed by the IETF PWE3 working group as one of the solutions for connecting the traditional communication network with the PSN network.

9.1.1 Introduction to PWE3

Definition

Pseudo-wire emulation edge to edge (PWE3) is a type of Layer 2 service carrying technology. It is mainly used to emulate the essential behavior and characteristics of the services such as the ATM, frame relay, Ethernet, low-rate time division multiplexing (TDM) circuit, and synchronous optical network (SONET)/synchronous digital hierarchy (SDH) as faithfully as possible in a packet switched network (PSN).

PWE3 is implemented on access devices through MPLS and IP technologies. MPLS supports PWE3 by using the LDP or RSVP-TE protocol as signaling.

Purpose

PWE3 can interconnect the traditional network with PSN to share resources and expand the reach of networks. For example, PWE3 can emulate services such as TDM, ATM, and Ethernet, and can implement service interoperation by using existing PSN (IP/MPLS) as the bearer network.

Benefit

PWE3 connects the traditional TDM, ATM, and Ethernet networks with PSN (IP/MPLS). In this way, PWE3 protects the investment on the traditional TDM, ATM, and Ethernet networks, and also implements the all-IP network architecture.

9.1.2 PWE3 Reference Standards and Protocols

The following lists the reference standards and protocols of this feature.

- RFC 3985: Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture
- RFC 4447: Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)
- RFC 3916: Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3)
- RFC 4446: IANA Allocations for Pseudo wire Edge to Edge Emulation (PWE3)
- RFC 4717, Encapsulation Methods for Transport of Asynchronous Transfer Mode (ATM) over MPLS Networks
- RFC 4816, Pseudowire Emulation Edge-to-Edge (PWE3) Asynchronous Transfer Mode (ATM) Transparent Cell Transport Service
- RFC 4448: Encapsulation Methods for Transport of Ethernet over MPLS Networks
- RFC 5085: PW vccv A control Channel for PW
- RFC 4553: Structure-Agnostic Time Division Multiplexing (TDM) over Packet (SAToP)
- RFC 5462: Multi-Protocol Label Switching (MPLS) Label Stack Entry EXP Field Renamed to Traffic Class Field
- RFC 4385: Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN

- RFC 6870: Pseudowire Preferential Forwarding Status Bit
- draft-bryant-filsfils-fat-pw-03.txt

9.1.3 PWE3 Principle

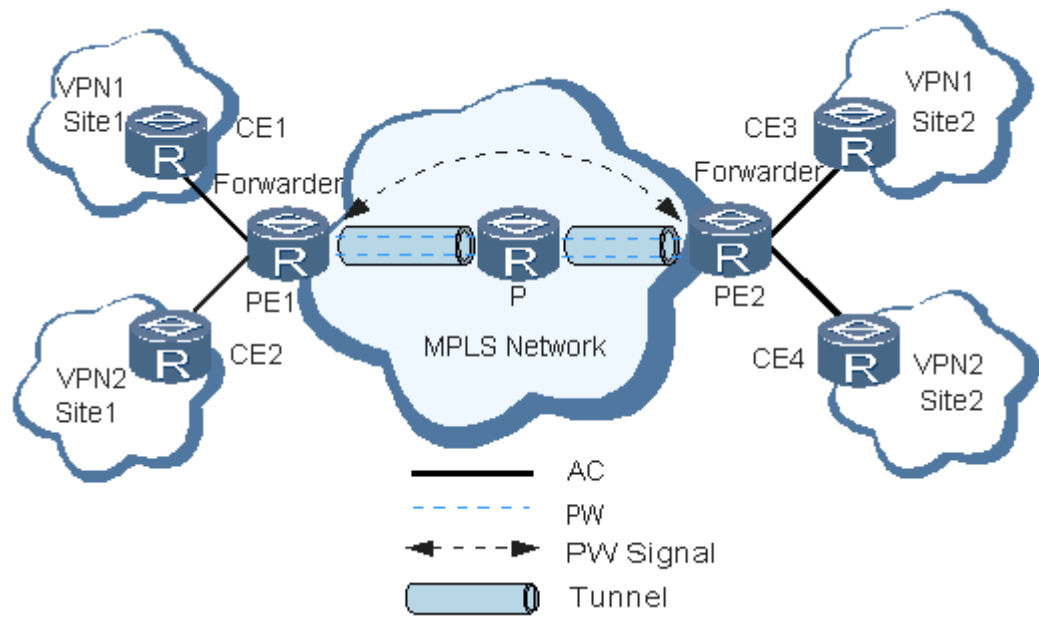
9.1.3.1 Basic Principle of PWE3

Basic PWE3 Transmission Components

Pseudo wire emulation edge-to-edge (PWE3), which uses LDP and RSVP-TE as the signaling protocols, carries various types of Layer 2 services, such as various types of Layer 2 data packets, from the customer edge (CE), and transparently transmits the Layer 2 data through tunnels (such as MPLS LSP or TE tunnels). As shown in [Figure 9-1](#), the basic PWE3 transmission components include the following:

- Attachment circuit (AC): a link between CE and PE. All user packets (including Layer 2 and Layer 3 protocol packets of users) on the AC are transparently forwarded to the peer end.
- Pseudo wire (PW): PW is a kind of virtual connection between two PEs. It is a mechanism for two PEs in the packet-switched network to transfer essential elements of emulation service. A PW conveys VC information by signaling (LDP or RSVP-TE). Since VC is directional, PW is directional too. For the PWE3 system, a PW is like a direct channel between a local AC and a peer AC and is used for transparently transmitting the Layer 2 data of users.
- Forwarder: After a PE receives data frames from an AC, the forwarder selects a PW for forwarding the frames. In fact, the forwarder is a forwarding table of PWE3.
- Tunnel: A tunnel is a direct channel between a local PE and a peer PE and is used for transparently transmitting data between the PEs. Tunnels are used for carrying PWs. A tunnel can carry multiple PWs. Generally, the tunnel refers to an MPLS tunnel.
- PW signaling protocol: A PW signaling protocol is the basis for implementing PWE3 and is used to create and maintain PWs. Current PW signaling protocols are mainly LDP and RSVP-TE.
- Encapsulation: The packets transmitted through the PW use the standard PW encapsulation format and technology. There are multiple PWE3 encapsulation types on a PW. The formats are defined in detail in draft-ietf-pwe3-iana-allocation-x.
- Quality of service (QoS): The priority information at the header of Layer 2 user packets is mapped to the QoS priority for transmitting the packets in the public network. In general, support for MPLS QoS is required.

Figure 9-1 Basic PWE3 transmission components

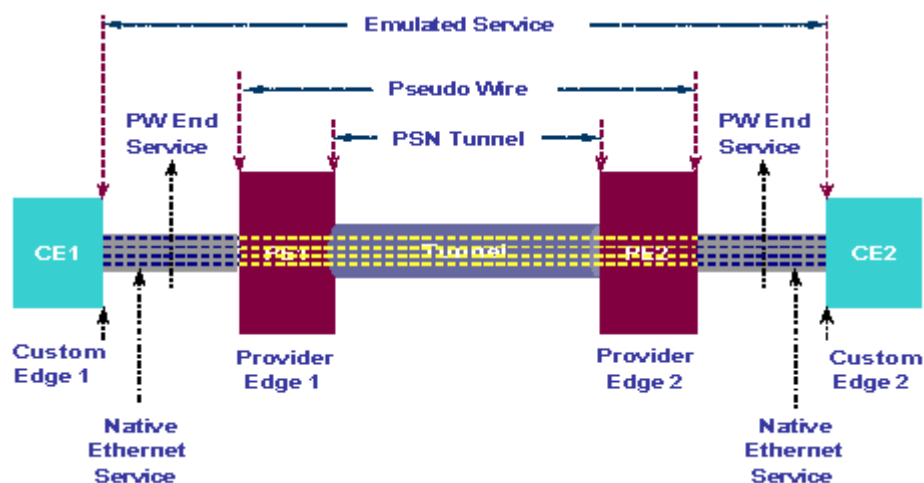


Assume that the VPN1 packet stream travels from CE1 to CE3. The basic data flow would be as follows:

- CE1 transmits a Layer 2 packet to PE1 through an AC.
- After PE1 receives the packet, the forwarder selects a PW for forwarding the packet.
- PE1 generates two MPLS labels according to the PW forwarding entry. The private network label is used for identifying the PW, and the public network label is used for transmitting the packet to PE2 through the tunnel.
- The Layer 2 packet arrives at PE2 through the public network tunnel. The system extracts the private network label (the public network label is extracted by the penultimate P device).
- The forwarder of PE2 selects an AC for forwarding the packet, and then PE2 forwards the packet to CE3.

PWE3 Network Model

Figure 9-2 shows a PWE3 reference model.

Figure 9-2 PWE3 network model

The channel set up in a PWE3 network is a point-to-point channel. Channels are isolated from each other. Layer 2 user packets are transparently transmitted between PWs. The following provides a detailed description.

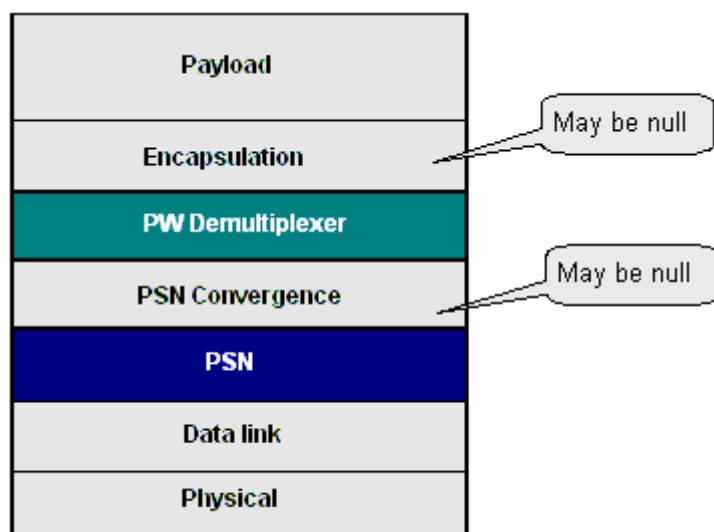
- According to the services requirements of the CE, one or more PWs are set up between PE1 and PE2. Multiple PWs can be carried on one PSN tunnel.
- For the PEs, after the PW is set up, the mapping between the user access interface (AC) and virtual link (PW) is determined.
- The PSN device only needs to forward the MPLS packet according to the MPLS label, regardless of the Layer 2 user packet encapsulated inside the MPLS packet.

PWE3 Service Model

Figure 9-3 shows a PWE3 service model. According to the PWE3 service model, PWE3 is presented by an outer label (PSN tunnel) and an inner label (PW demultiplexer).

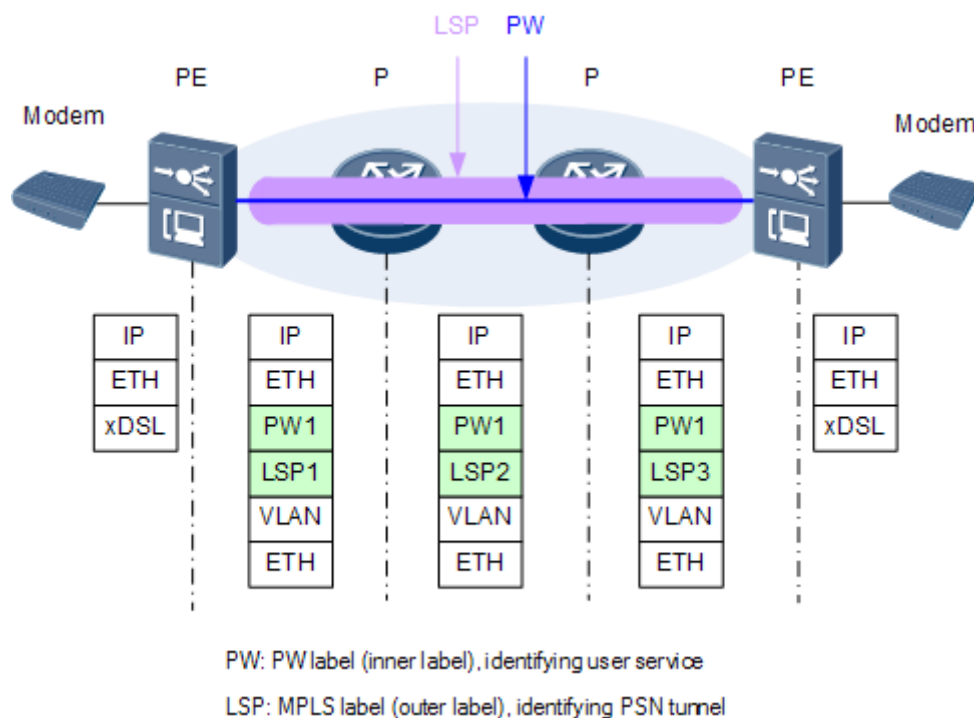
The PSN layer can adopt the MPLS and IP technologies, and the PW demultiplexer layer can adopt the MPLS, UDP, or L2TP technology. Hence, the supported combinations of PWE3 outer labels and inner labels are as follows: MPLS over MPLS, MPLS over IP, UDP over IP, and L2TP over IP.

Figure 9-3 PWE3 service model



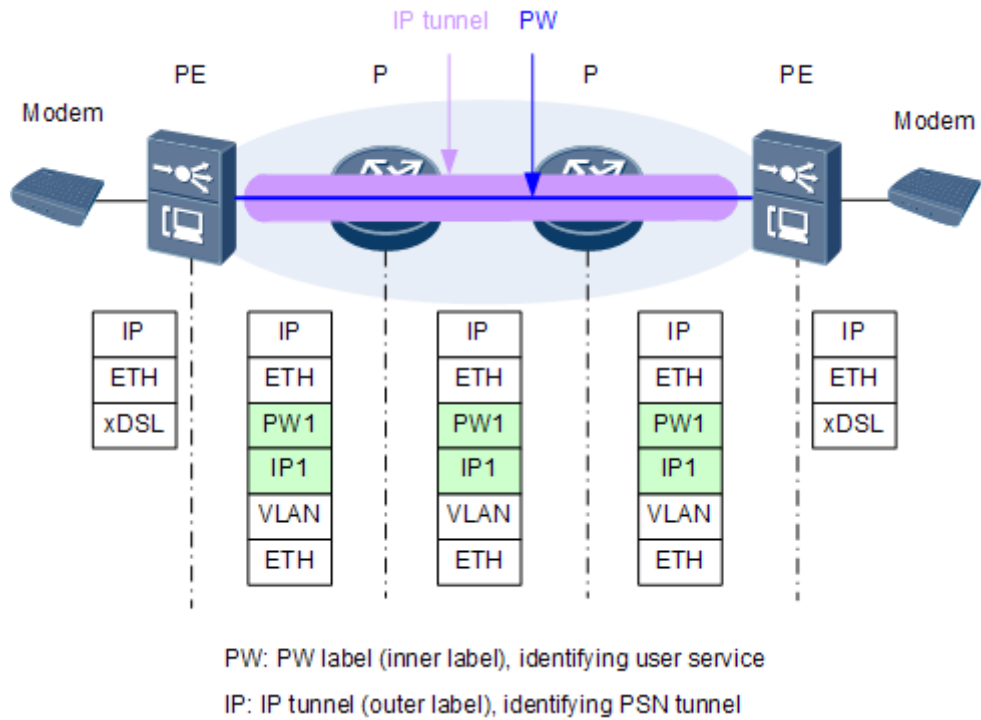
- **Figure 9-4** shows the PWE3 protocol stack in the MPLS over MPLS encapsulation mode.

Figure 9-4 PWE3 protocol stack in the MPLS over MPLS encapsulation mode



- **Figure 9-5** shows the PWE3 protocol stack in the MPLS over IP encapsulation mode.

Figure 9-5 PWE3 protocol stack in the MPLS over IP encapsulation mode



- Figure 9-6 shows the PWE3 protocol stack in the UDP over IP encapsulation mode.

Figure 9-6 PWE3 protocol stack in the UDP over IP encapsulation mode

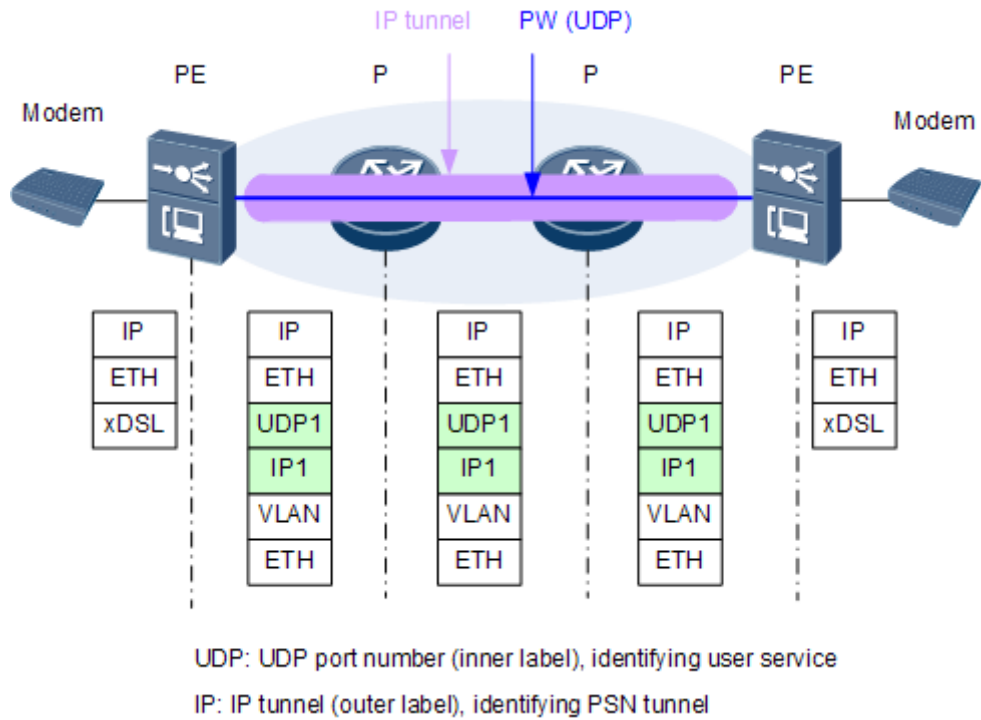
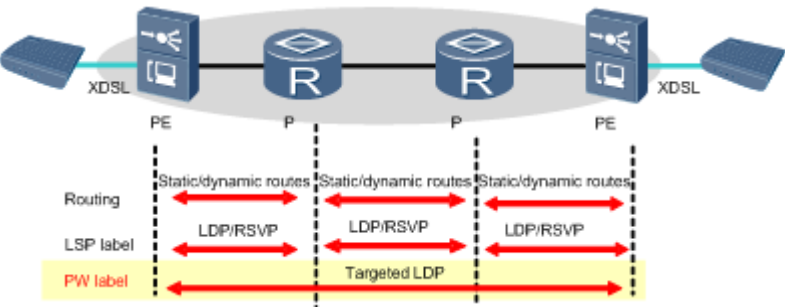


Figure 9-7 illustrates the principle of PW label distribution.

Figure 9-7 Principle of PW label distribution



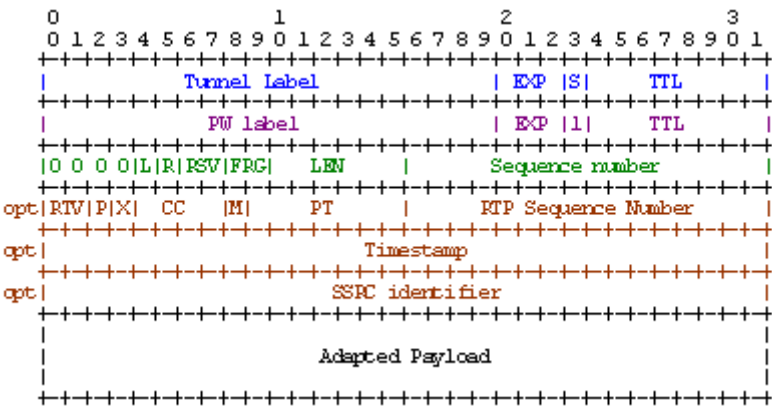
Packet Format

PWE3 has three packet formats: MPLS+PW, IP+PW, and IP+UDP.

- MPLS+PW: In this packet format, the combination of PWE3 outer label and inner label is MPLS over MPLS. It is applicable to MPLS network transmission.

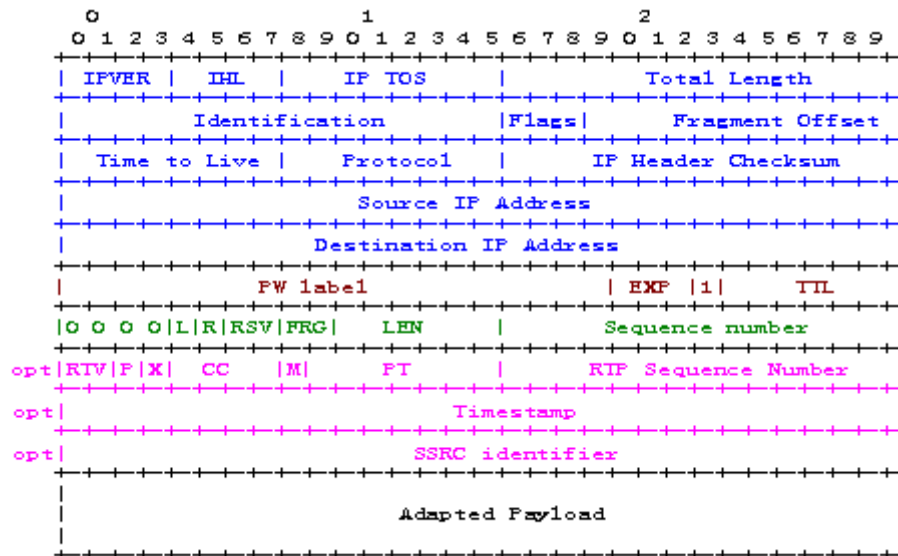
Figure 9-8 shows the format of an MPLS+PW PWE3 packet.

Figure 9-8 Format of an MPLS+PW PWE3 packet



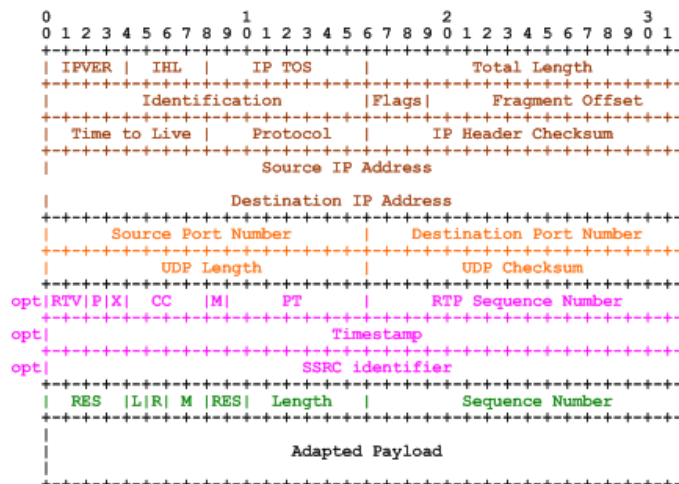
- IP+PW: In this packet format, the combination of PWE3 outer label and inner label is MPLS over IP. It is applicable to MPLS over IP network transmission. Different from MPLS+PW packets, IP+PW packets are forwarded at IP Layer 3 when transmitted over the PSN network.

Figure 9-9 shows the format of an IP+PW PWE3 packet.

Figure 9-9 Format of an IP+PW PWE3 packet

- IP+UDP: In this packet format, the combination of PWE3 outer label and inner label is UDP over IP. It is applicable to IP network transmission. Different from MPLS+PW packets, IP+UDP packets are forwarded at IP Layer 3 and meanwhile forwarded at Layer 2 by UDP port redirection when transmitted over the PSN network.

Figure 9-10 shows the format of an IP+UDP PWE3 packet.

Figure 9-10 Format of an IP+UDP PWE3 packet

9.1.3.2 Principle of TDM PWE3

The TDM service is transmitted over the PSN by circuit emulation. There are two packet encapsulation formats.

- The structure-aware packet, which is also called CESoPSN packet, is defined in RFC5086 and RFC5687.

 NOTE

Circuit emulation service over packet switched network (CESoPSN) is a generic term for circuit emulation service and also refers to structure-aware circuit emulation.

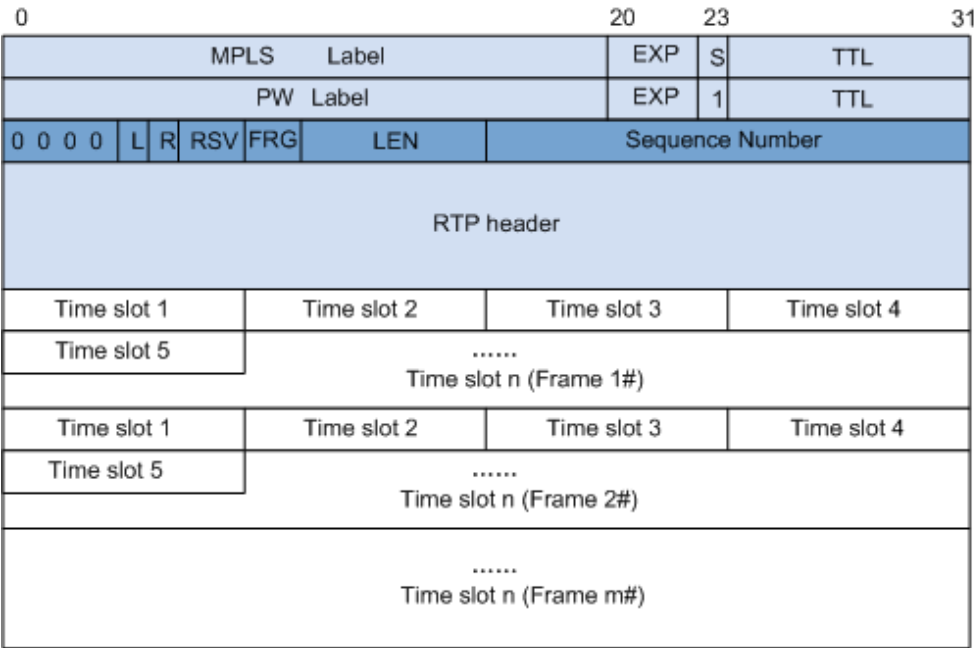
- The structure-agnostic packet, which is also called SAToP packet, is defined in RFC4553.

CESoPSN Packet Format (structure-aware packet format)

The CESoPSN standard provides the channelized TDM service with emulation and transmission functions, and can identify the TDM frame structure and in-frame signaling. Therefore, if the customer needs to provide services based on the timeslot, the CESoPSN packet format can meet this requirement.

Figure 9-11 shows the format of the CESoPSN packet.

Figure 9-11 CESoPSN packet format



- A CESoPSN packet contains a four-byte MPLS header and a four-byte PW header. The length of the CESoPSN control word is 4 bytes, including fields as shown in **Table 9-1**.
- The length of the Real-Time Transport Protocol (RTP) header is 12 bytes, including the version number, padding flag, and time stamp fields. The time stamp field, whose length is 32 bits, is used for clock synchronization. For format of the RTP header, see RFC3550.
- Time slot indicates the TS in the TDM frame. Each TS occupies 8 bits. All TSs comprise the encapsulated TDM data payload, which does not include the CRC bit. The number of encapsulated frames and the number of TSs in each frame can be set by users according to conditions.

Table 9-1 Fields of the control word

Field	Description
0000	This field is generally all 0s, with the length of 4 bits. When the virtual circuit connectivity verification (VCCV) is needed to help to monitor the SAToP PW status, these four bits are used to identify the start of the associated channel header (ACH).
L	Indicates whether the TDM data in the packet is valid. Its length is 1 bit. When it is set to 1, it indicates that the TDM data in the packet is invalid; that is, the TDM data in the packet can be neglected to save bandwidth resources.
R	Indicates whether the interconnection function of the local customer edge (CE) is in the packet loss state. When it is set to 0, it indicates that consecutive packets have been received and will no longer be lost.
RSV	Indicates the reserved bit. Its length is 2 bits.
FRG	Indicates the fragmentation status of the packet. Its length is 2 bits. Its values are as follows: • 00: Indicates that the packet encapsulates the entire TDM data. • 01: Indicates that the packet encapsulates the first fragmentation of the TDM data. • 10: Indicates that the packet encapsulates the last fragmentation of the TDM data. • 11: Indicates that the packet encapsulates the intermediate fragmentation of the TDM data.
LEN	Indicates the length of the entire CESoPSN packet (the size of the CESoPSN header and TDM data.) When the length is shorter than 64 bytes, LEN is a specific length value. When the length is equal to or longer than 64 bytes, LEN is 0.
Sequence Number	Indicates the sequence number for transmitting the CESoPSN packet. Its length is 16 bits. Its initial value should be random. It must be incremented by 1 with each CESoPSN data packet sent in the specific PW.

The CESoPSN packet structure has the following characteristics:

- CESoPSN provides emulation and transmission of structure-aware TDM service. That is, CESoPSN can identify the TDM frame structure and in-frame signaling and transmit the frames.
For example, a structure-aware E1 link consists of 32 timeslots. Except timeslot 0, the other 31 timeslots can each carry a channel of 64 kbit/s voice service. Timeslot 0 is used only for transmitting signaling and frame delimiter.

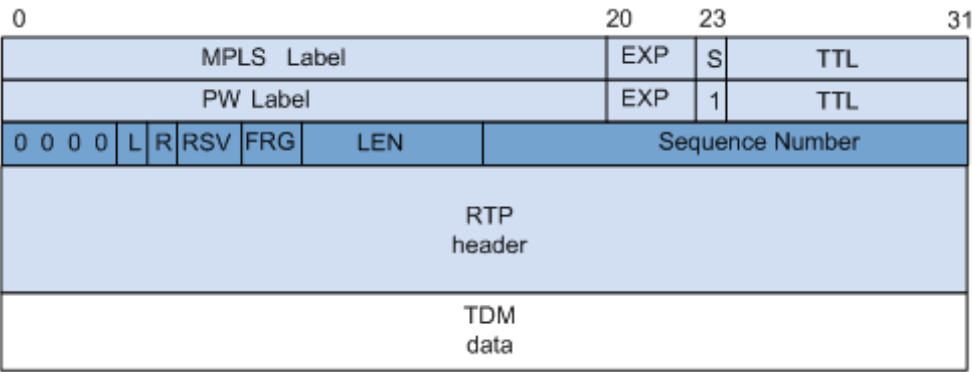
- CESoP can identify the TDM frame structure. Therefore, idle timeslots are not transmitted, and only the data in the timeslots that are useful for the CE devices is retrieved from the E1 service stream and transmitted after being encapsulated into CESoPSN frames.
- CESoPSN can identify and transmit the CAS and CCS signaling of E1 service streams.

SAToP Packet Format (structure-agnostic packet format)

The structure-agnostic TDM over PSN (SAToP) standard provides the non-channelized TDM service with the emulation and transmission functions. The protocol need not be aware of the structure of the TDM packets and transparently transmits the packets. Therefore, if the customer only needs to provide services based on E1/T1, SAToP (unstructured packet format) can meet this requirement.

Figure 9-12 shows the format of the SAToP packet.

Figure 9-12 SAToP packet format

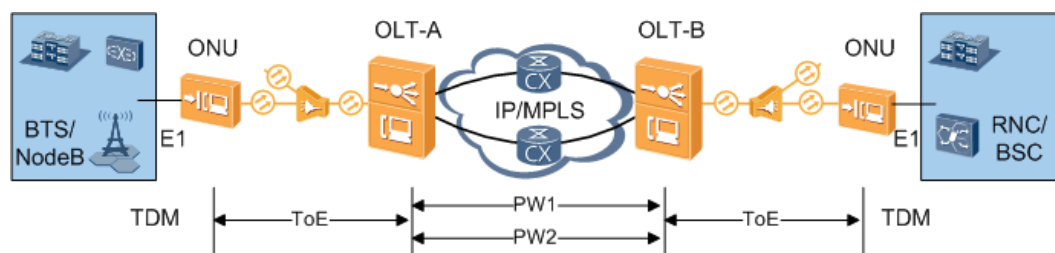


- An SAToP packet also contains a four-byte MPLS header and a four-byte PW header. The length of the SAToP control word is 4 bytes, including fields as shown in Table 9-1.
- The SAToP protocol treats the TDM service as serial data code stream for segmentation, and transmits the service over PWs after encapsulation. SAToP can transmit the synchronization timing information although it is unaware of the structure of the TDM frame.

Application Scenario

As shown in Figure 9-13, OLT-A and OLT-B are symmetrically deployed on both sides of the PSN network. Both OLT-A and OLT-B are connected to ONUs through GPON lines. Enterprise or base transceiver station (BTS) private line services are transmitted to the ONUs through E1 ports. Proprietary TOE channels between the ONUs and OLTs are used to encapsulate the packets of TDM services. Symmetrical TDM PWs are created between the 2 OLTs to provide cross-PSN-network access and backhaul for enterprise or BTS private line services.

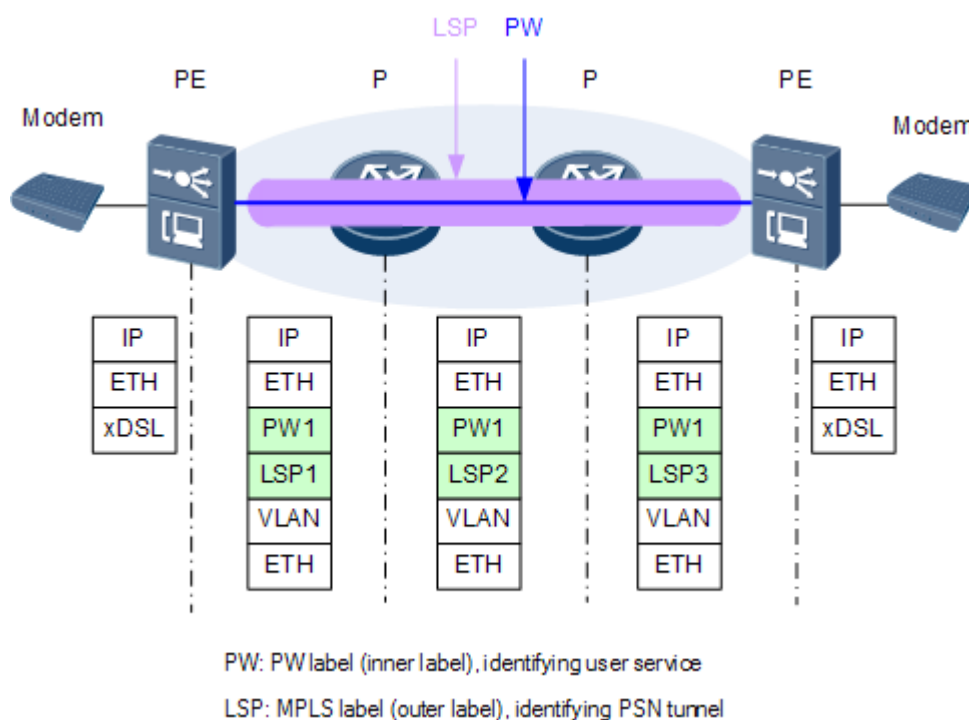
Figure 9-13 Example network of symmetrical GPON TDM PWE3 access



QoS Processing

Figure 9-14 shows the QoS processing flow of TDM PWE3 service, considering the example of SAToP (MPLS over MPLS encapsulation).

Figure 9-14 QoS processing flow of upstream SAToP service (MPLS over MPLS encapsulation)



9.1.3.3 Principle of ETH PWE3

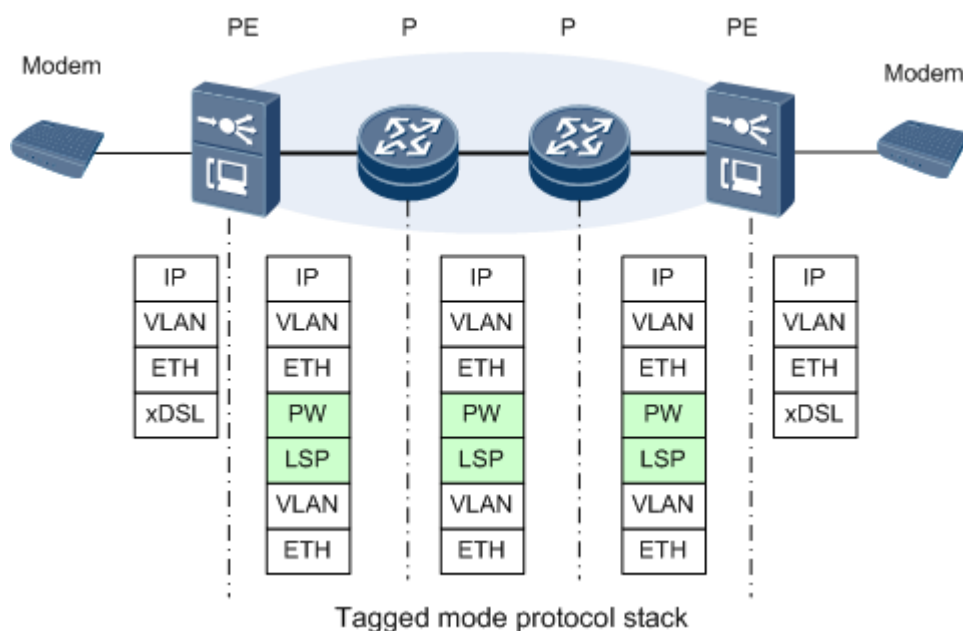
Processing Flow of ETH PWE3 Protocol Packets

Two encapsulation formats are defined in RFC4448 for the PWE3 emulation of Ethernet service in a PSN network.

- Tagged mode. In this mode, the packet going upstream carries the PW VLAN tag in the payload, and is stripped of the PW VLAN tag when going downstream.
- Raw mode. In this mode, the packet going upstream does not carry the PW VLAN tag; the PW payload, however, can carry the service VLAN tag.

Figure 9-15 shows the processing flow of ETH PWE3 protocol packets on the PE and P devices. The MA5800 can function as a PE or a P device. The PE establishes an MPLS-based PW tunnel, encapsulates the user data packets with two labels at the Tx end and transmits the packets. The P device forwards the packets. The PE at the Rx end decapsulates the received MPLS packets, restores the original user data packets, and transmits the packets to the user.

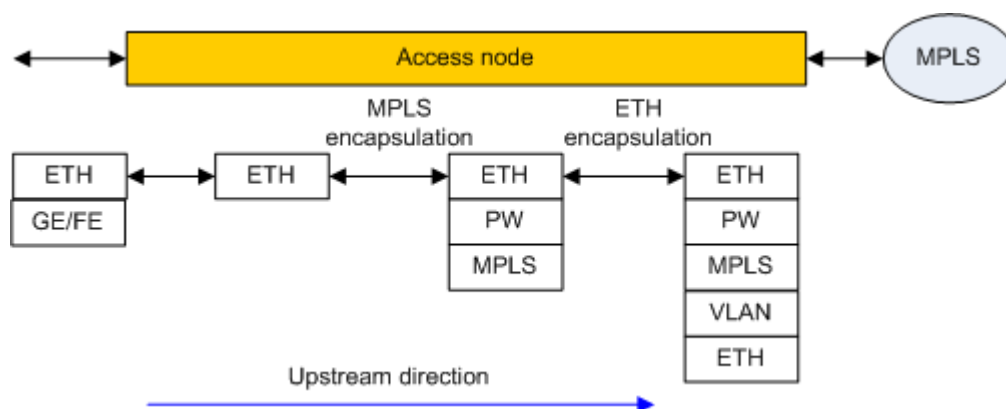
Figure 9-15 Processing flow of ETH PWE3 protocol packets



Processing Flow of ETH PWE3 Service

Figure 9-16 shows the processing flow of ETH PWE3 service (MPLS over MPLS encapsulation).

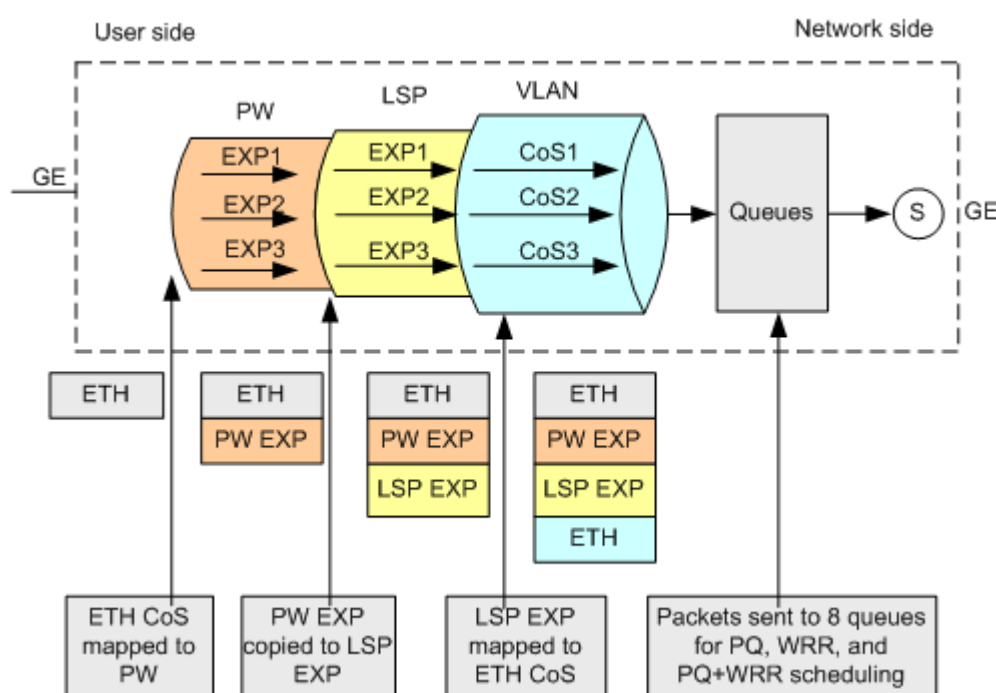
Figure 9-16 Processing flow of ETH PWE3 service



QoS Processing Flow of ETH PWE3 Service

Figure 9-17 shows the QoS processing flow of ETH PWE3 service (MPLS over MPLS encapsulation).

Figure 9-17 QoS processing flow of upstream ETH PWE3 service (MPLS over MPLS encapsulation)



9.1.3.4 Traffic Label Principle

Context

As services are developing, service traffic over a PW becomes heavier and heavier. For example, in the case of the wholesale service, certain carriers encapsulate all service traffic on hundreds or thousands of ports into a PW, and as a result traffic over the PW reaches the gigabit level. As such, a PW carrying heavy traffic is

called fat PW. The fat PW burdens the equipment that it traverses, and results in congestion, packet loss, and unguaranteed QoS.

To solve problems incurred by the fat PW, IETF proposed a traffic label solution: Traffic over a fat PW takes different paths from the PW ingress PE to the PW egress PE within the network through load balancing (ECMP). To achieve PWE3 load balancing, PW data at the PW ingress PE is segmented into bundles of data streams and an MPLS label (traffic label) is allocated to every data stream. In this way, every traffic label identifies a different data stream and the traffic label is stored in the innermost area of the ingress PE label stack. Later, data is forwarded in the load balancing mode according to the traffic label, taking different data streams along different paths within the network.

In terms of PW load balancing, data over a PW arrives at the destination along different paths and this may incur disordered packets. Given this, this technology is applicable to only those services that are not sensitive to disordered packets, such as the Ethernet service. For the ATM and TDM emulation services, this technology is not applied because they have strict requirements on timing and order of packets.

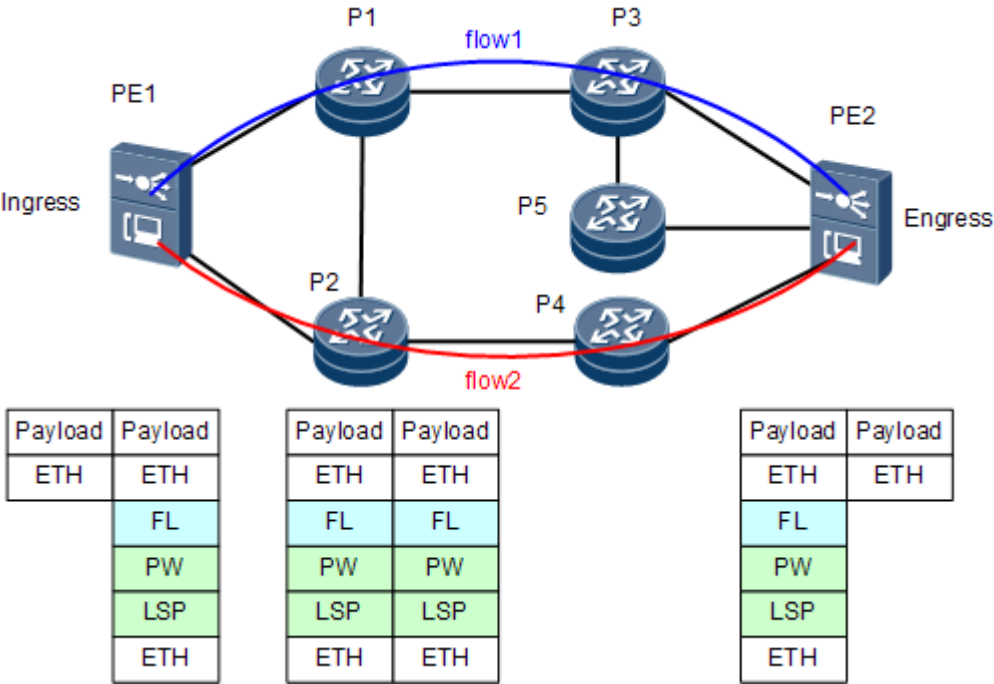
PW load balancing is implemented based on equal cost LSP that is based on the equal cost route.

Application Description

Figure 9-18 shows an application over an existing network where a large amount of the legacy equipment does not support the traffic label. In this application, the PE supports generating the traffic label and performing load balancing but the P has no traffic label capability (for example, the legacy equipment over the network).

- PE1 generates traffic label (FL) and at the same time performs load balancing (flow1 and flow2). PE2 removes the FL.
- P1, P2, and P3 do not support traffic label for load balancing and they only forward data like a common P.

Figure 9-18 Traffic label application (P equipment does not support traffic label for load balancing)



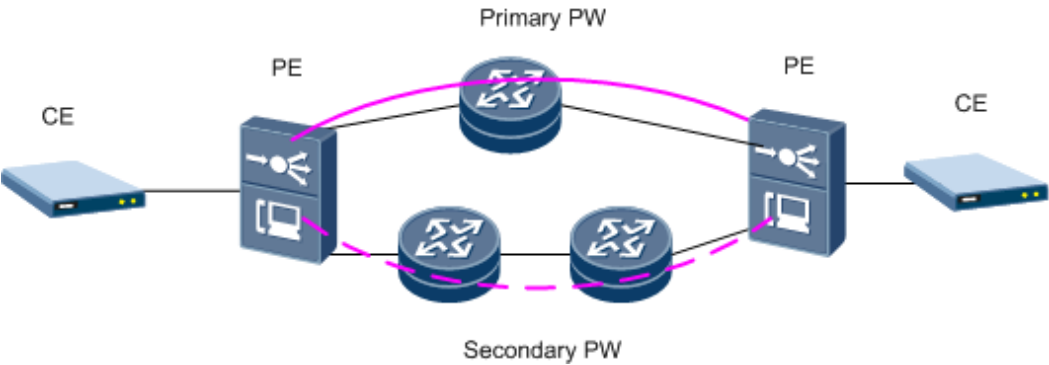
9.1.3.5 PW 1:1 Redundancy

PW redundancy is used for the PW protection switching, which has a similar function as the MPLS OAM. Different from the MPLS OAM (protecting the outer tunnel), PW redundancy protects the inner tunnel.

Through PW redundancy, data is switched to the standby PW if the active PW is faulty (such as the LDP session is down, the tunnel is deleted, the protocol communication is faulty, the route status is changed, or there is no VCCV response). In this case, the original standby PW becomes the active PW.

Figure 9-19 shows the MA5800 supports the following PW 1:1 redundancy applications.

Figure 9-19 PW 1:1 redundancy applications



9.1.3.6 PW Redundancy

PW Redundancy Signaling Mechanism

Introduction of the PW protection mechanism will break the original model of 1-to-1 mapping between AC and PW in PWE3. To keep the original forwarding action, you must ensure that only one PW in the redundancy PW group is in the active state and other PWs are in the standby state.

The LDP PW signaling (RFC4447) requires to use PW status TLV to transfer the PW forwarding status. PW status TLV can be carried by the label mapping message or notification message. PW status TLV is a 32-bit status code and each bit identifies a PW forwarding state. Based on this status code, PW redundancy introduces a new PW status code (0x00000020 - PW forwarding standby) to indicate that the PW is in the standby state currently.

Primary/Secondary and Active/Inactive

There are two couples of important concepts in PW redundancy and the detailed descriptions are as follows:

- Primary/Secondary refers to the PW forwarding priority and is the PW configuration parameter.

The primary PW is preferentially used to forward traffic and the secondary PW is used to protect primary PW. The primary PW is used to forward traffic when the state of the primary and secondary PWs is the same. Currently, only one secondary PW can be configured for each primary PW.

- Active/Inactive refers to the PW forwarding status. It indicates the PW running status and is not the configuration parameter.

Only the PW in the active state can be used to forward traffic. The local active or inactive state of a PW is determined by the local and remote signaling status and priority (configured primary/secondary) of the PW. Only the PW in the optimal state and with the highest priority can be selected as the active PW to forward traffic, and all other PWs are in the inactive state. PWs in the inactive state are not used to forward traffic but can be enabled to receive traffic (can be used only for VLL PW).

PW Redundancy Working Mode

The PW redundancy working mode is specified on PE that is configured with active and standby PWs.

Master/Slave mode:

In this mode, the local end determines the active or standby state of the PW and uses the signaling protocol to notify the remote end; the remote PE can sense the active or standby state. The active/standby relationship on the PW side and the active/standby relationship on the AC side do not affect each other. Therefore, faults can be isolated between the PW side and the AC side. The MA5800 currently can function as a master in this mode.

Independent mode:

In this mode, the active or standby state of the local PW is determined by the negotiation result of the remote AC side; the remote end notifies the local end of the active or standby state. The protection switching due to faults on the AC side will cause the protection switching on the PW side. Therefore, faults cannot be isolated.

9.1.3.7 PW OAM (VCCV)

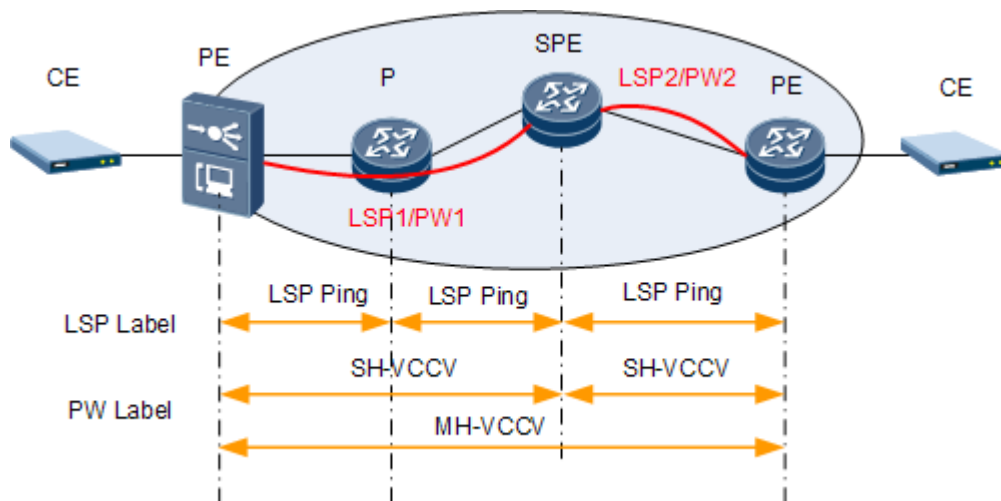
VCCV Ping Application

Virtual Circuit connectivity verification (VCCV) is an end-to-end mechanism to detect and diagnose PW faults. To put it simply, VCCV is a control channel for transmitting connectivity verification messages between PW ingress and PW egress.

VCCV ping is a tool for manually detecting the connectivity status of virtual circuits. It is implemented through extending LSP ping. VCCV defines a series of messages exchanged among PEs to verify PW connectivity. To ensure that the VCCV packet traverses the same path as the data packet in the PW, the VCCV packet must be encapsulated in the same encapsulation mode as the PW and must traverse the same tunnel as the PW packet.

VCCV ping can be used on the U-PE to detect PW connectivity, including detecting the connectivity of the static PW, dynamic PW, single-hop PW, and multi-hop PW. The MA5800 supports single-hop-VCCV (SH-VCCV) ping and does not support multi-hop-VCCV (MH-VCCV) ping temporarily. [Figure 9-20](#) shows the VCCV ping application.

Figure 9-20 VCCV ping application



Principle

VCCV ping is implemented through the VCCV packet and the LSP ping packet therein carries the target FEC stack. [Figure 9-21](#) describes the parameters of the VCCV packet.

Figure 9-21 VCCV packet parameters

0x0c	0x04	CC types	CV types
------	------	----------	----------

- CC Types indicates the control channel type. [Figure 9-22](#) describes the CC for the VCCV function, which is defined in RFC5085.

Figure 9-22 CC in the VCCV packet

MPLS Control Channel (CC) Types:

Bit (Value)	Description
=====	=====
Bit 0 (0x01)	- Type 1: PWE3 Control Word with 0001b as first nibble (PW-ACH, see [RFC4385])
Bit 1 (0x02)	- Type 2: MPLS Router Alert Label
Bit 2 (0x04)	- Type 3: MPLS PW Label with TTL == 1
Bit 3 (0x08)	- Reserved
Bit 4 (0x10)	- Reserved
Bit 5 (0x20)	- Reserved
Bit 6 (0x40)	- Reserved
Bit 7 (0x80)	- Reserved

- Type1: control word channel. Whether VCCV is performed depends on the control word (0001 or not). SH-VCCV and MH-VCCV are supported. If the PE supports control word, CC type1 is used preferentially.
- Type2: MPLS router alert channel. Whether VCCV is performed depends on a specific label value (label = 2). SH-VCCV is supported and MH-VCCV is not supported.
- Type3: maximum-hop channel. VCCV is performed if the TTL value of the inner label of MPLS is 1. SH-VCCV and MH-VCCV are supported.
- CV Types indicates the connectivity verification type. [Figure 9-23](#) describes the CV for the VCCV function, which is defined in RFC5085. The MA5800 supports only CV of the LSP ping type.

Figure 9-23 CV in the VCCV packet

MPLS Connectivity Verification (CV) Types:

Bit (Value)	Description
=====	=====
Bit 0 (0x01)	- ICMP Ping
Bit 1 (0x02)	- LSP Ping
Bit 2 (0x04)	- Reserved
Bit 3 (0x08)	- Reserved
Bit 4 (0x10)	- Reserved
Bit 5 (0x20)	- Reserved

T-PE peers at both sides negotiate CC and CV capabilities during PW set-up, and then send the same CC and CV types used by VCCV ping as the negotiation result. If the PE supports control word, CC type1 is used preferentially. SH-VCCV and MH-VCCV are implemented through setting different inner PW label TTL values.

[Figure 9-24](#) shows the CC Type1 VCCV flow.

Figure 9-24 CC Type1 MH-VCCV/SH-VCCV flow

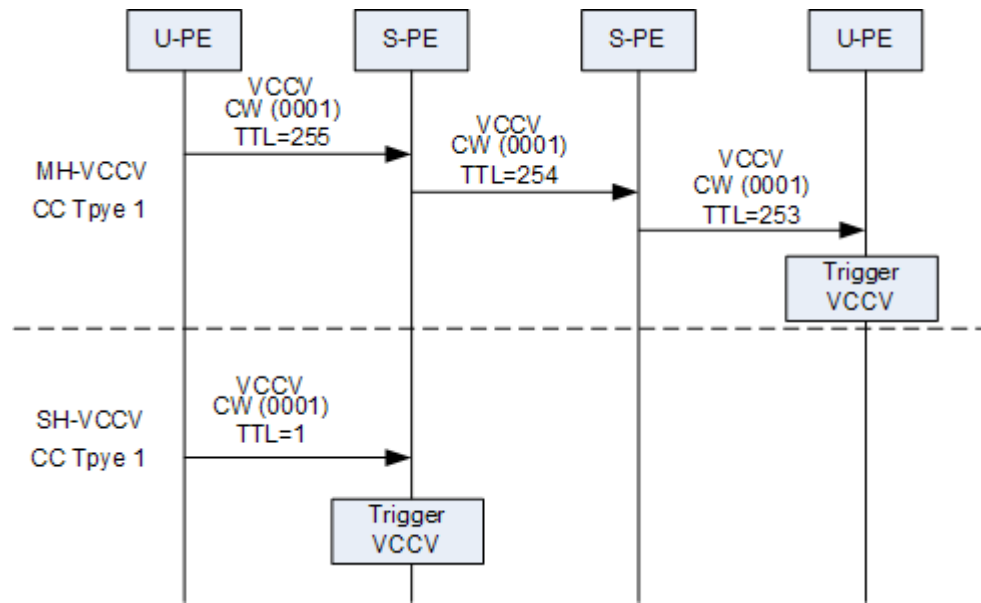
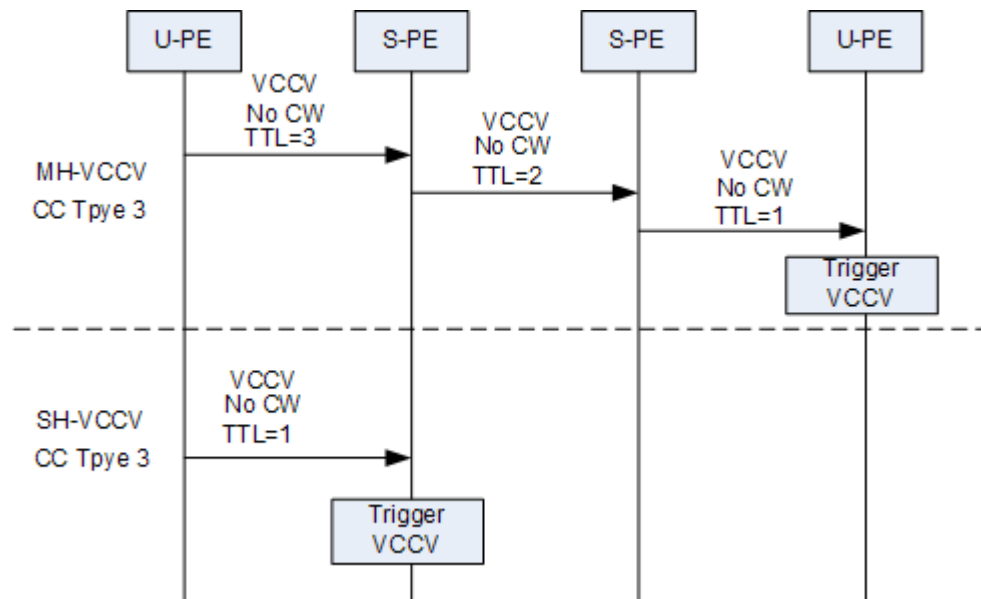


Figure 9-25 shows the CC Type3 VCCV flow.

Figure 9-25 CC Type3 MH-VCCV/SH-VCCV flow



The U-PE and S-PE differ in processing the VCCV packet:

- The S-PE pays attention to only the PW TTL value. If the PW TTL value is 1, VCCV is performed.
- The U-PE pays attention to not only CW (VCCV is performed if the first half-byte is 0001) but the PW TTL value (VCCV is performed if the PW TTL value is 1).
- If the U-PE initiates VCCV to the S-PE, a proper TTL value needs to be set, irrespective of whether CW is used.

9.1.4 PWE3 Network Applications

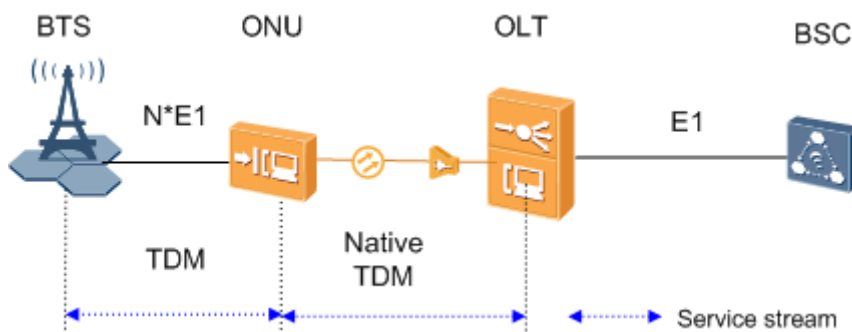
Network Applications of TDM PWE3

For details on the corresponding clock solution of the TDM service, see [14.3 Physical Layer Clock/Time Synchronization](#).

- Network application: converting the native TDM service into the E1 service for upstream transmission

As shown in [Figure 9-26](#), the mobile 2G base station is connected to the ONU through TDM E1. The ONU encapsulates the TDM frame into the GPON GEM frame directly to transmit TDM service over the GPON network (native TDM). The OLT terminates the TDM PWE3 signals and transmits the signals to the upstream network through the E1 port.

Figure 9-26 Network application: converting the TDM PWE3 service into the E1 service for upstream transmission

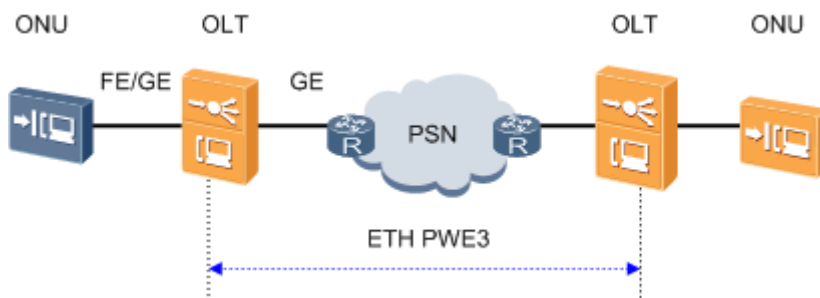


Network Applications of ETH PWE3

- Network application: implementing PWE3 private line upstream transmission in FE/GE access

As shown in [Figure 9-27](#), the enterprise router is connected to the OLT through FE/GE. The OLT interconnects with the peer ETH PWE3 device of the enterprise through the ETH PWE3 private line to implement the ETH private line service.

Figure 9-27 Network application: implementing PWE3 private line upstream transmission in FE/GE access



9.1.5 Configuring the PWE3 Private Line Service

Pseudo wire emulation edge-to-edge (PWE3) uses LDP or RSVP-TE as the signaling protocol and carries various Layer 2 services of the customer edge (CE) over the MPLS LSP or TE tunnel, transparently transmitting the Layer 2 data of the CE.

PWE3 Service Model

According to the PWE3 service model, PWE3 is indicated by the outer packet switch network (PSN) tunnel label and the inner label (PW demultiplexer).

Network Application

Figure 9-28 shows the network application of the MPLS PWE3.

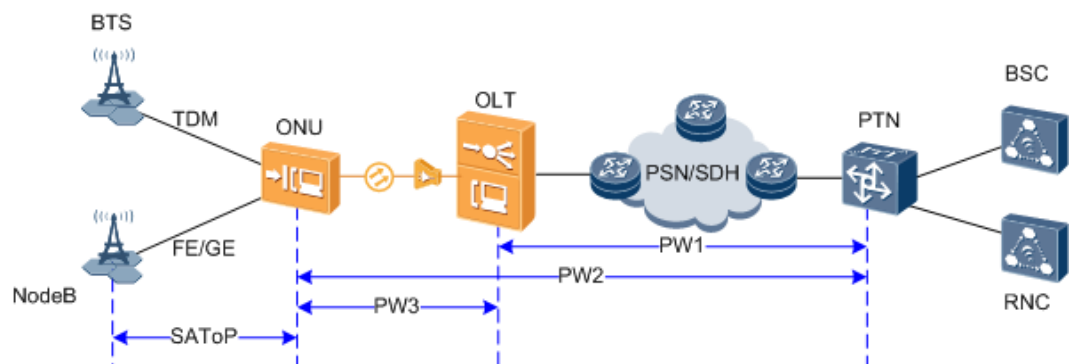
As shown in the figure, the mainstream applications of the MPLS PWE3 supported by the MA5800 are as follows:

- TDM PWE3: A mobile 2G base station is connected to the ONU through the TDM E1 port. The ONU implements the TDM PWE3, transmitting traffic streams to the peer TDM PWE3 device through the PSN. The MA5800 functions as a Layer 2 transparent transmission device, PE device, or P device.
- ETH PWE3: A 3G base station is connected to the ONU through the FE/GE port. The ONU performs the ETH PWE3 encapsulation for interconnecting with the peer ETH PWE3 device. The MA5800 functions as a Layer 2 transparent transmission device or P device.

NOTE

- The MA5800 can function as a Layer 2 transparent transmission device or PE/P device, determined by the service requirement.
- As shown in the following figure, in PW1 and PW3, the MA5800 functions as a PE device that initiates or terminates the PW; in PW2, the MA5800 functions as a Layer 2 transparent transmission device or P device.

Figure 9-28 MPLS PWE3 network application when the MA5800 functions as a Layer 2 transparent transmission device, PE device, or P device



Procedure

According to the PWE3 service model, PWE3 configurations include the outer tunnel configuration, inner PW configuration, and tunnel protection. Therefore, the configuration procedure is as follows.

9.1.5.1 Configuring the PWE3 Outer Tunnel

To provide services across the PSN network, the MA5800 supports PW over the MPLS tunnel to transparently transmit services in the PSN network.

Prerequisites

1. The loopback interface IP address must be configured.
2. The LSR ID must be configured.
3. The global MPLS and MPLS TE functions must be enabled.
4. The host route of each port must be successfully advertised on each device in the network (For example, the OSPF protocol was configured).

Context

Only the MPLS LSP is supported as PWE3 outer tunnel currently.

Procedure

- Configure the MPLS TE tunnel.
 - a. In the global config mode, run the **interface tunnel** command to create a tunnel interface and enter the tunnel interface mode.
 - b. Run the **tunnel-protocol mpls te** command to configure the tunnel protocol to MPLS TE, that is, configure the tunnel interface to work in the TE tunnel mode.
 - c. Run the **destination ip-address** command to configure the destination IP address of the tunnel. Generally, the LSR ID of the ingress is used.
 - d. Run the **mpls te tunnel-id** command to configure the tunnel ID.
 - e. Run the **mpls te signal-protocol { cr-static | rsvp-te }** command to configure the signaling protocol for the MPLS TE tunnel.

According to whether the MPLS TE tunnel uses the dynamic signaling protocol, the tunnel is categorized as create te tunnel based on static cr-lsp and MPLS RSVP-TE tunnel.

- Create te tunnel based on static cr-lsp : The forwarding information and resource information are configured manually, and the signaling protocol and path calculation are not involved. Because the MPLS-related control packets are not exchanged, fewer resources are used. The static tunnel, however, cannot be dynamically adjusted according to network changes. Therefore, the actual application is limited.
- MPLS RSVP-TE tunnel: MPLS TE creates the LSP tunnel along a specified path through RSVP-TE and reserves resources. Thus, carriers can accurately control the path that traffic traverses to avoid the node where congestion occurs. This solves the problem that certain

paths are overloaded and other paths are idle, utilizing the current bandwidth resources sufficiently.

- f. (Optional) Run the **mpls te bandwidth** command to configure the bandwidth for the tunnel. After the configuration is completed, only the VLAN interface meeting this bandwidth requirement is selected as the node traversed by an MPLS TE tunnel when the MPLS TE tunnel is created.

If the MPLS TE tunnel is only used to change the data transmission path, you may not configure the bandwidth of the tunnel.

- g. (Optional) Run the **mpls te path explicit-path** command to configure the explicit path used by the MPLS TE tunnel.

To limit only the bandwidth of the MPLS TE tunnel but not the transmission path, you may not configure the explicit path of the tunnel.

- h. Run the **display interface tunnel** command to query the configuration of the tunnel.

- For the configuration of LDP LSP, see [6.7.2 Configuring the LDP LSP](#).

----End

9.1.5.2 Configuring the Tunnel Policy

Configure the tunnel selection sequence for load balancing or the tunnel binding policy in the tunnel. After the configuration is successful, packets in the tunnel are processed according to tunnel policy.

Prerequisites

The PWE3 outer tunnel must be created.

Context

The tunnel selection sequence and the tunnel binding policy are mutually exclusive. This means that you can configure only one of them.

- The IP tunnel supports the configuration of only the tunnel selection sequence.
- The MPLS TE tunnel supports the configuration of only the tunnel binding policy.

Procedure

Step 1 Run the **tunnel-policy** command to create a tunnel policy name and enter the tunnel policy mode.

Step 2 For IP tunnel, run the **tunnel select-seq** command to configure the selection sequence of tunnels for load balancing.

To configure different tunnel types for load balancing according to priorities, run this command. The more the tunnel type close to keyword **select-seq**, the higher priority for load balancing.

The MA5800 does not support load balancing between different tunnels. In other words, tunnels for load balancing must be of the same type. The tunnels are selected according to the tunnel configuration.

Step 3 For MPLS TE tunnel, run the **tunnel binding** command to configure the tunnel binding policy.

To bind to a specified tunnel ID and configure the system to switch another tunnel according to the configured sequence when a tunnel is not available, run this command. After the tunnel binding policy is configured, run the **mpls te reserved-for-binding** command in the tunnel mode to allow the MPLS TE tunnel to be bound to the VPN instance.

destination *ip-addr* indicates the destination IP address of the tunnel, which must be the same as the destination IP address configured in the MPLS TE tunnel.

Step 4 In the global config mode, run the **display tunnel-policy** command to query the information about the tunnel policy.

----End

Example

To configure a tunnel policy named *te_policy* and bind to tunnels with the destination IP address 10.5.5.5 and IDs 10 and 20, do as follows:

```
huawei(config)#tunnel-policy te_policy
Info: New tunnel-policy is configured.
huawei(config-tunnel-policy-te_policy)#tunnel binding destination 10.5.5.5 te tunnel
10 tunnel 20
huawei(config)#display tunnel-policy
{ <cr>|string<S><Length 1-19> }:
```

Command:

display tunnel-policy

```
Total tunnel policy num:      1
Sel-Seq tunnel policy num:     0
Binding tunnel policy num:     1
Invalid tunnel policy num:     0
```

Tunnel Policy Name	Destination	Tunnel Intf	Down switch
te_policy	10.5.5.5	tunnel10	Disable
		tunnel20	

9.1.5.3 Configuring the PWE3 Inner PW

Configure the attribute of PW and use the PW parameters for PW binding.

Prerequisites

- MPLS L2VPN must be enabled.
- The outer tunnel must be configured.

Context

PW parameters include the following parameters: control word, jitter buffer (only for TDM PWs), maximum transmission unit (MTU), loopback IP address of the peer device, PW type, RTP control header, virtual circuit connectivity verification (VCCV), used tunnel policy, flow label classification, and TDM load time (only for TDM PWs). Different services have different configurations when the services are bound to a PW.

Procedure

Step 1 Run the **pw-para** command to create PW parameter.

PW parameters and the PW have a one-to-one mapping. One PW parameter can be used by only one PW.

Step 2 Run the **peer-address** command to configure the IP address of the peer device.

peer-address indicates the peer IP address in the PW for creating communication. In the actual transmission, data packets are automatically transmitted to the peer device according to this IP address.

Step 3 Run the **pw-type** command to configure the PW type.

The MA5800 supports TDM and ETH PWs.

ETH PWs are categorized as raw and tagged modes.

- Raw mode: The PW VLAN tag is not carried in the upstream direction, but the PW payload can carry the SVLAN.
- Tagged mode: The payload of an upstream packet carries the PW VLAN tag, and the PW VLAN tag is removed in the downstream direction.

For the same PW, the PW types at both ends must be the same. In this way, the PW can be available.

NOTICE

Among PW parameters, the IP address and PW type of the peer device cannot be changed after they are configured. To change these two parameters, run the **undo pw-para** command to delete them first, and then configure them again. Make sure that the two parameters are correctly configured the first time, so as to prevent repeated operations.

Step 4 (Optional) Run the **control-word** command to enable the control word mode.

When VCCV ping works in the control word mode, you need to enable the control word. It is recommended that you enable the control word mode.

Step 5 (Optional) Run the **jitter-buffer** command to configure the jitter buffer.

The jitter buffer can effectively prevent jitter and delay. By default, the jitter buffer size is 2000 μ s.

NOTE

- Only a TDM PW supports setting of the jitter buffer size.
- The jitter buffer size must be an integer multiple of 125.

Step 6 (Optional) Run the **mtu** command to configure the MTU.

Due to the limit in the system, the configurable MTU ranges for different PW types are different:

- MTU values set on the two devices at the ends of an ETH PW must be the same. If MTU values are different, an ETH PW can never be available.
- By default, the MTU is 1500 bytes. Do not modify this value unless there is a special requirement.

Step 7 Run the **rtp-header** command to configure the RTP control header.

 NOTE

This command is applicable to only TDM PWs.

The length of the RTP header is 12 bytes, including the version number, padding flag, and timestamp fields. The timestamp field, whose length is 32 bits, is used for clock synchronization. For format of the RTP header, see RFC3550.

After RTP is enabled, PW packets of the TDM type carry the RTP control header. Otherwise, the RTP control header is not carried.

The RTP configuration must be the same as that on the peer PW device. By default, the MA5800 disables the RTP control header.

Step 8 (Optional) Run the **vccv** command to enable VCCV, so as to notify the peer device of the VCCV types supported by the local device. After a successful negotiation between both devices, a virtual circuit connectivity verification is performed by using LSP ping according to the priority of the VCCV type.

VCCV is an end-to-end PW fault detection and diagnosis mechanism. Simply, VCCV is a control channel for the PW to send verification messages between the ingress and egress.

Enable the LSP ping function for alter, CW, and TTL channels or any of the three channels according to the VCCV types supported by the system. By default, VCCV is disabled.

Step 9 (Optional) Run the **tdm-load-time** command to configure the TDM load time.

 NOTE

Only a TDM PW supports the setting of the load time.

Because each TDM frame is 125 μ s, the load time must be an integer multiple of 125. If the entered number is not an integer multiple of 125, the system rounds it down to the nearest integer multiple of 125 μ s. The jitter buffer must be greater than the load time.

The default jitter buffer is 1000 μ s. Do not modify this value unless there is a special requirement.

Step 10 (Optional) Run the **tnl-policy** command to configure the tunnel policy used by the PW.

 NOTE

The tunnel policy and the PW flow label classification are mutually exclusive. Configure either of them.

After the tunnel policy used by the PW is configured, the PW can perform load balancing or path selection according to the tunnel policy.

Step 11 In the privilege mode or global config mode, run the **display pw-para** command to query the configuration of the PW.

----End

Example

To configure PW 10 with the following attributes, do as follows:

- IP address of the peer PW device: 10.10.10.20
- PW type: TDM CESOPSN
- Name of the tunnel policy used by the PW: **tdm-policy**
- Enable the RTP control header and the control word mode
- Enable the connectivity verification function of the alter, CW and TTL channels
- Other parameters: default settings

```
huawei(config)#pw-para pwindex 10
huawei(config-pw-para-index-10)#service-type vll
huawei(config-pw-para-index-10)#pwid 10
huawei(config-pw-para-index-10)#peer-address 10.10.10.20
huawei(config-pw-para-index-10)#pw-type tdm cesopsn
huawei(config-pw-para-index-10)#tnl-policy tdm-policy
huawei(config-pw-para-index-10)#rtp-header
huawei(config-pw-para-index-10)#control-word
huawei(config-pw-para-index-10)#vccv cc cw alert ttl cv lsp-ping
huawei(config-pw-para-index-10)#quit
huawei(config)#display pw-para pwindex 10
PW index      : 10
Service type  : VLL
PW ID         : 10
PeerIP        : 10.10.10.20
Tnl Policy Name : --
PW Type       : tdm satop e1
Remove Double Tag : --
Tag Mode      : --
Cos Group ID   : --
Pbits-to-pbits ID : --
CtrlWord       : enable
VCCV capability : cw alert ttl/lsp-ping
BFD compatibility : disable
MTU            : 1500
Statistic switch : disable
Dynamic in label : --
MaxAtmCells    : --
MaxEncapDelay  : --
RTP            : enable
PayloadType     : 0
SnStartNum     : 0
RcvSsrcId      : 0
TxSsrcId       : 0
JitterBuffer   : 2000
LoadTime(us)   : 1000
TimeSlotNum    : 32
PayLoadSize(bytes): 256
FlowLabel transmit : --
FlowLabel classification-rule : --
FlowLabel receive : --
Priority mapping profile name : default-profile-2
```

To configure PW 20 with the following attributes, do as follows:

- IP address of the peer PW device: 10.20.30.40
- PW type: ETH Tagged
- Name of the tunnel policy used by the PW: **eth-policy**
- Other parameters: default settings

```
huawei(config)#pw-para pwindex 20
huawei(config-pw-para-index-20)#service-type vll
huawei(config-pw-para-index-20)#pwid 20
huawei(config-pw-para-index-20)#peer-address 10.20.30.40
huawei(config-pw-para-index-20)#pw-type ethernet tagged
```

```
huawei(config-pw-para-index-20)#tnl-policy eth-policy
huawei(config-pw-para-index-20)#quit
huawei(config)#display pw-para pwindex 20
PW index          : 20
Service type      : VLL
PW ID             : 20
PeerIP            : 10.20.30.40
Tnl Policy Name   : --
PW Type           : ethernet tagged
Remove Double Tag : --
Tag Mode          : --
Cos Group ID      : 0
Pbits-to-pbits ID : --
CtrlWord          : disable
VCCV capability   : disable
BFD compatibility : disable
MTU               : 1500
Statistic switch  : disable
Dynamic in label  : --
MaxAtmCells       : --
MaxEncapDelay     : --
RTP               : --
PayloadType       : --
SnStartNum        : --
RcvSrcId          : --
TxSrcId           : --
JitterBuffer      : --
LoadTime(us)      : --
TimeSlotNum       : --
PayLoadSize(bytes): --
FlowLabel transmit : disable
FlowLabel classification-rule : --
FlowLabel receive  : disable
Priority mapping profile name : default-profile-0
```

9.1.5.4 Binding the Service to the PW

Bind various PWE3 services to a PW. After the binding, user packets are encapsulated and forwarded according to the modes defined in the PW parameters.

Prerequisites

- The PW must be configured.
- For TDM PWE3, the TDM connection must be created.
- For ETH PWE3, the ETH-based service port must be created.

Context

Only the dynamic PW is supported currently.

Dynamic PW is negotiated using the LDP protocol.

Procedure

- Bind the TDM service to a PW.
Run the **pw-ac-binding tdm** command to use a PW to create the TDM PW service.
Pay attention to the following points during the configuration:
 - To specify a PW as a static PW, you need to configure the in label and out label of the PW. The out label value must be an unallocated and idle

value at the peer end and the in label value must be an unallocated value at the local end.

- Bind the ETH service to a PW.

Run the **pw-ac-binding vlan** command to use a PW to create the ETH PW service.

----End

Example

To create a dynamic binding between TDM connection 0 and PW 20, do as follows:

```
huawei(config)#pw-ac-binding tdm 0 pw pwindex 20
```

To bind the ETH service to a PW with the following settings, do as follows.
Settings: VLAN ID 100, PW ID 30.

```
huawei(config)#pw-ac-binding vlan 100 pw pwindex 30
```

9.1.5.5 Configuring PW Protection

Create a standby PW for a PW. When the active PW is faulty, the system quickly switches to the standby PW to ensure the service reliability.

Prerequisites

- The active PW must be created.
- The basic parameters of secondary PW are configured. For the configuration method, see [9.1.5.3 Configuring the PWE3 Inner PW](#).

Context

PW protection: When a PW is faulty (such as an LDP session is down, a tunnel is deleted, the protocol communication is faulty, the route status changes, or VCCV has no response), the system can quickly switch to the standby PW. Then, the standby PW functions as the active PW.

The MA5800 supports PW 1:1 redundancy.

Procedure

Step 1 Run the **pw-protect** command to configure the standby PW.

Pay attention to the following points during the configuration:

- The standby PW ID cannot exist.
- The PW parameters of the active and standby PWs must be the same.
- Both active PW and the standby PW are not static PW.

Step 2 (Optional) Enable the PW protection group to support dual-sending and dual-receiving for the multicast service.

When the PW protection group supports dual-sending, both active and standby PWs can forward IGMP packets so that the multicast forwarding entry can also be created on the device corresponding to the standby PW. After the active/standby

PW switchover, the multicast service can be smoothly switched. This configuration is recommended when the multicast service is carried by the active and standby PWs.

When the PW protection group supports dual-receiving, both active and standby PWs can receive packets to avoid packet loss caused by signaling delay when switchback is performed after the faulty active PW recovers. This configuration is recommended when the multicast service is carried by the active and standby PWs.

1. Run the **igmp_send_dual-pw** command to set whether IGMP packets can be sent by both active and standby PWs.
2. Run the **pw-redundancy_stream-dual-receiving** command to set the PW protection group to work in the dual-receiving mode.

Step 3 Run the **pw-revertive-mode** command to configure the switchback policy for the PW protection group.

Switchback: When both active and standby PWs are available, if the original service traffic is carried on the standby PW, the service can be switched back to the active PW according to actual requirements. Set the switchback policy according to actual network conditions (such as whether the network topology often changes and whether the traffic should be carried on the active PW).

The switchback policy of a PW protection group can be immediate automatic switchback, automatic switchback after a period of time, and no automatic switchback.

Step 4 Run the **display pw-ps** command to query the configuration of the PW protection group.

----End

Example

To configure a PW protection group, set the parameters as follows: active PW ID to 10, standby PW ID to 20, and switchback policy to allowing automatic switchback for the PW protection group in 30 seconds.

```
huawei(config)#pw-protect primary-pw pwindex 10 secondary-pw pwindex 20
huawei(config)#pw-revertive-mode pwindex 10 revertive wtr 30
huawei(config)#display pw-ps pwindex 10
```

Primary-PW-Index	Primary-PW-state	Secondary-PW-Index	Secondary-PW-state
10	down	20	down

stream-dual-receiving: disable
pw-redundancy mode: master
pw-redundancy switchover config: primary
revertive-mode: revertive, in 30 seconds

9.1.5.6 Configuring MPLS Tunnel Protection

Create a protection tunnel for the MPLS TE tunnel. When the working tunnel is faulty, the system quickly switches to the protection tunnel to ensure the service reliability.

Prerequisites

- The forward LSP must be created.
- The backward LSP must be created.
- MPLS OAM must be enabled.

Context

MPLS tunnel protection is a part of the MPLS OAM connectivity detection mechanism.

The basic process of the MPLS OAM connectivity check and protection switching is as follows:

1. The source transmits the CV/FFD packets to the destination through the detected LSP.
2. The destination checks the correctness of the type and frequency carried in the received detection packets and measures the number of correct and incorrect packets that are received within the detection period to monitor the connectivity of the LSP in real time.
3. After detecting a defect, the destination transmits the BDI packets that carry the defect information to the source through the backward path.
4. The source learns about the status of the defect, and triggers the corresponding protection switching when the protect group is correctly configured.

Procedure

Step 1 Configure working MPLS TE tunnel.

1. In the global config mode, run the **interface tunnel** command to create a tunnel interface and enter the tunnel interface mode.
2. Run the **tunnel-protocol mpls te** command to configure the tunnel protocol to MPLS TE.
3. Run the **destination ip-address** command to configure the destination IP address of the tunnel. Generally, the egress LSR ID is used.
4. Run the **mpls te tunnel-id** command to configure the tunnel ID.
5. Run the **mpls te signal-protocol rsdp-te** command to configure the signaling protocol of the tunnel to RSVP-TE.
6. (Optional) Run the **mpls te bandwidth** command to configure the bandwidth for the tunnel. After the configuration is completed, only the VLAN interface that meets this bandwidth value can be selected as the node traversed by the MPLS TE tunnel path when the MPLS TE tunnel is created.

If the MPLS TE tunnel is only used to change the data transmission path, you may not configure the tunnel bandwidth.

7. (Optional) Run the **mpls te path explicit-path** command to configure the explicit path used by the MPLS TE tunnel.

If only the bandwidth used by the MPLS TE tunnel is limited but the transmission path is not limited, you may not configure the explicit path used by the MPLS TE tunnel.

Step 2 Configure protection MPLS TE tunnel.

The working mode of MPLS OAM protection switching is 1:1 protection. Normally, each working tunnel has a protection tunnel.

The configuration of the protection tunnel is the same as that of the working tunnel.

Step 3 Configure a tunnel protect group.

Configure the working tunnel and the protection tunnel as a tunnel protect group. When the source end finds the active LSP is defective through the MPLS OAM detection mechanism, and the protection switching is required, the system can switch the data to the protection tunnel for continuous transmission.

1. In the global config mode, run the **interface tunnel** command to enter the working tunnel interface mode.
2. Run the **mpls te protection tunnel** command to create a tunnel protect group and set the switchback mode of the protect group.

The switchback policy of a PW protection group can be immediate automatic switchback, automatic switchback after a period of time, and no automatic switchback.

Step 4 (Optional) Run the **mpls te protect-switch** command forcibly switch over the tunnel protect group.

To manually switch data streams between working and protection tunnels, run this command.

There are for forcible switching modes:

- **clear**: clears all external switching commands that are already executed in the system.
- **lock**: lock switching, which locks data streams on the working tunnel.
- **force**: forcible switching, which forcibly switches data streams to the protect tunnel.
- **manual work-lsp**: manually switches data streams on the working tunnel to the protection tunnel.
- **manual protect-lsp**: manually switches data streams on the protection tunnel to the working tunnel.

Keywords **clear**, **lock**, **force**, and **manual** corresponds to switching priorities in descending order. If a command with a higher priority is executed, a command with a lower priority cannot be executed.

Step 5 In the global config mode, run the **display mpls te protection tunnel** command to query the configuration of the tunnel protect group.

----End

Example

To configure RSVP-TE tunnel IDs to 10 and 30, destination IP address of the tunnels to 10.3.3.3, tunnel 30 as the protection tunnel of tunnel 10, switchback mode to revertive, and WTR time to 900s, do as follows:

```
huawei(config)#interface tunnel 10
huawei(config-if-tunnel10)#tunnel-protocol mpls te
huawei(config-if-tunnel10)#destination 10.3.3.3
```

```
huawei(config-if-tunnel10)#mpls te tunnel-id 10
huawei(config-if-tunnel10)#mpls te signal-protocol rsvp-te
huawei(config-if-tunnel10)#mpls te bandwidth ct0 5120 //(Optional) Configure the global bandwidth of
tunnel 10 to 5120 kbit/s.
huawei(config-if-tunnel10)#mpls te commit
huawei(config-if-tunnel10)#quit
huawei(config)#interface tunnel 30
huawei(config-if-tunnel30)#tunnel-protocol mpls te
huawei(config-if-tunnel30)#destination 10.3.3.3
huawei(config-if-tunnel30)#mpls te tunnel-id 30
huawei(config-if-tunnel30)#mpls te signal-protocol rsvp-te
huawei(config-if-tunnel30)#mpls te bandwidth ct0 5120 //(Optional) Configure the global bandwidth of
tunnel 30 to 5120 kbit/s.
huawei(config-if-tunnel30)#mpls te commit
huawei(config-if-tunnel30)#quit
huawei(config)#interface tunnel 10
huawei(config-if-tunnel10)#mpls te protection tunnel 30 mode revertive wtr 30
huawei(config-if-tunnel10)#mpls te commit
huawei(config-if-tunnel10)#quit
```

9.1.5.7 Configuring CR-LSP Backup

Backup CR-LSPs are established on networks requiring high reliability to provide end-to-end protection, ensuring network reliability. If a primary CR-LSP fails, traffic rapidly switches to a backup CR-LSP, ensuring uninterrupted traffic transmission.

Prerequisites

Before configuring CR-LSP backup, complete the following tasks:

- Setting up a primary RSVP-TE tunnel
- Enabling MPLS, MPLS TE, and RSVP-TE globally and on interfaces of each node along a backup CR-LSP

Context

Hot standby and ordinary backup modes are supported. If both primary and backup CR-LSPs fail, best-effort paths are established. The following table lists CR-LSP backup modes.

Backup Mode	Description	Advantage	Shortcoming
Hot standby	A hot-standby CR-LSP is set up over a separate path immediately after a primary CR-LSP is set up	A rapid traffic switchover can be performed	Additional bandwidth needs to be reserved for a hot-standby CR-LSP
Ordinary backup	The system attempts to set up an ordinary backup CR-LSP if a primary CR-LSP fails	No additional bandwidth is needed	Ordinary backup performs a traffic switchover slower than hot standby

Backup Mode	Description	Advantage	Shortcoming
Best-effort path	The system establishes a best-effort path over an available path if both the primary and backup CR-LSPs fail	Establishing a best-effort path is easy and a few constraints are needed	Some quality of service (QoS) requirements cannot be met

The following backup modes are supported for CR-LSP.

- Hot standby
- Ordinary backup
- Hot standby + best-effort path

Procedure

Step 1 Configure the backup mode of CR-LSP.

1. Run the **interface tunnel** command to enter MPLS TE tunnel mode.
2. Run the **mpls te backup** command to configure the backup mode of current tunnel.
 - The keyword **hot-standby** indicates the hot standby mode.
 - **ordinary** indicates the ordinary mode.
 - **ordinary best-effort** indicates the best-effort path mode.

Step 2 (Optional) Configure the explicit path for a backup CR-LSP.

After hot standby or ordinary backup is configured, the system automatically selects a path for a backup CR-LSP. To manually specify a path for a backup CR-LSP, you can set explicit path. An explicit path consists of a series of nodes, which constitute a vector path according to the configured sequence. The IP address in an explicit path is the IP address of the interface on the node. Generally, the loopback interface IP address on the egress is used as the destination IP address of the explicit path.

NOTE

Use a separate explicit path for the backup CR-LSP to prevent the backup CR-LSP from completely overlapping its primary CR-LSP. Protection will fail if the backup CR-LSP completely overlaps its primary CR-LSP.

1. Run the **explicit-path** command in the global config mode to create an explicit path.
2. Run the **next hop**, **modify hop**, and **delete hop** command to add a next hop node, modify a node, and delete a node respectively for the explicit path.
3. In the tunnel mode, run the **mpls te path explicit-path path-name secondary** command to specify the explicit path for the backup CR-LSP.

Step 3 (Optional) Configure the affinity property for a backup CR-LSP.

Affinity property masks determine the link properties that should be checked by a device. To ensure that a link can be used by a tunnel, for the bits that are 1 in a mask, it is required that at least one bit in the administrative group and the corresponding bit in the affinity property be 1. In addition, if the bits in the affinity property are 0, the corresponding bits in the administrative group cannot be 1.

The default affinity property is 0x0.

Run the **mpls te affinity property secondary** command to set the affinity property for the backup CR-LSP.

Step 4 (Optional) Configure the hop limit for a backup CR-LSP.

After a CR-LSP is configured with a hop limit, the hop limit acts as one of routing conditions such as the link bandwidth and affinity property when the CR-LSP is created. After the hop limit is set, the number of hops of a CR-LSP cannot exceed this limit.

The default hop limit is 32.

Run the **mpls te hop-limit secondary** command to set hop limit for the backup CR-LSP.

----End

Follow-up Procedure

After the configuration of CR-LSP backup is finished, you can query information about the tunnel interface and backup status.

- Run the **display mpls te tunnel-interface** command to check information about a tunnel interface.
- Run the **display mpls te hot-standby state** command to check information about the hot-standby status.
- Run the **display mpls te tunnel** command to check CR-LSP information.

9.2 Native TDM

In Native TDM, TDM frames are directly encapsulated to GPON GEM frames. This mode features simple encapsulation, small network cost, and guaranteed link quality. TDMoGEM mode and TDMoETH mode are encapsulated to NativeTDM in access network at present, and the MA5800 supports TDMoETH mode.

9.2.1 Introduction to Native TDM

Definition

By using the standard 8 kHz (125μm) frames, the GPON GTC layer is synchronous in nature. Therefore, GPON can support the TDM service. This is called Native TDM.

In Native TDM, TDM frames are encapsulated to ETH frames and then to GPON GEM frames in TDMoETH mode. This mode features simple encapsulation, small network cost, and guaranteed link quality.

Purpose

Currently, the circuit switched network is evolving to the packet switched network. During the deployment of the packet switched network, the method to provide traditional circuit switching service over the packet switched network must be considered. In a GPON network deployment, the traditional TDM service can be delivered over the PSTN network through the Native TDM mode.

9.2.2 Native TDM Reference Standards and Protocols

The following lists the reference documents of Native TDM:

- ITU-T G.984.1 General characteristics for Gigabit-capable Passive Optical Networks (GPON)
- ITU-T G.984.2 Gigabit-capable Passive Optical Networks (GPON): Physical Media Dependent (PMD) layer specification
- ITU-T G.984.3 Gigabit-capable Passive Optical Networks (GPON): Transmission convergence layer
- ITU-T G.984.4 Gigabit-capable Passive Optical Networks (GPON): ONT management and control interface specification

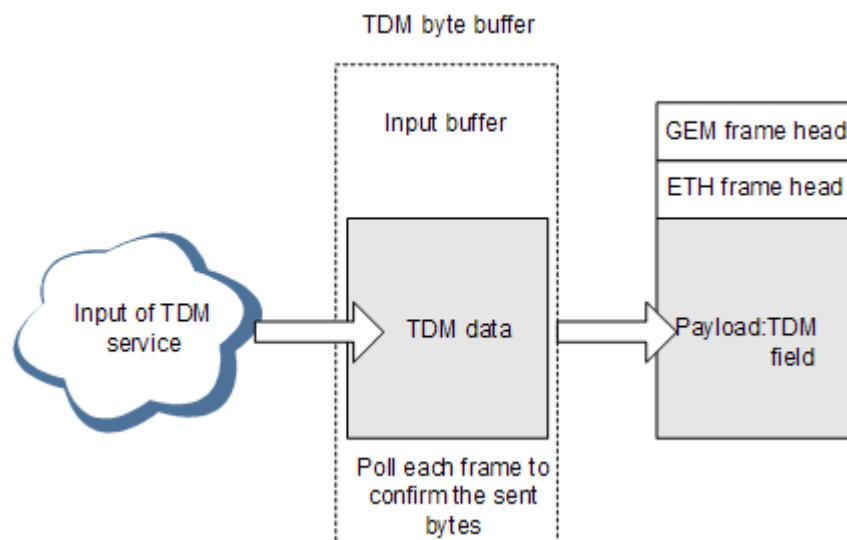
9.2.3 Native TDM Principle

Basic Principle

The MA5800 supports E1 upstream transmission mode. The following section uses E1 upstream transmission as an example.

In the TDMoETH mode, the TDM frame is directly encapsulated to the GPON GEM frame so that the TDM service can be transmitted in a GPON network. [Figure 9-29](#) shows the basic principle of Native TDM.

Figure 9-29 Basic principle of TDMoETH mode Native TDM



The TDMoETH mode does not distinguish whether it is a structured service such as the voice and PBX access services, or an un-structured service such as private line service. All services are handled as un-structured services. GPON access transparently delivers only the E1 service without performing the refined service processing. In other words, GPON access provides the long-haul E1 transmission.

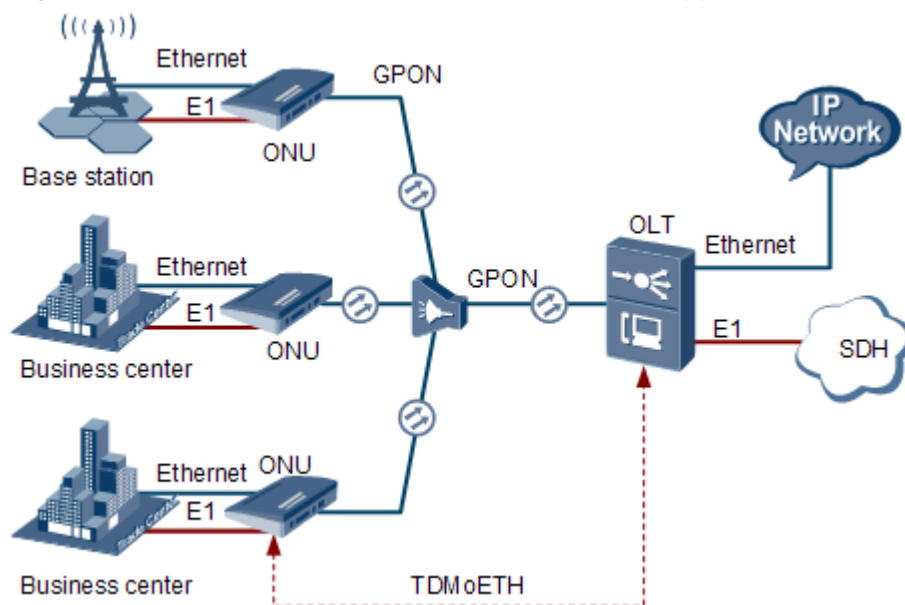
In general, the private line service has an independent clock, which is asynchronous with the GPON line clock. The jitter and frequency difference exist between the two clocks. Therefore, the E1 service traffic can be transmitted only after the E1 rate adjustment occurs at the ONT/ONU.

The bit asynchronous mapping mode of SDH is adopted while the GPON line clock or system clock is used as the reference clock. Through the bit adjustment, the E1 service traffic is mapped to the payload section of the tributary unit to form a standard VC12 virtual channel, which is delivered in the GEM frame. At the receiver end, de-byte adjustment is adopted to recover the original clock and the E1 service traffic.

Application

Figure 9-30 shows the TDMoETH network application. The E1 ports of the ONU/ONT access the TDM traffic from the base stations and enterprises. The ONU/ONT sends both the Ethernet traffic and the TDM traffic to the OLT. The OLT differentiates the Ethernet traffic and the TDM traffic, and sends the traffic to the IP network and the SDH network, respectively.

Figure 9-30 TDMoETH mode Native TDM network application



9.3 VPLS

The Virtual Private LAN Service (VPLS), also called the Transparent LAN Service (TLS) or virtual private switched network service, is a Layer 2 VPN (L2VPN)

technology that is based on Multi-Protocol Label Switching (MPLS) and Ethernet technologies.

9.3.1 What Is VPLS

Definition

The Virtual Private LAN Service (VPLS), also called the Transparent LAN Service (TLS) or virtual private switched network service, is a Layer 2 VPN (L2VPN) technology that is based on Multi-Protocol Label Switching (MPLS) and Ethernet technologies.

Purpose

The primary goal of VPLS is to interconnect multiple Ethernet LANs through the Packet Switched Network (PSN). In this manner, these LANs can function as one LAN. VPLS can implement the multipoint-to-multipoint VPN networking; therefore, by using the VPLS technology, service providers (SPs) can provide the Ethernet-based multipoint services through MPLS backbone networks. In addition, by utilizing the VPLS solution in which MPLS virtual circuits (VCs) function as the Ethernet bridge links, SPs can transparently transmit LAN services on the MPLS network.

9.3.2 VPLS Reference Standards and Protocols

The following table lists the references of this document.

Document No.	Description
RFC 4762	Virtual Private LAN Service (VPLS) Using Label Distribution Protocol (LDP) Signaling
draft-ietf-l2vpn-oam-req-frmk-01	VPLS OAM Requirements and Framework
RFC 4447	Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)
draft-ietf-l2vpn-signaling-08	Provisioning, Autodiscovery, and Signaling in L2VPNs
draft-ietf-pwe3-redundancy-04	Pseudowire Redundancy

9.3.3 VPLS Principles

9.3.3.1 Introduction to VPLS

Basic VPLS Transport Structure

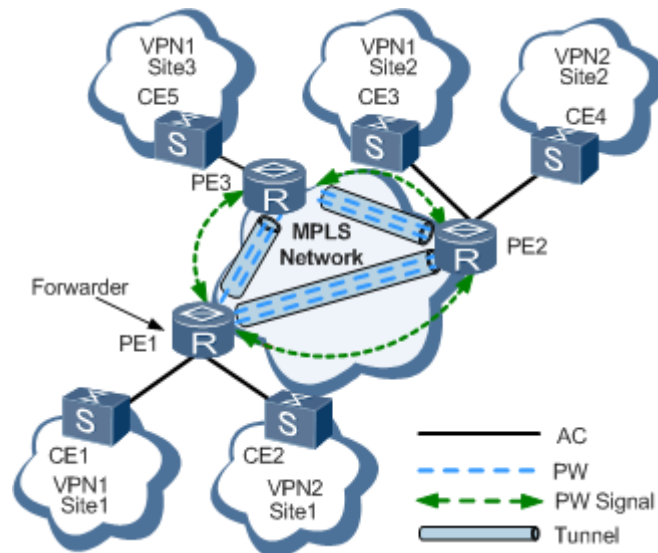
Figure 9-31 shows an example of a VPLS network. The entire VPLS network is similar to a switch. PWs are established over MPLS tunnels between VPN sites to

transparently transmit Layer 2 packets between sites. When forwarding packets, PEs learn the source MAC addresses of these packets and create MAC entries, mapping MAC addresses to attachment circuits (ACs) and PWs.

The following table describes the various concepts related to VPLS networks.

- **AC** A link between a CE and a PE. An AC must be established using Ethernet interfaces. On a VPLS network, AC interfaces can be Ethernet interfaces, Ethernet sub-interfaces, VLANIF interfaces, Eth-Trunk interfaces, Eth-Trunk sub-interfaces, VE interfaces, QinQ interfaces, and VE (ATM 1483B) interfaces.
- **PW** A bidirectional virtual connection between two virtual switch instances (VSIs) residing on two PEs. A PW consists of a pair of unidirectional MPLS VCs transmitting in opposite directions.
- **VSI** A type of instance used to map ACs to PWs. A VSI independently provides VPLS services and forwards Layer 2 packets based on MAC addresses and VLAN tags. A VSI has the Ethernet bridge function and can terminate PWs.
- **PW signaling** A type of signaling used to create and maintain PWs. PW signaling is the foundation for VPLS implementation. Currently, the PW signaling is LDP or BGP. MA5800 supports only LDP PW signaling.
- **Tunnels** are used for carrying PWs. A tunnel can carry multiple PWs. A tunnel is a direct channel that transparently transmits data between the local and remote PE devices. It can be an MPLS or a GRE tunnel. MA5800 supports only MPLS tunnels.
- **Forwarder** Similar to a VPLS forwarding table. After a PE receives packets from an AC, the forwarder of the PE selects a PW to forward these packets. It is similar to a VPLS forwarding table.

Figure 9-31 Basic VPLS transmission process



The forwarding of a packet from CE1 to CE3 on VPN1 is used as an example:

1. CE1 sends a Layer 2 packet to PE1 over an AC.
2. After PE1 receives the packet, the forwarder of PE1 selects a PW for forwarding the packet.

3. PE1 then adds two MPLS labels to the packet based on the PW forwarding entry and sends the packet to PE2. The private network label identifies the PW, and the public network label identifies the tunnel between PE1 and PE2.
4. After PE2 receives the packet from the public tunnel, PE2 removes the private network label of the packet.
5. The forwarder of PE2 selects an AC and forwards the packet to CE3 over the AC.

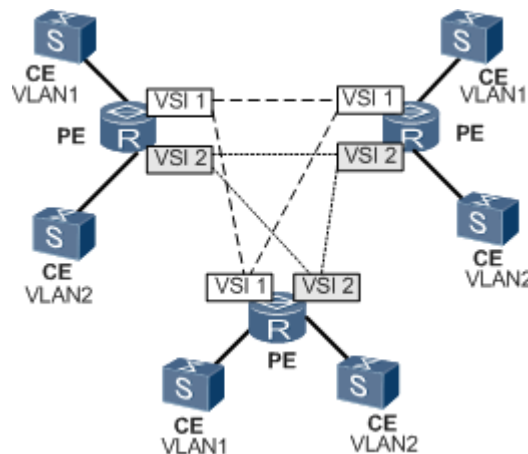
VPLS Implementation Process

Transmission of packets between CEs relies on VSIs configured on PEs, and PWs established between the VSIs. [Figure 9-31](#) shows transmission of Ethernet frames over full-mesh PWs between PEs.

The Ethernet often uses the Spanning Tree Protocol (STP) to prevent loops. VPLS networks, however, use full-mesh PWs and split horizon to avoid loops as follows:

The PEs in a VSI must be fully meshed. That is, a PE must create a tree path to every other PE in the VSI. Each PE must support split horizon to avoid loops. Split horizon requires that packets received from a PW in a VSI should not be forwarded to other PWs in the VSI. Any two PEs in a VSI must communicate over a direct PW, which is why full-mesh PWs are required between PEs in a VSI.

Figure 9-32 VPLS forwarding model



A VPLS network consists of a control plane and a forwarding plane.

- The control plane of a VPLS PE provides the following functions:
 - Member discovery: a process in which a PE in a VSI discovers the other PEs in the same VSI. This process can be implemented manually or automatically using protocols. BGP VPLS and BGP AD VPLS both support automatic member discovery.
 - Signaling mechanism: PWs between PEs in the same VSI are established, maintained, or torn down using signaling protocols such as LDP and BGP.
- The forwarding plane of a VPLS PE provides the following functions:
 - Encapsulation: After receiving Ethernet frames from a CE, a PE encapsulates the frames into packets and sends the packets to a PSN.

- Forwarding: A PE determines how to forward a packet based on the inbound interface and destination MAC address of the packet. For details, see [Table 9-3](#).
- Decapsulation: After receiving packets from a PSN, a PE decapsulates these packets into Ethernet frames and sends the frames to a CE.

VPLS Implementation Modes

VPLS can be implemented in LDP, BGP, or BGP AD mode.

- VPLS implemented in LDP mode is also called Martini VPLS.
- VPLS implemented in BGP mode is also called Kompella VPLS.
- VPLS BGP AD uses extended BGP Update packets to implement automatic member discovery. It also uses LDP FEC 129 signaling packets for local and remote VSIs to automatically negotiate and establish VPLS PWs.

NOTE

MA5800 only supports LDP mode.

The differences between the three tunnel setup modes are as follows:

- In LDP tunnel setup mode, the requirements for PEs are low, but no auto-discovery mechanism for VPN members can be provided, which has to be configured manually. In BGP tunnel setup mode, the requirements for PEs are high. That is, PEs must run BGP. In addition, the auto-discovery mechanism for VPN members can be provided. Therefore, if the LDP mode is used, you need to configure the PW to the new PE on each PE when adding a PE. In BGP mode, if the number of PEs does not exceed the label block size, you only need to configure new PEs.
- In LDP tunnel setup mode, an LDP session must be created between every two PEs. The number of sessions is in direct ratio to the square of the number of PEs. In BGP tunnel setup mode, route reflector (RR) can be used to reduce the number of BGP connections.
- In LDP tunnel setup mode, each PE is assigned with a label only if necessary. In BGP tunnel setup mode, each PE is assigned with a label block, which leads to the waste of labels.
- In LDP tunnel setup mode, the VSIs configured in all domains must use the same VSI ID range. In BGP tunnel setup mode, the VPN target is used to identify VPNs.
- The BGP AD VPLS mode integrates the advantages of the Kompella and Martini VPLS modes. With support for automatic VPLS member discovery and PW deployment, BGP AD VPLS simplifies VPLS configurations on newly added nodes as compared with Martini VPLS. BGP AD VPLS also saves label resources and is compatible with PWE3, which are not supported by Kompella VPLS.

[Table 9-2](#) shows the comparison between the two VPLS tunnel setup modes.

Table 9-2 Comparison between two VPLS tunnel setup modes

Type	LDP	BGP
Requirements for PEs	Common	High
Auto-discovery supported	No	Yes
Implementation complexity	Low	High
Expansibility	Poor	Good
Label utilization ratio	High	Low
Configuration workload	High	Low
Cross-domain restrictions	High	Low

After the preceding comparison, the following conclusions can be drawn:

- The LDP tunnel setup mode is preferable when the number of VPLS sites is relatively small, the VPLS network seldom or never traverses multiple domains, and PEs do not run BGP.
- The BGP tunnel setup mode is applicable at the core layer of a large-scale network when PEs run BGP and cross-domain is required.

If the scale of a VPLS network is large (a great number of nodes in a wide geographical range), you can use HVPLS to combine the two modes. That is, the core layer uses the BGP tunnel setup mode and the access layer uses the LDP tunnel setup mode. VPLS assumes that each PE is capable of setting up tunnels; PW labels functions as the identifiers for services; tunnels are responsible for transmitting VPLS data from a PE to another PE.

VPLS Encapsulation Modes

- Packet encapsulation on ACs
Packet encapsulation on ACs depends on the user access mode, which can be VLAN or Ethernet access.

NOTE

Currently, the MA5800 supports only packet encapsulation type of VLAN.

Table 9-3 Packet encapsulation on ACs

Packet Encapsulation Type	Description
VLAN	The header of each Ethernet frame sent between CEs and PEs carries a VLAN tag, known as the SVLAN. This is a service delimiter identifying users on an ISP network.

Packet Encapsulation Type	Description
Ethernet	The header of each Ethernet frame sent between CEs and PEs does not carry an SVLAN. If the frame header contains a VLAN tag, it is an inner VLAN tag called the CVLAN. A CE does not add the CVLAN to an Ethernet frame; instead, the tag is carried in a packet before the packet is sent to the CE. A CVLAN informs the CE to which VLAN the packet belongs, and is meaningless to PEs.

- Packet encapsulation on PWs

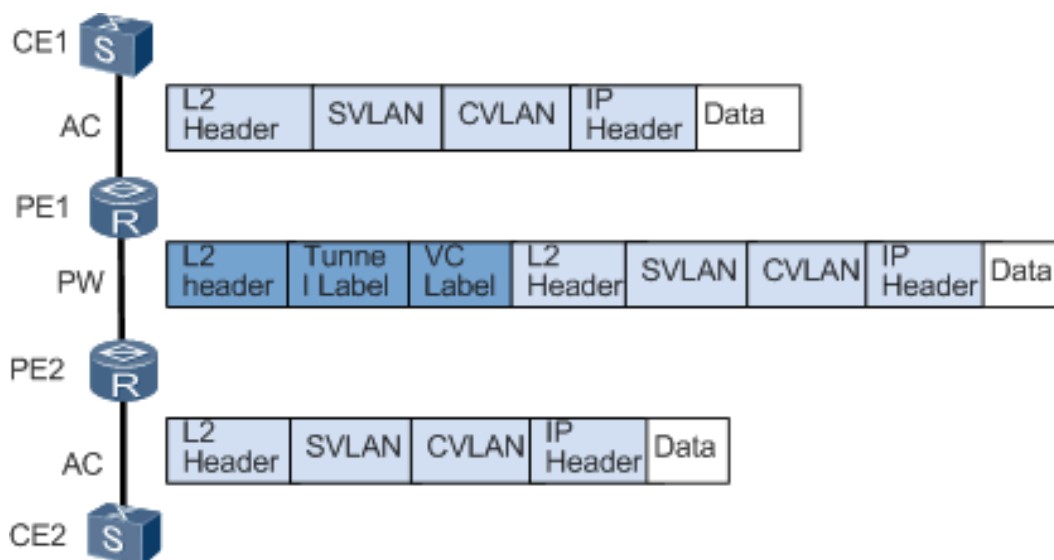
The PW ID and PW encapsulation type uniquely identify a PW. The PW IDs and PW encapsulation types configured on the two end PEs of a PW must be the same. The packet encapsulation types of packets on PWs can be raw or tagged. By default, packets on PWs are encapsulated in tagged mode.

Table 9-4 Packet encapsulation on PWs

Packet Encapsulation Type	Description
Raw	Packets transmitted over a PW cannot carry SVLANs. If a PE receives a packet with the SVLAN from a CE, the PE strips the SVLAN and adds double labels (outer tunnel label and inner VC label) to the packet before forwarding it. If a PE receives a packet with no SVLAN from a CE, the PE directly adds double labels (outer tunnel label and inner VC label) to the packet before forwarding it. The PE determines whether to add the SVLAN to a packet based on actual configurations before sending it to a CE. The PE is not allowed to rewrite or remove an existing CVLAN.
Tagged	Packets transmitted over a PW must carry SVLANs. If a PE receives a packet with the SVLAN from a CE, the PE directly adds double labels (outer tunnel label and inner VC label) to the packet before forwarding it. If a PE receives a packet with no SVLAN from a CE, the PE adds a null SVLAN and double labels (outer tunnel label and inner VC label) to the packet before forwarding it. The PE determines whether to rewrite, remove, or preserve the SVLAN of a packet based on actual configurations before forwarding it to a CE.

Encapsulation modes of packets transmitted over ACs and PWs can be used together. The following uses VLAN+tagged encapsulation (with the CVLAN) as examples to describe the packet exchange process.

VLAN+tagged encapsulation (with the CVLAN)

Figure 9-33 VLAN+tagged encapsulation (with the CVLAN)

As shown in [Figure 9-33](#), ACs use VLAN encapsulation and PWs use tagged encapsulation; packets transmitted from CEs to PEs carry U-Tags and SVLANs.

The packet exchange process is as follows:

1. CE1 sends a packet that has Layer 2 encapsulation and carries both a CVLAN and an SVLAN to PE1.
2. Upon receiving the packet that contains the CVLAN and SVLAN, PE1 does not process the CVLAN and regards it as user data.
3. The PW is encapsulated in tagged mode. A frame to be sent to the PW must carry the SVLAN. After receiving the packet with the SVLAN, PE1 does not process the packet.
4. PE1 queries entries in the VSI, and selects a tunnel and a PW for the packet.
5. PE1 adds double MPLS labels (outer tunnel label and inner VC label) to the packet based on the selected tunnel and PW, performs Layer 2 encapsulation, and forwards the packet to PE2.
6. PE2 receives the packet from PE1 and decapsulates the packet to remove Layer 2 encapsulation information and two MPLS labels.
7. PE2 forwards the original Layer 2 packet from CE1 to CE2. The packet carries the C-VLAN and S-VLAN tags.

The processing of sending a packet from CE2 to CE1 is similar to this process.

Derivative VPLS Functions

Traffic Statistics

Traffic statistics can be collected based on ACs or PWs, and the status of various types of traffic can be viewed in real time.

VPLS Service Isolation

VPLS service isolation allows you to prohibit communication between users that use the same service and bound to the same VSI.

By default, traffic can be forwarded between AC interfaces, between UPE PWs, and between AC interfaces and UPE PWs in a VSI. After VPLS forwarding isolation is enabled, traffic cannot be forwarded between AC interfaces, between UPE PWs, or between an AC and a UPE PW in a VSI.

NOTE

On a non-hierarchical VPLS network, VPLS service isolation prohibits traffic forwarding between AC interfaces. On an HVPLS network, VPLS service isolation prohibits traffic forwarding between AC interfaces, between UPE PWs, and between AC interfaces and UPE PWs.

9.3.3.2 VPLS Layer 2 Functions

Background

A characteristic of the Ethernet is that a port sends unicast packets with unknown destination MAC addresses, broadcast packets, and multicast packets to all other ports on the Ethernet. As an Ethernet-based technology, VPLS emulates an Ethernet bridge for user networks. To forward packets on a VPLS network, PEs must establish MAC address tables and forward packets based on MAC addresses or MAC addresses and VLAN tags.

On a VPLS network, each VSI maintains a MAC address forwarding table and provides the functions of MAC address learning, flooding, forwarding, and aging to forward packets.

Related Concepts

- MAC address learning
[Table 9-5](#) describes MAC address learning modes.

NOTE

At present, the MA5800 supports only MAC address learning in qualified mode.

Table 9-5 MAC address learning modes

MAC Address Learning Mode	Description	Characteristic
Qualified	A PE learns the MAC addresses and VLAN tags of received Ethernet frames. In this mode, each user VLAN is an independent broadcast domain and has independent MAC address space.	The broadcast domain is confined to each user VLAN. Qualified learning can result in large FIB table sizes, because the logical MAC address is now a VLAN tag + MAC address.

MAC Address Learning Mode	Description	Characteristic
Unqualified	A PE learns only the MAC addresses of Ethernet frames. In this mode, all user VLANs share the same broadcast domain and MAC address space. The MAC address of each user VLAN must be unique.	If an AC interface is associated with multiple user VLANs, this AC interface must be a physical interface bound to a unique VSI.

- MAC address aging

An aging mechanism removes MAC entries that a PE no longer needs. If a MAC entry is not updated within a specified period of time, this entry will be aged.

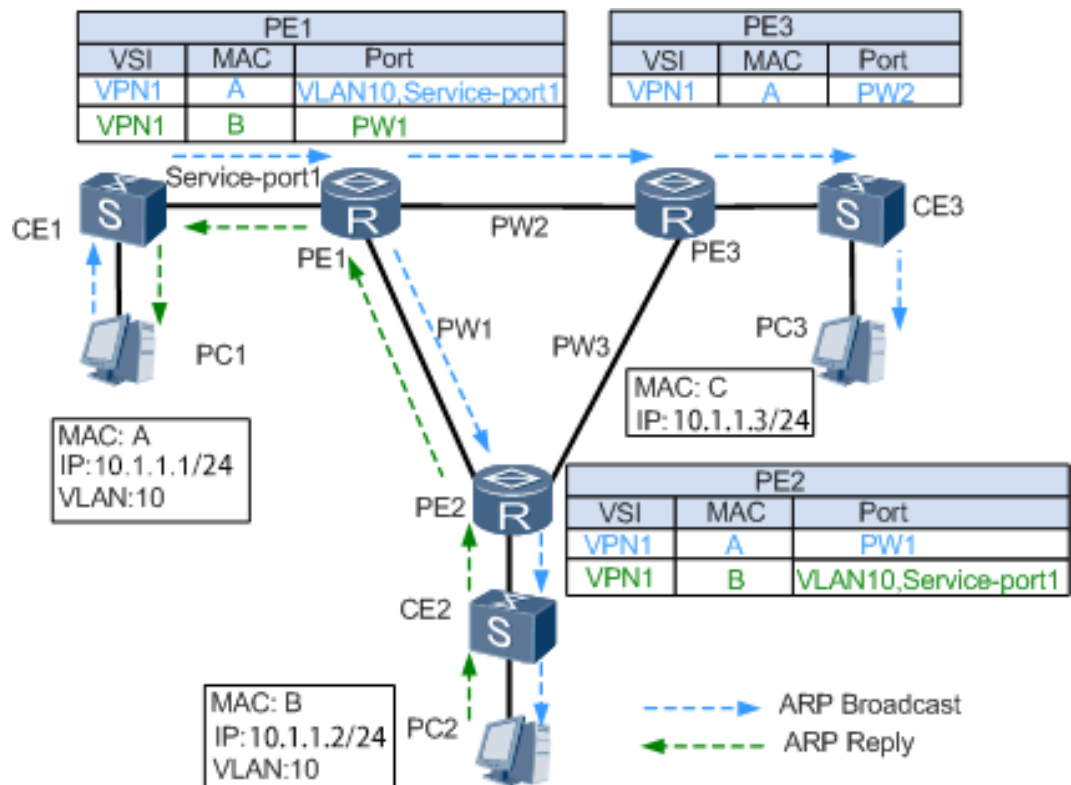
Implementation

PEs establish MAC address tables based on dynamic MAC address learning and associates destination MAC addresses with PWs. [Table 9-6](#) describes the MAC address learning process.

Table 9-6 MAC address learning process

MAC Address Learning Process	Description
Learning MAC addresses from user-side packets	After receiving packets from a CE, a PE maps their source MAC addresses to the service port corresponding to CE.
Learning MAC addresses from PW-side packets	A PW consists of a pair of MPLS VCs transmitting in opposite directions. A PW will go Up only after the two MPLS VCs are established. After a PE receives a packet with an unknown source MAC address from a PW, the PE maps the source MAC address to the AC interface receiving the packet.

[Figure 9-34](#) shows the process of MAC address learning and flooding on a PE. PC1 and PC2 both belong to VLAN10. When PC1 pings IP address 10.1.1.2, PC1 does not know the MAC address corresponding to this IP address and advertises an ARP Request packet.

Figure 9-34 MAC address learning process

1. After receiving the ARP Request packet sent by PC1 from service port1 that connects to CE1, PE1 adds the MAC address of PC1 to its own MAC address table, as shown in the blue section of the MAC entry.
2. PE1 advertises the ARP Request packet to its other ports (PW1 and PW2 can be viewed as ports).
3. After receiving the ARP Request packet from PW1, PE2 adds the MAC address of PC1 to its own MAC address table, as shown in the blue section of the MAC entry.
4. Based on split horizon, PE2 sends the ARP Request packet to only the port connecting to CE2 (as indicated by the blue dashed line), but not to PW1. This ensures that only PC2 receives the ARP Request packet. VPLS split horizon ensures that packets received from public network PWs are forwarded to only private networks, not to other public network PWs.
5. After PC2 receives the ARP Request packet and finds that it is the destination of this packet, PC2 sends an ARP Reply packet to PC1 (as indicated by the green dashed line).
6. After receiving the ARP Reply packet from PC2, PE2 adds the MAC address of PC2 to its own MAC address table, as indicated by the blue section of the MAC entry. The destination MAC address of the ARP Reply packet is the MAC address of PC1 (MAC A). After searching its MAC address table, PE2 sends the ARP Reply packet to PE1 over PW1.
7. After receiving the ARP Reply packet from PE2, PE1 adds the MAC address of PC2 to its own MAC address table. After searching its MAC address table, PE1 sends the ARP Reply packet to PC1 through service port1.

8. After receiving the ARP Reply packet from PC2, PC1 completes MAC address learning.
9. While advertising the ARP Request packet to PW1, PE1 also advertises the ARP Request packet to PE3 over PW2. After receiving the ARP Request packet, PE3 adds the MAC address of PC1 to its MAC address table. Based on split horizon, PE3 sends the ARP Request packet to only PC3. Because PC3 is not the destination of the ARP Request packet, PC3 does not send any ARP Reply packet.

Derivative Functions

Traffic Restriction

On a VPLS network, you can limit the rates of broadcast, multicast, and unknown unicast packets to:

- Enhance traffic management and appropriately allocate user bandwidth.
- Prevent traffic attacks and enhance network security.

Limit on the Number of Learned MAC Addresses

After the number of MAC entries or MAC address learning time reaches the set threshold, a device forwards or drops newly received packets and decides whether to report an alarm to the network management system (NMS).

This function applies to networks with relatively fixed users but insufficient security, such as residential access networks and enterprise intranets without security management.

9.3.3.3 LDP VPLS

Background

LDP VPLS (Martini VPLS) uses a static discovery mechanism to discover VPLS members using LDP signaling. VPLS information is carried in extended TLV fields of LDP signaling packets.

Related Concepts

LDP VPLS involves the following concepts:

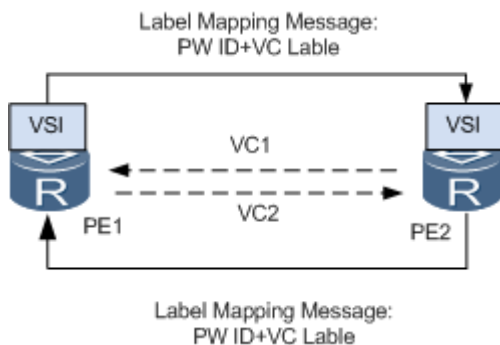
- FEC: A set of packets with similar or identical characteristics and forwarded in the same way by LSRs. Characteristics determining the FEC of a packet include the destination address, service type, and QoS attribute. Currently, the MA5800 only supports VLAN as FEC.
- TLV: A highly efficient and expandable coding mode for protocol packets. To support new features, you only need to add new types of TLVs to carry information required by the features.
- DU: A label distribution mode in which an LSR distributes labels to FECs without having to receive Label Request messages from its upstream LSR.
- Liberal: A label retention mode in which an LSR retains the label mapping received from a neighboring LSR, regardless of whether the neighboring LSR is its next hop. In liberal label retention mode, an LSR can use the labels sent

from neighboring LSRs that are not at the next hop to re-establish an LSP. This mode requires more memory and label space than the conservative mode.

Implementation Process

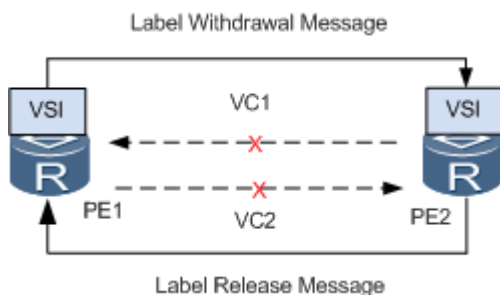
- **Figure 9-35** shows the process of establishing a PW using LDP signaling.

Figure 9-35 Establishing a PW using LDP signaling



- After PE1 is associated with a VSI, and PE2 is configured as a peer of PE1, PE1 sends a Label Mapping message to PE2 in DU mode if an LDP session already exists between PE1 and PE2. The Label Mapping message carries information required to establish a PW, such as the PW ID, VC label, and interface parameters.
 - Upon receipt of the message, PE2 checks whether itself has been associated with the VSI. If PE2 has been associated with the VSI and PW parameters on PE1 and PE2 are consistent, PE1 and PE2 belong to the same VSI. In this case, PE2 establishes a unidirectional VC named VC1 immediately after PE2 receives the Label Mapping message. Meanwhile, PE2 sends a Label Mapping message to PE1. After receiving the message, PE1 takes a similar sequence of actions to PE2 and establishes VC2.
- **Figure 9-36** shows the process of tearing down a PW using LDP signaling.

Figure 9-36 Tearing down a PW using LDP signaling



- After the peer configuration about PE2 is deleted from PE1, PE1 sends a Label Withdrawal message to PE2. After receiving the Label Withdrawal

- message, PE2 withdraws its local VC label, tears down VC1, and sends a Label Release message to PE1.
- b. After receiving the Label Release message, PE1 withdraws its local VC label and tears down VC2.

Derivative Functions

Compatibility and switchover between PWE3 VPLS and LDP VPLS

The differences between PWE3 and LDP VPLS are as follows:

- In PWE3 mode, the Label Mapping Message is sent as long as the PW is configured. In LDP VPLS mode, the message is sent only when the local up conditions are met.
- In LDP VPLS, the Label Mapping Message packet does not contain the PW Status. The Label Mapping Message and Label Withdrawal Message are used to notify the local device of the Up and Down states.
- LDP VPLS does not support notification messages to notify status constraints.

MAC Withdrawal

- After receiving a MAC-Withdraw message that carries the NULL MAC TLV, the remote PE clears all MAC address entries in the VSI by default. You can configure a PE to delete MAC address entries in standard mode defined in RFC 4762. In standard mode, only MAC address entries for those ports that are not used by the corresponding PW are deleted.
- After receiving a MAC-Withdraw message that carries the PE-ID TLV, the remote PE clears the MAC address entry for the corresponding PW.

Ignorance of the AC Status by a VSI

Before the replacement of CEs, you can configure VSIs on UPEs to temporarily ignore the AC interface status check. Then, check whether VSIs on UPEs can work properly after new CEs are deployed. A VSI can be Up only if at least one AC interface and one PW are Up. After you configure a VSI to ignore the AC interface status check, the VSI remains Up as long as one PW is Up, regardless of whether the AC interface status is Up or Down.

Receiving of Group Messages by PWs

The IETF defines the usage scenario of this function. If multiple PWs, belonging to the same group and having the same status, are configured on a physical interface, Group messages can be used to notify PWs of the interface status change when the physical interface goes Up or Down, reducing the number of Notification messages required.

NOTE

At present, the MA5800 can only receive group messages and cannot send group messages.

PW Reliability

LDP VPLS ensures PW reliability by manual configuration. When the primary PW fails, traffic from the primary PW switch to the secondary PW; When primary PW recovers, traffic can be immediate or delayed switch back to the primary PW.

Usage Scenario

The LDP mode applies to VPLS networks that do not have many sites, do not span multiple ASs, or with PEs that do not run BGP.

Benefits

LDP VPLS brings the following benefits:

- Easy configuration
- Label resource saving

9.3.3.4 VPLS PW Redundancy

Implementation

To ensure the same forwarding capability, the PW redundancy protection mechanism to be used must allow the configuration of a single PW in a PW group to be an active PW and the remaining to be standby PWs, which requires corresponding signaling control.

RFC 4447 (Pseudowire Setup and Maintenance Using the Label Distribution Protocol [LDP]) specifies the PW Status TLV to transmit the PW forwarding status. The PW Status TLV is transported to the remote PW peer using a Label Mapping or LDP Notification message. The PW Status TLV is a 32-bit status code field. Each bit in the status code field can be set individually to indicate more than one failure. PW redundancy introduces a new PW status code 0x00000020. When the code is set, it indicates "PW forwarding standby".

Forwarding priorities (Primary or Secondary) must be configured for PWs that back up each other. The highest priority PW will be selected as the primary PW to forward traffic. The remaining PWs will be in the Secondary state to protect the primary PW.

NOTE

Currently, only one secondary PW can be configured for a primary PW.

The forwarding status of a PW determines whether the PW is used to forward traffic. The PW forwarding statuses depend on:

- Local and remote PW signaling statuses: A PE monitors the local signaling status and uses PW redundancy signaling to obtain remote signaling status from a remote PE.
- PW redundancy mode: Master/Slave or Independent mode is specified on PE1.
- PW forwarding priorities: PW forwarding priorities (Primary or Secondary) are specified on PE1.

Figure 9-37 shows that VPLS PW redundancy is configured on PE1. In normal cases, all local and remote PW signaling statuses on PE1 are Up. PEs at the two ends of a PW in different VPLS PW redundancy modes use different methods to select the same PW for transmitting user packets.

- In Master/Slave mode, PE1 determines local PW forwarding statuses based on preset forwarding priorities and informs PE2 and PE5 of the PW forwarding

statuses; PE2 and PE5 determine their PW forwarding statuses based on the received PW primary and secondary statuses.

- In Independent mode, PE1 determines local PW forwarding statuses based on the forwarding statuses learned from PE2 and PE5; PE2 and PE5 determine their PW primary and secondary statuses based on signaling, which can be enhanced trunk (E-Trunk), enhanced automatic protection switching (E-APS), or Virtual Router Redundancy Protocol (VRRP) signaling, and notifies PE1 of the forwarding statuses.

In both Master/Slave and Independent modes, if a primary PW is faulty, it becomes inactive and its secondary PW becomes active. PW-side faults do not affect the AC status. If AC-side faults occur (for example, a PE or AC link is faulty), the PW primary and secondary statuses in Independent mode will change because the statuses are determined by the master and backup statuses of the dual-homing devices; the PW primary and secondary statuses in Master/Slave mode will not change because they are determined by PW side.

NOTE

VPLS PW redundancy is similar to VPWS PW redundancy, with the exception that a virtual switch instance (VSI) has multiple PWs to different PEs. These PWs form various PW groups. PW switching in one group does not affect other PW groups.

Derivative Function

In addition to protection against network faults in real time, VPLS PW redundancy allows users to manually switch traffic between PWs in a group during network operation and maintenance. For example, if a device providing a primary PW needs to be maintained, a user can switch traffic to the secondary PW and switch it back to the primary PW after the maintenance.

NOTE

The interval between a switchover and a switchback must be at least 15s.

Usage Scenarios

VPLS PW redundancy can be used on hierarchical virtual private LAN service (HVPLS) networks and VPLS and virtual leased line (VLL) interconnected networks. These two types of networks can bear any services, but when newly planned or deployed, these networks are suggested to carry different services based on their networking characteristics.

- HVPLS networks are suitable for bearing multicast services, such as Internet Protocol television (IPTV) services, because HVPLS networks can save VPLS core network bandwidth. For details, see [9.3.4.3 VPLS PW Redundancy for Protecting Multicast Services](#).
- VPLS and VLL interconnected networks are suitable for bearing unicast services, such as high-speed internet (HSI) and voice over IP (VoIP) services, because VLL PEs do not need to learn user MAC addresses. For details, see [9.3.4.4 VPLS PW Redundancy for Protecting Unicast Services](#).

VPLS PW redundancy can also be used to improve reliability of existing networks. On the VPLS network in [Figure 9-37](#), CE1 communicates with CE2, CE3, and CE4 through PWs between one VSI on PE1 and PE2, PE3, and PE4.

As services develop, services between CE1 and CE2, and between CE1 and CE3 require high reliability. Services between CE1 and CE4 do not require high reliability.

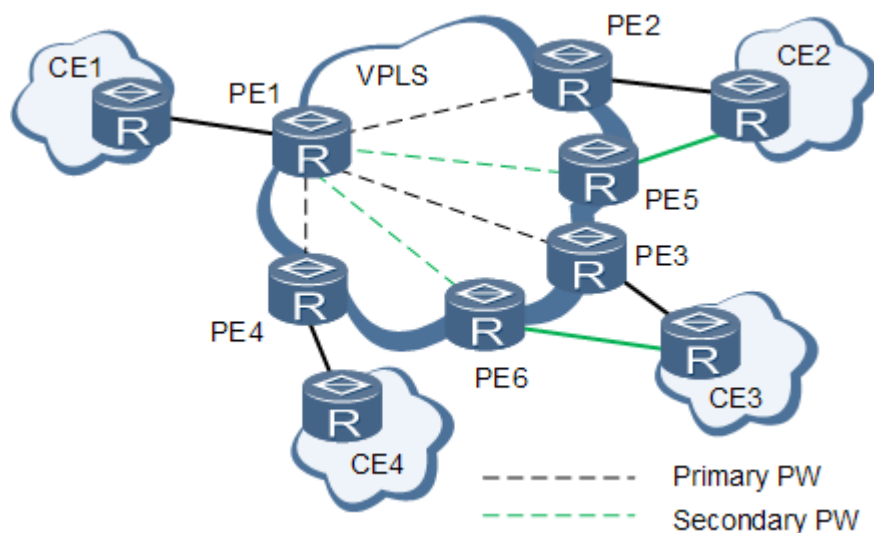
To meet the reliability requirements, PE5 and PE6 are deployed on the VPLS network to provide VPLS PW redundancy protection for PE2 and PE3, respectively. In addition, multiple PW groups to peer PEs are configured in one VSI on PE1. Links between CE1 and CE4 remain unchanged.

VPLS PW redundancy protects services against failures on the network side, AC side, or PEs without affecting existing services, improving network reliability.

NOTE

VPLS PW redundancy can be provided for the desired services without affecting services on other PWs, which reduces costs and maximizes profits.

Figure 9-37 VPLS PW redundancy networking



9.3.4 VPLS PW Redundancy Applications

9.3.4.1 Application of VPLS Individual Access

Service Overview

The traffic of individual services such as high speed internet (HSI), voice over IP (VoIP) and broadband TV (BTV) are carried by the carrier's metropolitan area network (MAN).

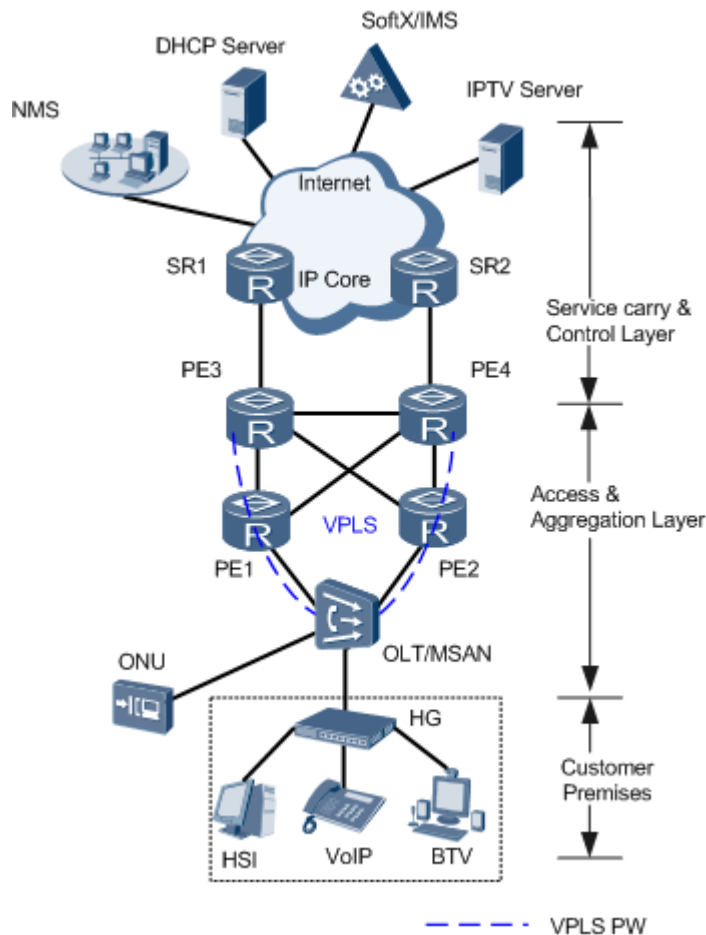
The traditional bearing technologies such as the asynchronous transfer mode (ATM) and frame relay (FR) have some defects such as high cost for network construction, slow speed and complicated deployment. Moreover, the traditional bearing technologies only support the point-to-point (P2P) interconnection for users. With the development of IP technology, the Ethernet-based virtual private LAN service (VPLS) technology supports transparent transmission of the above-mentioned individual services and achieves the point-to-multipoint (P2MP)

interconnection for users. In addition, the Ethernet-based VPLS has many advantages, such as low cost for network construction, high speed and simple deployment. Therefore, the VPLS technology is widely used in the current MAN to transmit the user traffic.

Example Network

Figure 9-38 shows the VPLS individual access service.

Figure 9-38 Example network of VPLS individual access



The HSI service is used as an example in the example network.

- The MSAN/OLT is dual-homed to two AGS devices through the VPLS.
- The user HSI access service is provided through the PPPoE dialup and maps to the VPLS domain through a VLAN in upstream direction.
- PADI packets initiated from the user side are broadcast in the VPLS domain to which the packets belong. The broadcast packets are received on PE1 and PE2.
- The delay response is used between PE devices to terminate the dialups of some users so that the load sharing can be achieved.
- The split horizon between the VPLS and PW is enabled.

9.3.4.2 Application of VPLS Enterprise Access

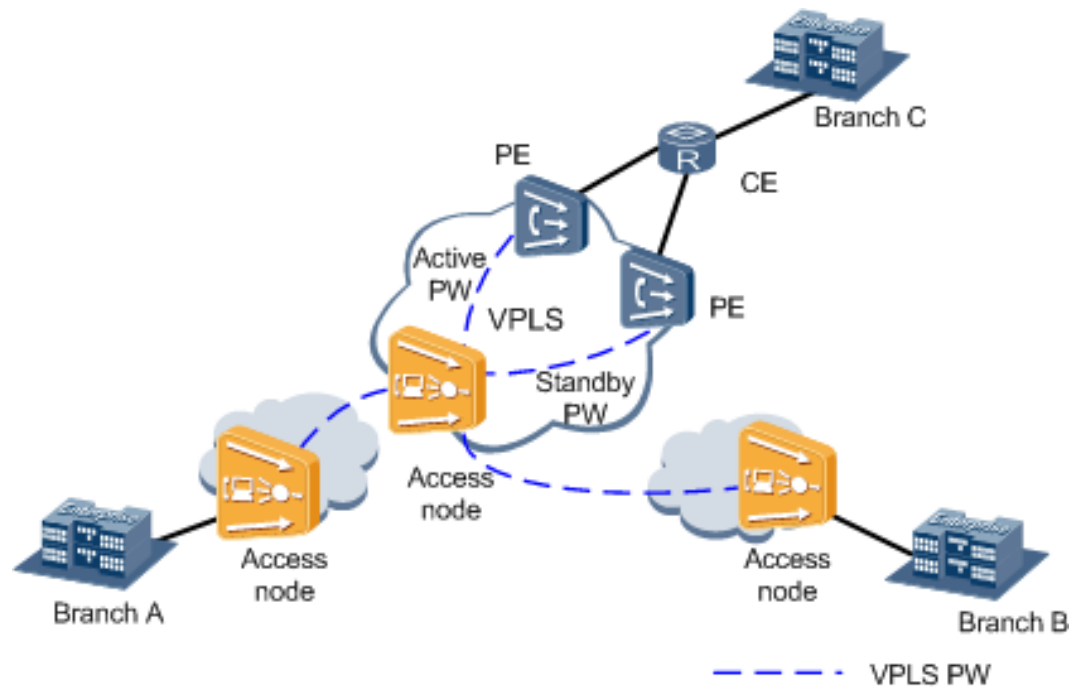
Service Overview

With the business expansion, many enterprises establish branches in different areas and employees are often on business trips. Therefore, some applications (such as the VoIP, instant messages and network conference) are used widely in enterprises. These applications require a network that supports point-to-multipoint (P2MP) services. In addition, the network reliability must be ensured and a transparent and secure data channel is required for multi-point transmission because of the privacy of the enterprise business data. The VPLS technology is suitable to be deployed in this scenario.

Example Network

Figure 9-39 shows the example network of VPLS enterprise access.

Figure 9-39 Example network of VPLS enterprise access



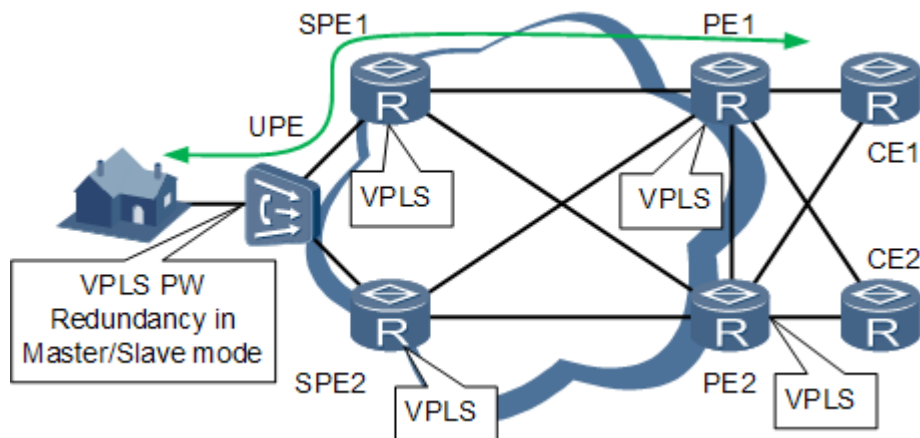
- The virtual private network (VPN) between different branches is achieved by deploying the VPLS.
- The pseudo wire (PW) redundancy is used to protect the important branches (such as branch C in the figure).
- An OLT/MSAN, functioning as the main node, implements the Layer 2 label switching, and other branches are connected to the VPLS network through backup PWs.
- The split horizon between the VPLS and PW is canceled.
- The basic Layer 2 forwarding mechanism in this scenario is consistent with that in the VPLS individual access scenario except that the split horizon needs

to be canceled and the PW protection needs to be supported for Layer 2 forwarding in this scenario.

9.3.4.3 VPLS PW Redundancy for Protecting Multicast Services

Figure 9-40 illustrates an application of VPLS PW redundancy for protecting multicast services, such as Internet Protocol television (IPTV) services, on a hierarchical virtual private LAN service (HVPLS) network. VPLS PW redundancy is used to ensure network reliability.

Figure 9-40 VPLS PW redundancy for protecting multicast services



Multicast sources CE1 and CE2 are each dual-homed to provider edge 1 (PE1) and PE2 through enhanced trunks (E-Trunks); common PWs connect PEs and superstratum PEs (SPEs). A gateway user-end provider edge (UPE) connects the user end to SPE1/SPE2. The link between the UPE and SPE1 and the link between the UPE and SPE2 back up each other.

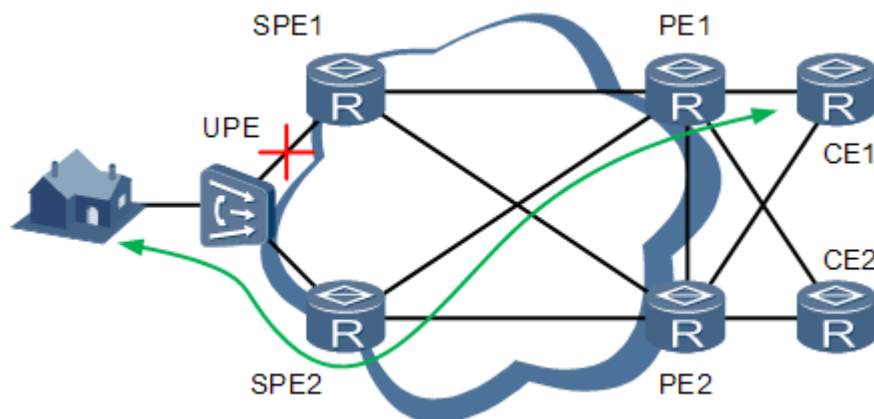
For this networking, the UPE must use PW redundancy in Master/Slave mode because SPE1 and SPE2 do not exchange signaling for determining which one is the master SPE. Upon detecting that the primary PW fails, the UPE rapidly switches traffic to the secondary PW, instructs SPE2 to work as the primary SPE, and sends MAC Withdraw messages to SPE2 instructing SPE2 to delete the MAC addresses learned from SPE1. SPE2 transmits the MAC Withdraw messages to PE1 and PE2, instructing PE1 and PE2 to clear the MAC addresses learned from SPE1. After deleting the MAC addresses learned from SPE1, PE1 will relearn MAC addresses through multicast packets upon receiving traffic from CE1 and CE2 and switch received traffic to the secondary link.

Figure 9-40 shows service traffic when no fault occurs. The following describes how VPLS PW redundancy protects traffic after faults occur.

Primary PW Failure Between the UPE and SPE1

Figure 9-41 shows how traffic is switched if the primary PW between the UPE and SPE1 fails.

Figure 9-41 VPLS PW redundancy protecting services against a failure in the primary PW between the UPE and SPE1



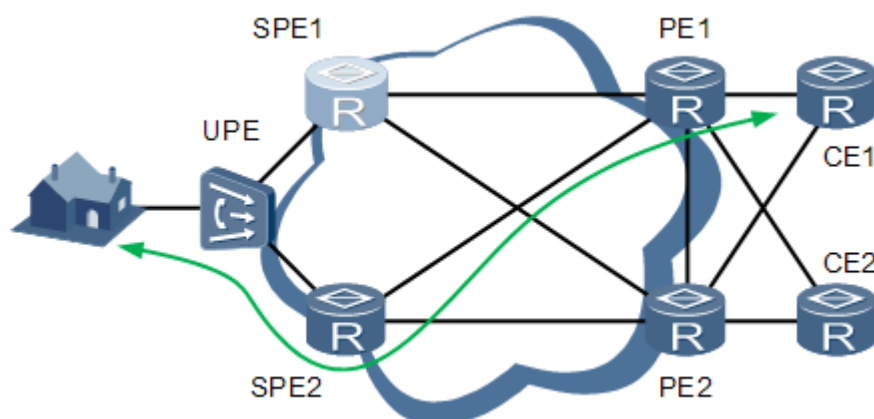
Label switched path (LSP) down events or BFD for PW may cause a PW failure. Upon detecting that the primary PW fails, the UPE switches traffic to the secondary PW and sends MAC Withdraw messages in which the PE ID field carries the SPE1 LSR ID to SPE2. SPE2 transparently transmits the MAC Withdraw messages to PE1 and PE2. SPE2, PE1, and PE2 clear the MAC addresses learned from SPE1.

Switchback: After the primary PW recovers, the UPE instructs SPE2 to change its PW status to secondary and SPE1 to change its PW status to primary. The UPE sends MAC Withdraw messages in which the PE ID field carries the SPE2 LSR ID to SPE1. SPE1 transparently transmits the MAC Withdraw messages to PE1 and PE2. SPE1, PE1, and PE2 clear the MAC addresses learned from SPE2. PE1 and PE2 then relearn MAC addresses through multicast packets from the primary PW.

SPE1 Failure

Figure 9-42 shows how traffic is switched if SPE1 fails.

Figure 9-42 VPLS PW redundancy protecting services against an SPE1 failure



After detecting that SPE1 fails, the UPE switches traffic to the secondary PW and sends MAC Withdraw messages in which the PE ID field carries the SPE1 LSR ID to SPE2. SPE2 transparently transmits the MAC Withdraw messages to PE1 and PE2. SPE2, PE1, and PE2 clear the MAC addresses learned from SPE1. Sometimes, PE1

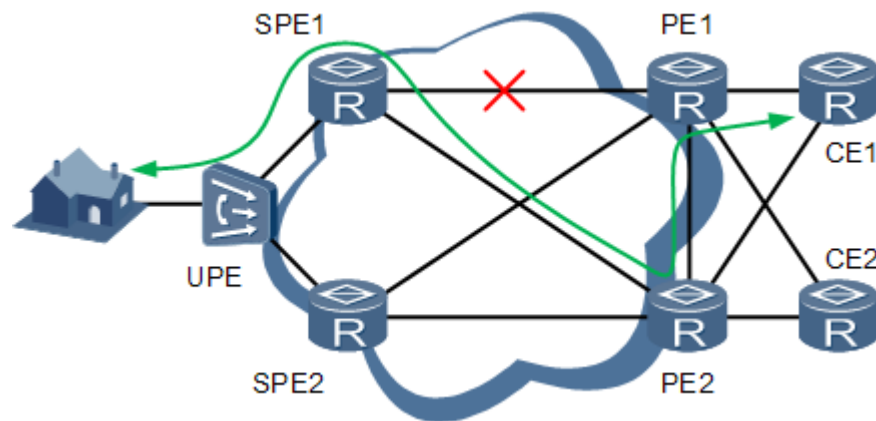
and PE2 detect that the PW passing through SPE1 is faulty before receiving the MAC Withdraw messages and directly clear the MAC addresses learned from SPE1.

Switchback: After the primary PW recovers, the UPE instructs the PW passing through SPE2 to work as a secondary PW and the PW passing through SPE1 to work as the primary PW. The UPE sends MAC Withdraw messages in which the PE ID field carries the SPE2 LSR ID to SPE1. SPE1 transparently transmits the MAC Withdraw messages to PE1 and PE2. SPE1, PE1, and PE2 clear the MAC addresses learned from SPE2. PE1 and PE2 then relearn MAC addresses through multicast packets from the primary PW.

Link Failure Between SPE1 and PE1

Figure 9-43 shows how traffic is switched if the link between SPE1 and PE1 fails.

Figure 9-43 VPLS PW redundancy protecting services against a link failure between SPE1 and PE1

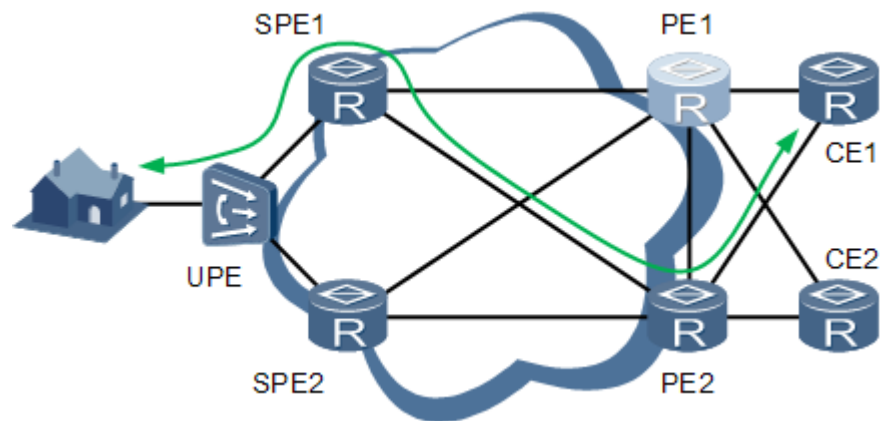


If deployed between SPE1 and PE1, Label Distribution Protocol (LDP) fast reroute (FRR) ensures the availability of traffic between SPE1 and PE1. If LDP FRR is not deployed, LDP LSP ensures the availability of traffic between SPE1 and PE1.

Switchback: Traffic will not be switched back to the primary PW. After LDP LSP convergence, the primary PW is carried by a new LSP.

PE1 Failure

Figure 9-44 shows how traffic is switched if PE1 fails.

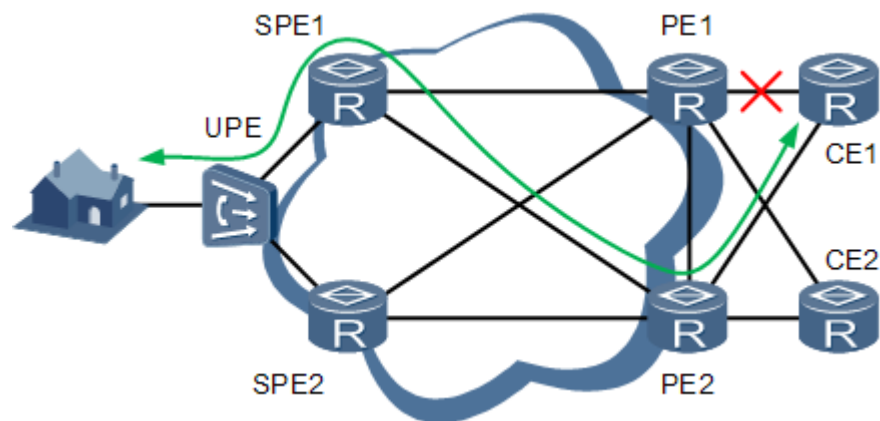
Figure 9-44 VPLS PW redundancy protecting services against a PE1 failure

CE1 and CE2 are each dual-homed to PE1 and PE2 through E-Trunk. If PE1 fails, the E-Trunk primary and secondary status changes. PE2 detects E-Trunk status changes and sends MAC Withdraw messages to SPE1 and SPE2, instructing SPE1 and SPE2 to clear MAC addresses in the associated VSI. Sometimes, SPE1 and SPE2 detect that the PW passing through PE1 is faulty before receiving the MAC Withdraw messages and directly clear MAC addresses associated with the PW.

Switchback: If PE1 recovers, traffic switches back to PE1 after a default E-Trunk switchback delay. Upon detecting E-Trunk changes, PE1 and PE2 send MAC Withdraw messages to SPE1 and SPE2, instructing SPE1 and SPE2 to clear MAC addresses learned from PE2.

Primary AC Link Failure

Figure 9-45 shows how traffic is switched if the link between CE1 and PE1 fails.

Figure 9-45 VPLS PW redundancy protecting services against a link failure between CE1 and PE1

CE1 and CE2 are each dual-homed to PE1 and PE2 through E-Trunk. After the link between CE1 and PE1 fails, the E-Trunk primary and secondary status changes. Upon detecting E-Trunk status changes, PE1 and PE2 send MAC Withdraw messages to SPE1, instructing SPE1 to clear all MAC addresses in the VSI.

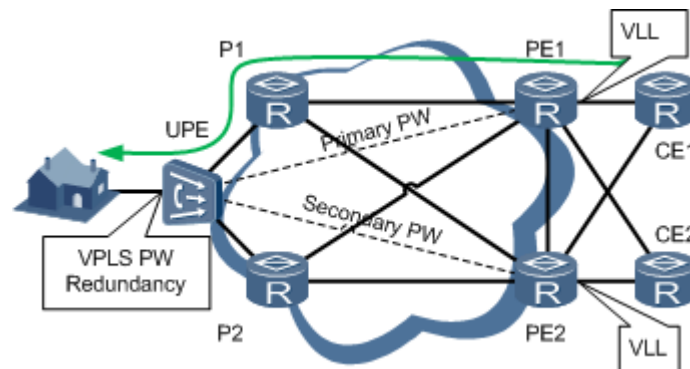
Switchback: After the link between CE1 and PE1 recovers, the E-Trunk primary and secondary status changes back. Upon detecting E-Trunk changes, PE1 and PE2

send MAC Withdraw messages to SPE1, instructing SPE1 to clear all MAC addresses.

9.3.4.4 VPLS PW Redundancy for Protecting Unicast Services

Figure 9-46 illustrates an application of VPLS PW redundancy for protecting unicast services, such as high-speed internet (HSI) or voice over IP (VoIP) services, on a virtual private LAN service (VPLS) and virtual leased line (VLL) interconnected network. VPLS PW redundancy is used to ensure network reliability.

Figure 9-46 VPLS PW redundancy for protecting unicast services



Authentication servers CE1 and CE2 are each dual-homed to PE1 and PE2 through enhanced trunks (E-Trunks). A UPE connects the user end and PE1/PE2. The link between the UPE and PE1 and the link between the UPE and PE2 back up each other.

For this networking, PE1 and PE2 can determine their master and backup statuses through E-Trunk negotiation. Therefore, the UPE can use PW redundancy in Independent mode to determine the PW primary and secondary statuses based on the status of PE1 and PE2. Upon detecting that the primary PW fails, the UPE rapidly switches traffic to the secondary PW and instructs PE2 to work as the master PE. After the E-Trunk detects that the primary PW fails, it switches traffic to the secondary AC link.

Figure 9-46 shows service traffic when no fault occurs. The following describes how VPLS PW redundancy protects services after a fault occurs.

NOTE

When a fault occurs, VPLS PW redundancy protects services differently in Master/Slave and Independent modes. The following describes the difference in service protection provided by VPLS PW redundancy in Master/Slave and Independent modes. If no description is provided, no difference exists.

Network Side Failure

Label switched path (LSP) or traffic engineering (TE) tunnels and PW redundancy can protect services against faults on the UPE network side.

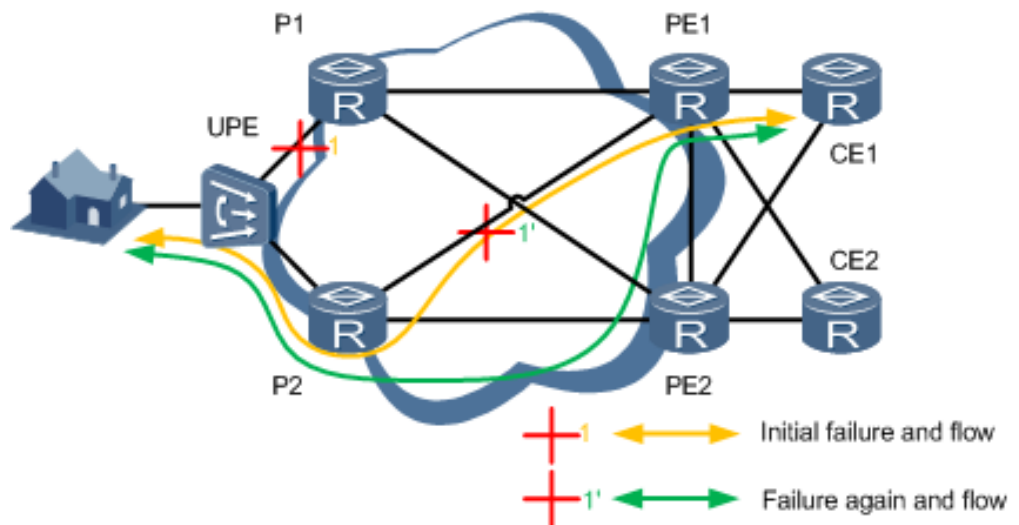
NOTE

If a network-side fault occurs, LSP or TE tunnels detect the fault and switch traffic to other tunnels. If tunnel protection is unavailable or fails, PW redundancy is required to protect traffic. A bypass PW needs to be configured between PE1 and PE2 for PW redundancy.

- LSP or TE tunnel protection: After a network-side fault occurs, routes and LSPs are recomputed. The LSP where the primary PW is located is converged to a new path. **Figure 9-47** shows how traffic is switched.

After the fault is rectified, LSPs re-converge and the primary PW is carried by a new LSP.

Figure 9-47 Protecting services against an LSP failure (bypass PW not configured)



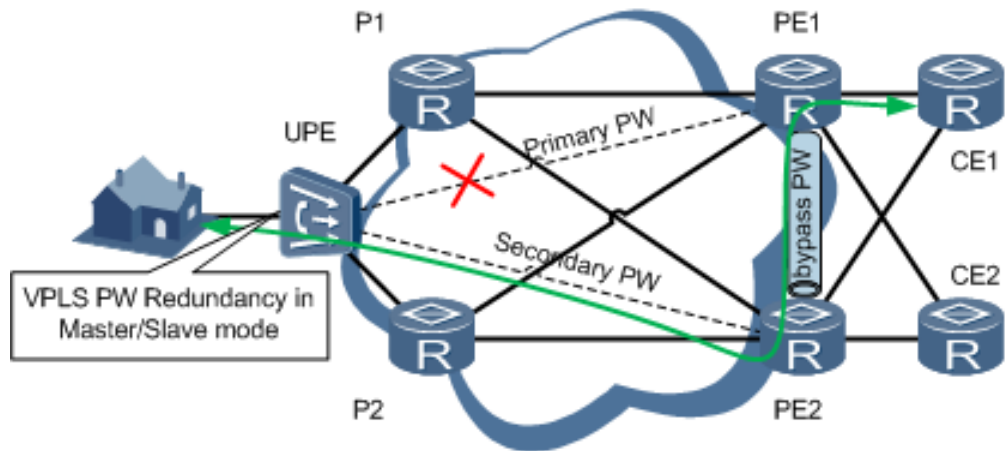
- PW redundancy: If LSP or TE tunnel switching fails, traffic is switched to the secondary PW. **Figure 9-48** shows how traffic is switched.

After the fault is rectified, traffic will be switched back based on preset switchback policies.

NOTE

Bypass PWs are required for PW redundancy to transmit traffic between PE1 and PE2.

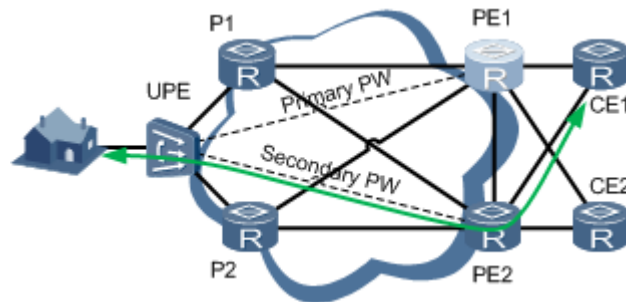
Figure 9-48 Protecting services against a primary PW failure (bypass PW configured)



PE1 Failure

Figure 9-49 shows how traffic is switched if PE1 fails.

Figure 9-49 VPLS PW redundancy protecting services against a PE1 failure



PE2 becomes the master and PE1 becomes the backup after E-Trunk negotiation. The UPE is informed of the switchover. Upon detecting that the primary PW fails, the UPE clears MAC addresses learned from the primary PW and switches traffic to the secondary PW.

Switchback: After the PE1 fault is rectified, PE1 becomes the master through E-Trunk negotiation. Upon detecting PE1 and PE2 status changes, the UPE clears MAC addresses learned from PE2 and relearns MAC addresses through multicast packets.

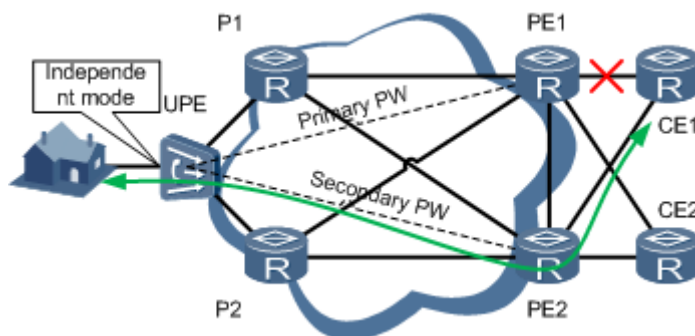
Primary AC Link Failure

Figure 9-50 shows how traffic is switched if the link between PE1 and CE1 fails.

- In Independent mode
After the primary AC link between CE1 and PE1 fails, PE2 works as the master after E-Trunk negotiation. The UPE is informed of the switchover. The UPE detects that the primary AC link fails and switches traffic to the secondary PW.

After the link between CE1 and PE1 recovers, PE1 becomes the master after E-Trunk negotiation. Upon detecting PE1 and PE2 status changes, the UPE clears MAC addresses learned from PE2 and relearns MAC addresses through multicast packets.

Figure 9-50 VPLS PW redundancy in Independent mode protecting services against a failure in the primary AC link

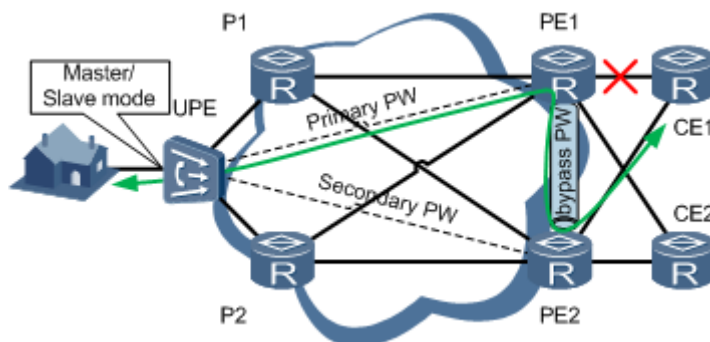


- In Master/Slave mode

After the primary AC link between CE1 and PE1 fails, PE2 works as the master after E-Trunk negotiation. The PW status on the UPE remains unchanged.

After the link between CE1 and PE1 recovers, PE1 becomes the master after E-Trunk negotiation. Upon detecting PE1 and PE2 status changes, the UPE clears MAC addresses learned from PE2 and relearns MAC addresses through multicast packets.

Figure 9-51 VPLS PW redundancy in Master/Slave mode protecting services against a failure in the primary AC link



9.3.5 Configuring VPLS MP2MP Intercommunication

VPLS can implement the multipoint-to-multipoint (MP2MP) VPN networking; therefore, by using the VPLS technology, service providers (SPs) can provide the Ethernet-based multipoint services through MPLS backbone networks.

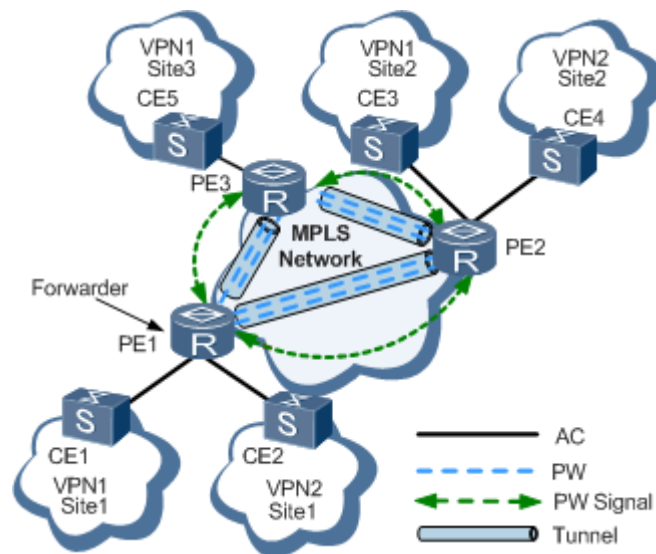
Application Context

A lot of private line services in carriers' network use the virtual private network (VPN) virtual private wire service (VPWS) technology, which can provide point-to-point (P2P) communication services on Layer 2 or Layer 3 network. With the development of Ethernet and MPLS technologies, carriers hope to provide not only P2P services on the private network, but Ethernet-like point-to-multipoint (P2MP)

services on the metropolitan area network (MAN) and wide area network (WAN). By deploying virtual private LAN service (VPLS) technology on the provider edge (PE), carriers can provide Ethernet-based MP2MP services for users through MPLS backbone networks, achieving the local area network (LAN) simulation.

Figure 9-52 shows the basic VPLS transmission process. Full-meshed PWs are created through signaling transmission by PE routers. Transmission of packets between CEs relies on VSIs configured on PEs, and PWs established between the VSIs.

Figure 9-52 Basic VPLS transmission process



Prerequisite

1. The IP address of the loopback interface must be configured.
2. The LSR ID must be configured.
3. The VLAN for MPLS label forwarding must be created.
4. The global MPLS, VLAN MPLS, and VLAN interface MPLS must be enabled.
5. MPLS L2VPN must be enabled.
6. A static or dynamic route must be successfully configured on each device in the network (so that LSRs can reach each other through the IP route).
7. The global LDP function is enabled and remote LDP sessions are configured.
8. The vlan-based traffic stream must be created.

Data preparation

Before configuring the VPLS P2MP intercommunication services, plan the data items as listed in [Table 9-7](#).

Table 9-7 Plan of VPLS P2MP intercommunication service data items

Item	Data	Remarks
MA5800	VSI	VLANs are mapped to the VPLS domain after a VSI is bound to the VLAN and PW. VLAN mapping allows service packets to be broadcast in the VPLS domain.
	VPLS PW	-

Procedure

Step 1 Configure a VSI.

VSIs are the core of VPLS services. With VSIs, actual links carrying VPLS services can be mapped into PWs.

1. In global config mode, run the **vsi** command to create a VSI and enter the VSI mode.
2. Run the **pwsignal ldp** command to configure the signaling type for VSI as LDP, or run the **bgp-ad** command to configure the signaling type for VSI as Bgp-ad.
3. Run the **vsi-id** command to configure the VSI ID.

Once the VSI ID is successfully set, it cannot be changed or deleted. If you need to change it, delete the VSI.

Step 2 (Optional) Configure VSI attributes.

In VSI mode, configure VSI basic attributes based on actual requirements. VSI basic attributes include the VSI description information, encapsulation type, control words, maximum transmission unit (MTU), and traffic suppression.

- Run the **description** command to configure the description of a VSI.
- Run the **encapsulation** command to configure the encapsulation type of a VSI.
- Run the **control-word** command to enable the control word of a VSI. After the control word is enabled, control information will be added to packets.

NOTE

If you use the **control-word** command in VSI mode and the **control-word** command in PW-para-index mode to configure the control word concurrently, the one set by the **control-word** command in PW-para-index mode takes effect.

- Run the **mtu** command to set the MTU of a VSI.
- Run the **traffic-suppress** command to set the suppression level of the broadcast, unknown multicast, and unknown unicast traffic for a VSI.

Before configuring the multicast service carried in VPLS, you must disable the VSI unknown multicast suppression. Otherwise, packet loss will occur in the multicast services.

Step 3 Configure LDP PW.

1. In global config mode, run the **pw-para pwindex** *pwindex* command to create a PW and enter the PW-para-index mode.

For a VPLS PW, you must first create the PW-para-index mode and then perform the PW binding.

2. Run the **service-type vpls** command to configure the service type of a PW as VPLS.
3. Run the **pwid** command to configure the ID of a PW.
4. Run the **peer-address** command to set the IP address of the peer device of a PW.
5. Run the **pw-type ethernet** command to configure the type of a PW as Ethernet.

When the service type is VPLS, you can set the PW type only to **Ethernet**. The PW type must be identical to the VSI encapsulation type.

6. (Optional) Run the **control-word** command to enable the control word of a PW.
7. (Optional) Run the **dyn-receive-label** command to specify the incoming label of a dynamic PW.
8. In VSI mode, run the **vsi-pw-binding** command to bind the VSI to the PW to create a VPLS PW service.

Step 4 Or configure Bgp-ad PW.

1. Run the **bgp-ad** command in VSI mode to specify the current VSI PW setup mode to automatic discovery or automatic deployment and enter the VSI BGP AD mode.
2. Run the **vpls-id** command to allocate the BGP AD mode VSI identifier.
3. Run the **vpn-target** command to associate the current VSI with one or more VPN targets. The Import VPN Target of the local PE must be the same as Export VPN Target of the peer PE. PWs can only be set up between the BGP AD VSI instances.

Step 5 In VSI mode, run the **vsi-ac-binding vlan** command to bind a VLAN to the VSI.

After the above configurations are complete, VLAN service packets can be forwarded within a VSI.

----End

Example

Assume that VLAN 100 is used for MPLS forwarding, a VSI and a PW are created, and the PW and VLAN 100 are bound to the VSI respectively. To configure VSI and PW parameters as follows:

- To set the VSI ID to **1**, the VSI name to **hsi**, and the signaling mode to **LDP**, and retain the default values for other parameters, do as follows:
- To set the PW index to **1**, the service type to **VPLS**, the PW ID to **1**, the IP address of the peer device to **10.1.1.1**, the encapsulation type to **Ethernet tagged**, and the dynamic PW incoming label to **10240**, do as follows:

```
huawei(config)#vsi hsi
huawei(config-vsi-hsi)#pwsignal ldp
```

```
huawei(config-vsi-hsi-ldp)#vsi-id 1
huawei(config-vsi-hsi-ldp)#quit
huawei(config-vsi-hsi)#quit
huawei(config)#pw-para pwindex 1
huawei(config-pw-para-index-1)#service-type vpls
huawei(config-pw-para-index-1)#pwid 1
huawei(config-pw-para-index-1)#peer-address 10.1.1.1
huawei(config-pw-para-index-1)#pw-type ethernet tagged
huawei(config-pw-para-index-1)#dyn-receive-label 10240
huawei(config-pw-para-index-1)#quit
huawei(config)#vsi hsi
huawei(config-vsi-hsi)#pwsignal ldp
huawei(config-vsi-hsi-ldp)#vsi-pw-binding pwindex 1
huawei(config-vsi-hsi-ldp)#quit
huawei(config-vsi-hsi)#vsi-ac-binding vlan 100
```

9.3.6 Configuration Example of VPLS

Virtual private LAN service (VPLS) enables geographically isolated users (individuals or branch offices of an enterprise) to establish point-to-multipoint connections between each other using Ethernet links, achieving fast and flexible service deployment.

Context

As a combination of Ethernet and Multiprotocol Label Switching (MPLS) technologies, VPLS emulates all functions of the traditional local area network (LAN), with a purpose to connect multiple geographically isolated LANs that consist of Ethernet using the IP or MPLS network provided by carriers and make the LANs work as a LAN.

Currently, the MA5800 only supports Label Distribution Protocol (LDP)-based VPLS.

[Table 9-8](#) provides basic concepts of VPLS.

Table 9-8 Basic concepts of VPLS

Concept	Description
VSI	Virtual switch instance. This concept corresponds to virtual local area network (VLAN) of Ethernet switch. Each VSI provides independent VPLS service. VSI supports the Ethernet bridge function and can terminate PW.

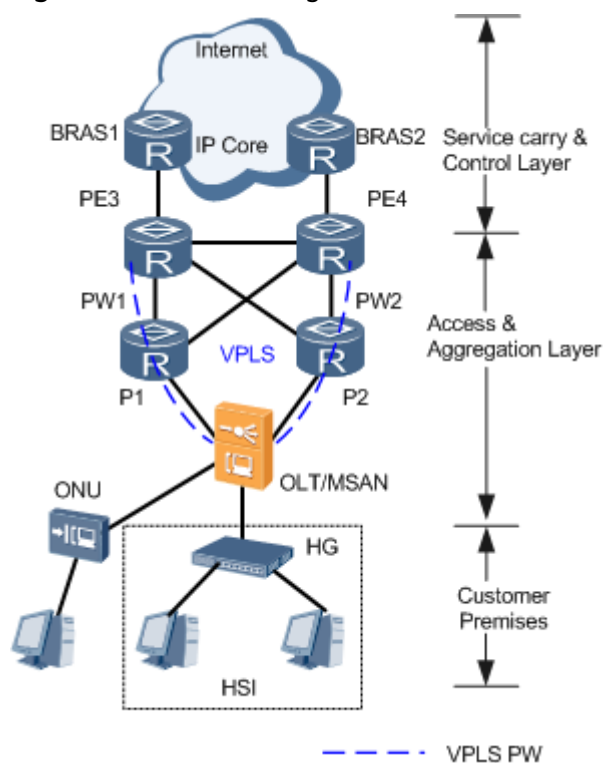
Concept	Description
PW	Pseudo wire. PW is a virtual connection between two PEs and transmits frames between the PEs. PEs use signaling to establish PWs and maintain PW status. On a VPLS network, PE routers transmit signaling to each other to establish PWs of full interconnection. Signaling exchange modes are as follows: • Martini mode: In this mode, signaling is exchanged using the LDP protocol. This mode does not support the PE automatic discovery function. PEs need to be configured manually. With this mode, the networking is simple, and low requirements are imposed on PEs which do not need to cross domains. • Kompella mode: Signaling is exchanged using the Border Gateway Protocol (BGP). The MA5800 does not support this mode.
AC	Attachment circuit. AC attaches a CE to a PE. An AC can be a physical or logical link. It transmits frames between the CE and PE.
Split horizon	Split horizon is a technology that prevents route loops and speeds up route convergence. In a VPLS network, full mesh and split horizon are used to prevent loops. Split horizon in VPLS means that the data packets received from the PW at the PSN side are not forwarded to other PWs. Instead, they are forwarded to the private network.

9.3.6.1 Configuration Example of the VPLS Internet Access Service

This topic describes how to configure the Internet access service for individual users when the VPLS networking is used at the access and aggregation layers.

Application Context

As shown in [Figure 9-53](#), the MA5800 is dual homed to two AGS devices (aggregation switches) PE3 and PE4 through VPLS, and the Internet access service is received in PPPoE dialup mode. In the upstream direction, the traffic stream is mapped into the VPLS domain through VLAN. The PPPOE active discovery initiation (PADI) packets initiated by the user are broadcast in the VPLS domain it belongs to, and then the broadcast packets are received by the two AGS devices. The AGS devices terminate packets of some users respectively in delay response mode to achieve load sharing. When a BRAS device is faulty, the user dials up again. Then the VPLS MAC learning and forwarding mechanism automatically selects a new BRAS to provide services.

Figure 9-53 Networking for the VPLS Internet access service for individual users

Prerequisite

Traffic streams have been configured on the MA5800 for the Internet access service.

NOTE

To configure the Internet access service, you must configure SVLAN 100-based traffic streams on the MA5800 and perform corresponding configurations on the HG. The configurations are the same as those for common Internet access service, which are not described here.

Data Plan

Table 9-9 provides the key data plan for the MA5800.

Table 9-9 Key data plan

Configuration Item	Data	Remarks	Requirement on PE3 and PE4
MPLS	- LSR ID: 10.10.10.10 - VLAN: 4001	MPLS must be enabled at three layers. - MPLS must be enabled globally. - MPLS must be enabled for VLAN. - MPLS must be enabled at VLAN interfaces.	The LSR ID must be unique on the entire network and MPLS must be enabled.
LDP	- MPLS LDP is enabled. - Split horizon is enabled.	MPLS LDP must be enabled at three layers. - MPLS LDP must be enabled globally. - MPLS LDP must be enabled at VLAN interfaces.	MPLS LDP is enabled. The remote LDP session to the MA5800 is configured on PE3 and PE4.
Routing protocol	The Open Shortest Path First (OSPF) protocol is used.	Ensure that the Layer 3 interfaces on the MA5800 and those on PE3 and PE4 can ping each other.	Layer 3 interfaces and routes are configured on PE3 and PE4. Ensure that the Layer 3 interfaces and LSR IDs on PE3 and PE4 and those on the MA5800 can ping each other.
VPLS PW	- PW ID: 1 and 2 - Service type: vpls - Encapsulation type: ethernet tagged - The control word is enabled.	On the MA5800, PW1 and PW2 are created for PE3 and PE4 respectively. In this way, packets can be transmitted to BRAS devices over two trails.	The LDP VPLS is supported. VPLS PWs to the MA5800 are configured on PE3 and PE4, and attributes of PWs are consistent with those on the MA5800.

Configuration Item	Data	Remarks	Requirement on PE3 and PE4
VSI	- PW1 and PW2 are bound to VSI. - VLAN 100 of the Internet access service is bound to VSI.	VSI binds VLAN and PW to map VLAN to the VPLS domain, so that PADI packets for the Internet access service can be broadcast in the VPLS domain at first, until one of the BRAS responses.	VSI is configured on PE3 and PE4 and the VSI ID must bind the corresponding PW.

Procedure

Step 1 Configure the basic MPLS.

1. Configure a loopback interface.

Set the ID of the loopback interface to **0** and its IP address to **10.10.10.10/32**.

```
huawei(config)#interface loopback 0
huawei(config-if-loopback0)#ip address 10.10.10.10 32
huawei(config-if-loopback0)#quit
```

2. Configure the MPLS LSR-ID. Use the IP address of loopback interface 0 as the LSR ID.

```
huawei(config)#mpls lsr-id 10.10.10.10
```

3. Enable MPLS globally.

Trigger LDP by the IP address of the host to set up an LSP.

```
huawei(config)#mpls
huawei(config-mpls)#lsp-trigger host
huawei(config-mpls)#quit
```

4. Enable the L2VPN function.

```
huawei(config)#mpls l2vpn
```

5. Enable the LDP function globally and enable the split horizon policy.

```
huawei(config)#mpls ldp
huawei(config-mpls-ldp)#outbound peer all split-horizon
huawei(config-mpls-ldp)#quit
```

Step 2 Configure VLAN, and enable MPLS for VLAN and VLAN interfaces.

1. Add VLAN 4001 for forwarding MPLS packets and add upstream port 0/9/0 and 0/9/1 to it.

```
huawei(config)#vlan 4001 smart
huawei(config)#port vlan 4001 0/9/0
huawei(config)#port vlan 4001 0/9/1
```

2. Enable MPLS for VLAN 4001. Set the IP address of VLAN interface 4001 to 10.50.50.50/24 and enable MPLS LDP for the VLAN interface.

```
huawei(config)#interface vlanif 4001
huawei(config-if-vlanif4001)#ip address 10.50.50.50 24
huawei(config-if-vlanif4001)#mpls
```

```
huawei(config-if-vlanif4001)#mpls ldp
huawei(config-if-vlanif4001)#quit
```

Step 3 Configure routes.

VPLS has no special requirements on routing policy. You can use static route, RIP, or OSPF policy. In the following example, OSPF is used.

Set the OSPF process ID to **100** and OSPF area ID to **1**. In addition, configure the interfaces (VLAN interface and loopback interface) that run OSPF and configure the areas of the interfaces.

```
huawei(config)#ospf 1
huawei(config-ospf-1)#area 100
huawei(config-ospf-1-area-0.0.0.100)#network 10.50.50.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.100)#network 10.10.10.0 0.0.0.0
huawei(config-ospf-1-area-0.0.0.100)#return
```

Step 4 Configure the remote LDP session.

Configure the remote LDP session from the MA5800 to PE3 (LSR ID: 10.3.3.3) and PE4 (LSR ID: 10.4.4.4) respectively. Name the sessions **to_pe3** and **to_pe4** respectively.

```
huawei(config)#mpls ldp remote-peer to_pe3
huawei(config-mpls-ldp-remote-to_pe3)#remote-ip 10.3.3.3
huawei(config-mpls-ldp-remote-to_pe3)#remote-ip auto-dod-request
huawei(config-mpls-ldp-remote-to_pe3)#quit
huawei(config)#mpls ldp remote-peer to_pe4
huawei(config-mpls-ldp-remote-to_pe4)#remote-ip 10.4.4.4
huawei(config-mpls-ldp-remote-to_pe4)#remote-ip auto-dod-request
huawei(config-mpls-ldp-remote-to_pe4)#quit
```

Step 5 Configure a VSI.

1. Add a VSI.

Create a VSI named **hsi**. Set the signaling protocol to LDP and VSI ID to 1.

```
huawei(config)#vsi hsi
huawei(config-vsi-hsi)#pwsignal ldp
huawei(config-vsi-hsi-ldp)#vsi-id 1
```

2. (Optional) Configure the attributes of VSI.

Configure basic attributes of VSI as required, including the encapsulation type, control word, MTU value, and traffic suppression policy. In the following example, the control word is enabled and default values are used for other parameters.

```
huawei(config-vsi-hsi)#control-word
```

Step 6 Configure PWs.

Create two PWs with IDs 1 and 2. Set the service type to **vpls**, the remote IP addresses to **10.3.3.3** and **10.4.4.4** respectively, and encapsulation type to **ethernet tagged**. Enable the control word, and set the receive labels of dynamic PW to **10240** and **10250** respectively.

```
huawei(config)#pw para pwindex 1
huawei(config-pw-para-index-1)#service-type vpls
huawei(config-pw-para-index-1)#pwid 1
huawei(config-pw-para-index-1)#peer-address 10.3.3.3
huawei(config-pw-para-index-1)#pw-type ethernet tagged
huawei(config-pw-para-index-1)#control-word enable
huawei(config-pw-para-index-1)#dyn-receive-label 10240
huawei(config-pw-para-index-1)#quit
```

```
huawei(config)#pw-para pwindex 2
huawei(config-pw-para-index-2)#service-type vpls
huawei(config-pw-para-index-2)#pwid 2
huawei(config-pw-para-index-2)#peer-address 10.4.4.4
huawei(config-pw-para-index-2)#pw-type ethernet tagged
huawei(config-pw-para-index-2)#control-word enable
huawei(config-pw-para-index-2)#dyn-receive-label 10250
huawei(config-pw-para-index-2)#quit
```

Step 7 Bind PW and VSI.

Dynamically bind PW1 and PW2 to the VSI named **hsi** to establish the VPLS PW service.

```
huawei(config)#vsi hsi
huawei(config-vsi-hsi)#pwsignal ldp
huawei(config-vsi-hsi-ldp)#vsi-pw-binding pwindex 1
huawei(config-vsi-hsi-ldp)#vsi-pw-binding pwindex 2
```

Step 8 Bind AC and VSI.

Bind VLAN 100 to the VSI named hsi, so that the Internet access service packets of VLAN 100 can be forwarded in the VSI.

```
huawei(config-vsi-hsi)#vsi-ac-binding vlan 100
```

----End

Result

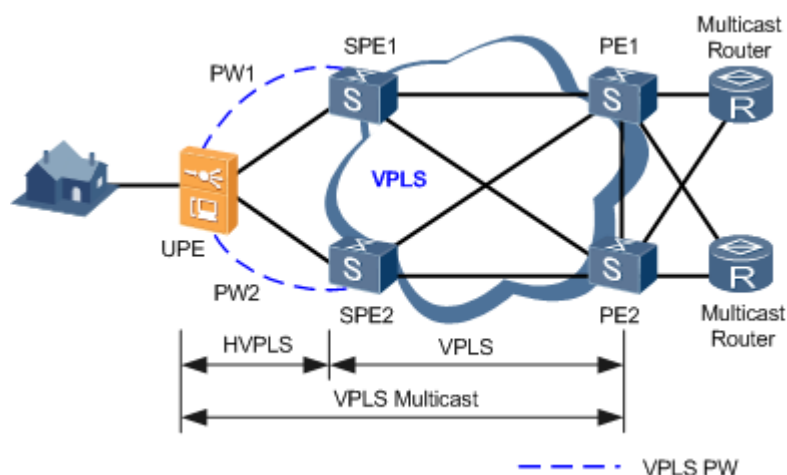
1. A user performs PPPoE dialup. A PADI packet is transmitted upstream.
2. The OLT maps the PADI packet to VSI based on SVLAN carried in the packet and broadcasts the packet on two PWs. At the same time, the OLT learns user's MAC address.
3. After receiving the PADI packet, two BRAS devices respond with PPPOE active discovery offer (PADO) packets in random delay mode.
4. After receiving the PADO packets from PWs, the OLT learns the MAC address carried in the packets from PWs and forwards the packets to the user.
5. The user receives two PADO packets at different time and only responds to the first received PADO packet to establish a PPPoE session.
6. The OLT forwards subsequent PPPOE active discovery request (PADR) and PPPOE active discovery session-confirmation (PADS) packets based on learnt MAC addresses.

9.3.6.2 Configuration Example of the VPLS Multicast Service

In the networking for multicast services, VPLS deployed on the MA5800 enables the MA5800 to be dual homed to AGS devices (aggregation switches), which ensures network reliability.

Application Context

In the VPLS network, multicast services are still deployed based on multicast VLAN other than based on VSI (VPLS instance). The multicast VLAN is bound to VSI for carrying multicast services over the VPLS network, including upstream IGMP packets and downstream multicast traffic streams.

Figure 9-54 Networking for the VPLS multicast service

As shown in **Figure 9-54**:

- The MA5800, functioning as a UPE (underlayer PE), is located on the edge network of HVPLS. In the downstream direction, the MA5800 accesses multicast users through multicast VLAN whose IGMP mode is proxy or snooping. In the upstream direction, the MA5800 is dual homed to two AGS devices that serve as SPEs (superstratum PEs) through two PWs. The same VSI is set up on the MA5800 and AGS and the two upstream PWs belong to the VSI.
- Multiple AGS devices form a VPLS core bearer network. The AGS devices learn the VPLS multicast forwarding table and duplicate multicast traffic based on VPLS PW connections. Two edge AGS devices functioning as SPEs in the downstream direction access the UPE on the edge network, and two edge AGS devices functioning as PEs in the upstream direction terminate VPLS and are connected to multicast routers.
- Two multicast routers back up each other and import multicast traffic streams from the multicast source to the VPLS bearer network.

NOTE

Currently, a maximum of two PWs are supported for VPLS multicast services and both two PWs are used for transmitting multicast packets upstream.

Prerequisite

The MA5800 has been configured with multicast VLAN 100-based multicast traffic streams, and corresponding configurations have been performed on the HG. The configurations are similar to those for common multicast services. The difference is that multicast upstream ports do not need to be configured for VPLS multicast services and the default mode is used for the multicast upstream ports.

Data Plan

Table 9-10 provides the key data plan for the MA5800.

Table 9-10 Key data plan

Configuration Item	Data	Remarks	Requirement on SPE1 and SPE2
MPLS	- LSR ID: 10.10.10.10 - VLAN: 4001	MPLS must be enabled at three layers. - MPLS must be enabled globally. - MPLS must be enabled for VLAN. - MPLS must be enabled at VLAN interfaces.	The LSR ID must be unique on the entire network and MPLS must be enabled.
LDP	- MPLS LDP is enabled. - Split horizon is enabled.	MPLS LDP must be enabled at two layers. - MPLS LDP must be enabled globally. - MPLS LDP must be enabled at VLAN interfaces.	MPLS LDP is enabled. The remote LDP session to the MA5800 is configured on SPE1 and SPE2.
Routing protocol	The Open Shortest Path First (OSPF) protocol is used.	Ensure that the Layer 3 interfaces on the MA5800 and those on SPE1 and SPE2 can ping each other.	Layer 3 interfaces and routes are configured on SPE1 and SPE2. Ensure that the Layer 3 interfaces and loopback interfaces on SPE1 and SPE2 and those on the MA5800 can ping each other.
VPLS PW	- PW ID: 1 and 2 - Service type: vpls - Encapsulation type: ethernet tagged - The control word is enabled.	L2VPN must be enabled. On the MA5800, PW1 and PW2 are created for SPE1 and SPE2 respectively.	The LDP VPLS is supported. VPLS PWs to the MA5800 are configured on SPE1 and SPE2, and attributes of PWs are consistent with those on the MA5800.

Configuration Item	Data	Remarks	Requirement on SPE1 and SPE2
VSI	- PW1 and PW2 are bound to VSI. - Multicast service VLAN 100 is bound to VSI.	Multicast VLAN is bound through VSI to map VLAN to the VPLS domain, so that multicast service packets can be broadcast in the VPLS domain.	VSI is configured on SPE1 and SPE2 and the VSI ID must bind the corresponding PW.

Procedure

Step 1 Configure the basic MPLS.

1. Configure a loopback interface.

Set the ID of the loopback interface to **0** and its IP address to **10.10.10.10/32**.

```
huawei(config)#interface loopback 0
huawei(config-if-loopback0)#ip address 10.10.10.10 32
huawei(config-if-loopback0)#quit
```

2. Configure the MPLS LSR-ID. Use the IP address of loopback interface 0 as the LSR ID.

```
huawei(config)#mpls lsr-id 10.10.10.10
```

3. Enable MPLS globally.

Trigger LDP by the IP address of the host to set up an LSP.

```
huawei(config)#mpls
huawei(config-mpls)#lsp-trigger host
huawei(config-mpls)#quit
```

4. Enable the L2VPN function.

```
huawei(config)#mpls l2vpn
```

5. Enable the LDP function globally and enable the split horizon policy.

```
huawei(config)#mpls ldp
huawei(config-mpls-ldp)#outbound peer all split-horizon
huawei(config-mpls-ldp)#quit
```

Step 2 Configure VLAN, and enable MPLS for VLAN and VLAN interfaces.

1. Add VLAN 4001 for forwarding MPLS packets and add two upstream ports to it.

```
huawei(config)#vlan 4001 smart
huawei(config)#port vlan 4001 0/9/0
huawei(config)#port vlan 4001 0/9/1
```

2. Set the IP address of VLAN interface 4001 to **10.50.50.50/24** and enable MPLS LDP for the VLAN interface.

```
huawei(config)#interface vlanif 4001
huawei(config-if-vlanif4001)#ip address 10.50.50.50 24
huawei(config-if-vlanif4001)#mpls
huawei(config-if-vlanif4001)#mpls ldp
huawei(config-if-vlanif4001)#quit
```

Step 3 Configure routes.

VPLS has no special requirements on routing policy. You can use static route, RIP, or OSPF policy. In the following example, OSPF is used.

Set the OSPF process ID to **100** and OSPF area ID to **1**. In addition, configure the interfaces (VLAN interface and loopback interface) that run OSPF and configure the areas of the interfaces.

```
huawei(config)#ospf 1
huawei(config-ospf-1)#area 100
huawei(config-ospf-1-area-0.0.0.100)#network 10.50.50.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.100)#network 10.10.10.10 0.0.0.0
huawei(config-ospf-1-area-0.0.0.100)#return
```

Step 4 Configure the remote LDP session.

Configure the remote LDP session from the MA5800 to SPE1 (LSR ID: 10.1.1.1) and SPE2 (LSR ID: 10.2.2.2) respectively. Name the sessions **to_spe1** and **to_spe2** respectively.

```
huawei(config)#mpls ldp remote-peer to_spe1
huawei(config-mpls-ldp-remote-to_spe1)#remote-ip 10.1.1.1
huawei(config-mpls-ldp-remote-to_spe1)#remote-ip auto-dod-request
huawei(config-mpls-ldp-remote-to_spe1)#quit
huawei(config)#mpls ldp remote-peer to_spe2
huawei(config-mpls-ldp-remote-to_spe2)#remote-ip 10.2.2.2
huawei(config-mpls-ldp-remote-to_spe2)#remote-ip auto-dod-request
huawei(config-mpls-ldp-remote-to_spe2)#quit
```

Step 5 Configure a VSI.

1. Add a VSI.

Create a VSI named **multicast**. Set the signaling protocol to **LDP** and VSI ID to **1**.

```
huawei(config)#vsi multicast
huawei(config-vsi-multicast)#pwsignal ldp
huawei(config-vsi-multicast-ldp)#vsi-id 1
```

2. (Optional) Disable the suppression of the unknown multicast of the VSI.

If the VSI unknown multicast suppression is enabled, you need to configure this step. Otherwise, packet loss will occur in the multicast services.

```
huawei(config-vsi-multicast)#undo traffic-suppress multicast
```

3. (Optional) Configure the attributes of VSI.

Configure basic attributes of VSI as required, including the encapsulation type, control word, and MTU value. In the following example, the control word is enabled and default values are used for other parameters.

```
huawei(config-vsi-multicast)#control-word
```

Step 6 Configure PWs.

Create two PWs with IDs 1 and 2. Set the service type to **vpls**, the remote IP addresses to **10.1.1.1** and **10.2.2.2** respectively, and encapsulation type to **ethernet tagged**. Enable the control word, and set the receive labels of dynamic PW to **10240** and **10250** respectively.

```
huawei(config)#pw-para pwindex 1
huawei(config-pw-para-index-1)#service-type vpls
huawei(config-pw-para-index-1)#pwid 1
```

```
huawei(config-pw-para-index-1)#peer-address 10.1.1.1
huawei(config-pw-para-index-1)#pw-type ethernet tagged
huawei(config-pw-para-index-1)#control-word enable
huawei(config-pw-para-index-1)#dyn-receive-label 10240
huawei(config-pw-para-index-1)#quit
huawei(config)#pw-para pwindex 2
huawei(config-pw-para-index-2)#service-type vpls
huawei(config-pw-para-index-2)#pwid 2
huawei(config-pw-para-index-2)#peer-address 10.2.2.2
huawei(config-pw-para-index-2)#pw-type ethernet tagged
huawei(config-pw-para-index-2)#control-word enable
huawei(config-pw-para-index-2)#dyn-receive-label 10250
huawei(config-pw-para-index-2)#quit
```

Step 7 Bind PW and VSI.

Dynamically bind PW1 and PW2 to the VSI named multicast to establish the VPLS PW service.

```
huawei(config)#vsi multicast
huawei(config-vsi-multicast)#pwsignal ldp
huawei(config-vsi-multicast-ldp)#vsi-pw-binding pwindex 1
huawei(config-vsi-multicast-ldp)#vsi-pw-binding pwindex 2
```

Step 8 Bind AC and VSI.

Bind multicast VLAN 100 to the VSI named multicast, so that the multicast service packets of VLAN 100 can be forwarded in VSI.

- The same multicast VLAN cannot be bound to the VPLS instance and PW at the same time.
- The same restrictions are set for binding multicast VLANs and VSI as those for binding unicast VLANs and VSI. That is, when the VPLS encapsulation type is raw, one VSI can only be bound to a multicast VLAN; when the VPLS encapsulation type is tag, one VSI can be bound to multiple multicast VLANs.

```
huawei(config-vsi-multicast)#vsi-ac-binding vlan 100
```

----End

Result

1. A user orders a multicast program. An IGMP packet is transmitted upstream.
2. The MA5800 broadcasts the IGMP packet over two upstream PWs which serve as the multicast upstream ports of the multicast VLAN.
3. On the AGS devices, VPLS exchange is performed on the IGMP packet. The AGS devices learn the VPLS multicast forwarding table and duplicate multicast traffic based on VPLS PW connections.
4. Finally, multicast traffic streams are transmitted over one PW. The MA5800 forwards the multicast traffic streams to the corresponding user port based on the local multicast forwarding table. Then the user can watch the multicast program normally.

9.3.6.3 Configuration Example of the VPLS Enterprise Private Line Service

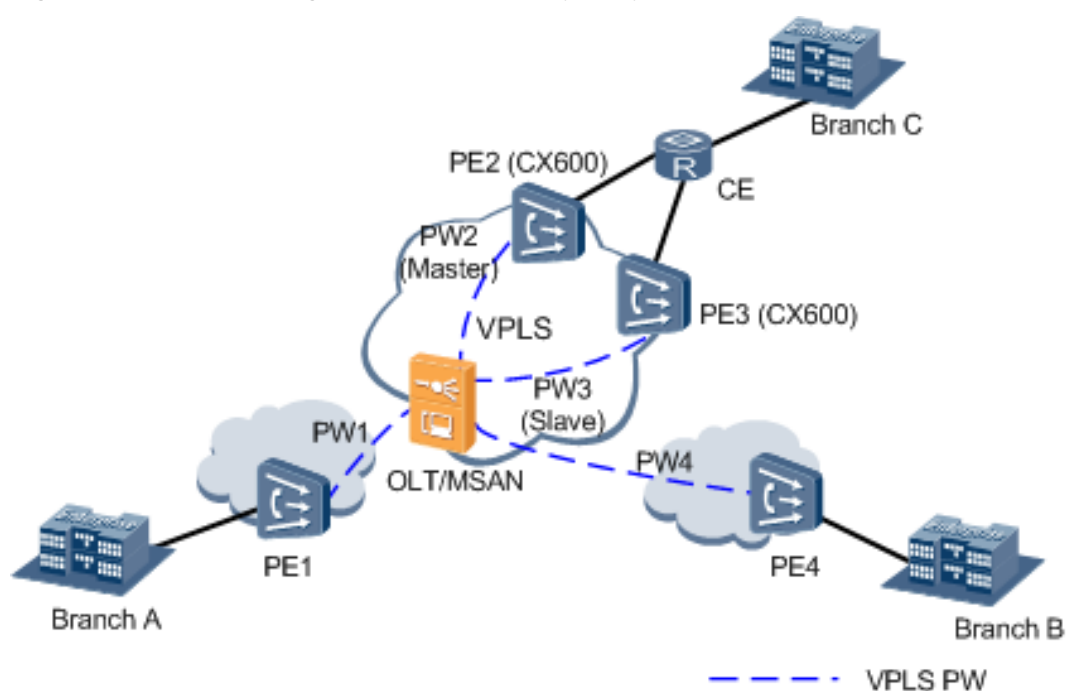
This topic describes how to configure the enterprise private line service when the VPLS networking is used at the access and aggregation layers.

Application Context

As shown in [Figure 9-55](#), branch offices of an enterprise access the VPLS network through a CE or PE. By deploying VPLS PWs between PEs, the service provider can provide Ethernet-based multipoint services to enterprise users over the MPLS backbone network and achieve emulation of the local area network (LAN). For important branch offices (for example, branch C in the following figure), PW redundancy is configured to provide protection.

In the following figure, as a key node, the OLT/MSAN (MA5800) exchanges data with PEs (PE1-PE4) through VPLS PWs. For important branch offices, a PW protection group is configured to provide protection. PEs are connected to the OLT/MSAN using Spoke PW.

Figure 9-55 Networking for the VPLS enterprise private line service



Prerequisite

QinQ traffic streams have been configured on PE1-PE4 for the private line service of different branch offices.

NOTE

To configure the Ethernet-based enterprise private line service, you must configure QinQ VLAN-based Ethernet traffic streams on PE1-PE4, and perform corresponding configurations on routers for branch offices of the enterprise. The configurations are the same as those for common QinQ VLAN private line service, which are not described here.

Data Plan

[Table 9-11](#) provides the key data plan for the OLT/MSAN (MA5800).

Table 9-11 Key data plan

Configuration Item	Data	Remarks	Requirement on PE1-PE4
MPLS	- LSR ID: 10.10.10.10 - VLAN: 4001	MPLS must be enabled at three layers. - MPLS must be enabled globally. - MPLS must be enabled for VLAN. - MPLS must be enabled at VLAN interfaces.	The LSR ID must be unique on the entire network and MPLS must be enabled.
LDP	MPLS LDP is enabled.	MPLS LDP must be enabled at three layers. - MPLS LDP must be enabled globally. - MPLS LDP must be enabled at VLAN interfaces.	MPLS LDP is enabled. The remote LDP session to the MA5800 is configured on PE1-PE4.
Routing protocol	The Open Shortest Path First (OSPF) protocol is used.	Ensure that the Layer 3 interfaces on the MA5800 and those on PE1-PE4 can ping each other.	Layer 3 interfaces and routes are configured on PE1-PE4. Ensure that the Layer 3 interfaces and LSR IDs on PE1-PE4 and those on the MA5800 can ping each other.

Configuration Item	Data	Remarks	Requirement on PE1-PE4
VPLS PW	- PW ID: 1, 2, 3, 4 - Service type: vpls - Encapsulation type: ethernet tagged - The control word is enabled. PW protection group: - PW ID: 2, 3 - Working mode: master-slave - The dual receiving function is enabled for PWs.	On the OLT/MSAN, PW1 and PW4 are created for PE1 and PE4 respectively, and PW2 and PW3 are created for PE2 and PE3 respectively. PW2 and PW3 back up each other.	The LDP VPLS is supported, and VPLS PWs to the MA5800 are configured on PE1-PE4, and attributes of PWs are consistent with those on the MA5800.
VSI	- PW1-PW4 are bound to VSI. - Binding mode of PW 1 and PW 4: spoke - VLAN 100 of the private line service is bound to VSI.	VSI binds VLAN and PW to map VLAN to the VPLS domain, so that packets for the enterprise private line service can be broadcast in the VPLS domain.	VSI is configured on PE1-PE4 and the VSI ID must bind the corresponding PW.

Procedure

Step 1 Configure the basic MPLS.

1. Configure a loopback interface.

Set the ID of the loopback interface to **0** and its IP address to **10.10.10.10/32**.

```
huawei(config)#interface loopback 0
huawei(config-if-loopback0)#ip address 10.10.10.10 32
huawei(config-if-loopback0)#quit
```

2. Configure the MPLS LSR-ID. Use the IP address of loopback interface 0 as the LSR ID.

```
huawei(config)#mpls lsr-id 10.10.10.10
```

3. Enable MPLS globally.

Trigger LDP by the IP address of the host to set up an LSP.

```
huawei(config)#mpls
huawei(config-mpls)#lsp-trigger host
huawei(config-mpls)#quit
```

4. Enable the L2VPN function.

```
huawei(config)#mpls l2vpn
```

5. Enable LDP globally.

```
huawei(config)#mpls ldp
huawei(config-mpls-ldp)#quit
```

Step 2 Configure VLAN, and enable MPLS for VLAN and VLAN interfaces.

1. Add VLAN 4001 for forwarding MPLS packets and add four upstream ports to it.

```
huawei(config)#vlan 4001 smart
huawei(config)#port vlan 4001 0/9 0
huawei(config)#port vlan 4001 0/9 1
huawei(config)#port vlan 4001 0/9 2
huawei(config)#port vlan 4001 0/9 3
```

2. Set the IP address of VLAN interface 4001 to **10.50.50.50/24** and enable MPLS LDP for the VLAN interface.

```
huawei(config)#interface vlanif 4001
huawei(config-if-vlanif4001)#ip address 10.50.50.50 24
huawei(config-if-vlanif4001)#mpls
huawei(config-if-vlanif4001)#mpls ldp
huawei(config-if-vlanif4001)#quit
```

Step 3 Configure routes.

VPLS has no special requirements on routing policy. You can use static route, RIP, or OSPF policy. In the following example, OSPF is used.

Set the OSPF process ID to **100** and OSPF area ID to **1**. In addition, configure the interfaces (VLAN interface and loopback interface) that run OSPF and configure the areas of the interfaces.

```
huawei(config)#ospf 1
huawei(config-ospf-1)#area 100
huawei(config-ospf-1-area-0.0.0.100)#network 10.50.50.0 0.0.0.255
huawei(config-ospf-1-area-0.0.0.100)#network 10.10.10.0 0.0.0.0
huawei(config-ospf-1-area-0.0.0.100)#return
```

Step 4 Configure the remote LDP session.

Configure the remote LDP session from the MA5800 to PE1 (LSR ID: 10.5.5.5), PE2 (LSR ID: 10.2.2.2), PE3 (LSR ID: 10.3.3.3), and PE4 (LSR ID: 10.4.4.4) respectively. Name the sessions **to_pe1**, **to_pe2**, **to_pe3**, and **to_pe4** respectively.

```
huawei(config)#mpls ldp remote-peer to_pe1
huawei(config-mpls-ldp-remote-to_pe1)#remote-ip 10.5.5.5
huawei(config-mpls-ldp-remote-to_pe1)#remote-ip auto-dod-request
huawei(config-mpls-ldp-remote-to_pe1)#quit
huawei(config)#mpls ldp remote-peer to_pe2
huawei(config-mpls-ldp-remote-to_pe2)#remote-ip 10.2.2.2
huawei(config-mpls-ldp-remote-to_pe2)#remote-ip auto-dod-request
huawei(config-mpls-ldp-remote-to_pe2)#quit
huawei(config)#mpls ldp remote-peer to_pe3
huawei(config-mpls-ldp-remote-to_pe3)#remote-ip 10.3.3.3
huawei(config-mpls-ldp-remote-to_pe3)#remote-ip auto-dod-request
huawei(config-mpls-ldp-remote-to_pe3)#quit
```

```
huawei(config)#mpls ldp remote-peer to_pe4
huawei(config-mpls-ldp-remote-to_pe4)#remote-ip 10.4.4.4
huawei(config-mpls-ldp-remote-to_pe4)#remote-ip auto-dod-request
huawei(config-mpls-ldp-remote-to_pe4)#quit
```

Step 5 Configure VSI.

1. Add a VSI.

Create a VSI named **enterprise_vpn**. Set the signaling protocol to **LDP** and VSI ID to **1**.

```
huawei(config)#vsi enterprise_vpn
huawei(config-vsi-enterprise_vpn)#pwsignal ldp
huawei(config-vsi-enterprise_vpn-ldp)#vsi-id 1
```

2. (Optional) Configure the attributes of VSI.

Configure basic attributes of VSI as required, including the encapsulation type, control word, MTU value, and traffic suppression policy. In the following example, the control word is enabled and default values are used for other parameters.

```
huawei(config-vsi-enterprise_vpn)#control-word
```

Step 6 Configure PWs.

Create four PWs with IDs 1-4. Set the service type to **vpls**, the remote IP addresses to the IP addresses of PE1-PE4, and encapsulation type to **ethernet tagged**. Enable the control word, and set the receive labels of dynamic PW to **10240**, **10250**, **10260**, and **10270** respectively.

```
huawei(config)#pw para pwindex 1
huawei(config-pw-para-index-1)#service-type vpls
huawei(config-pw-para-index-1)#pwid 1
huawei(config-pw-para-index-1)#peer-address 10.5.5.5
huawei(config-pw-para-index-1)#pw-type ethernet tagged
huawei(config-pw-para-index-1)#control-word enable
huawei(config-pw-para-index-1)#dyn-receive-label 10240
huawei(config-pw-para-index-1)#quit
huawei(config)#pw para pwindex 2
huawei(config-pw-para-index-2)#service-type vpls
huawei(config-pw-para-index-2)#pwid 2
huawei(config-pw-para-index-2)#peer-address 10.2.2.2
huawei(config-pw-para-index-2)#pw-type ethernet tagged
huawei(config-pw-para-index-2)#control-word enable
huawei(config-pw-para-index-2)#dyn-receive-label 10250
huawei(config-pw-para-index-2)#quit
huawei(config)#pw para pwindex 3
huawei(config-pw-para-index-3)#service-type vpls
huawei(config-pw-para-index-3)#pwid 3
huawei(config-pw-para-index-3)#peer-address 10.3.3.3
huawei(config-pw-para-index-3)#pw-type ethernet tagged
huawei(config-pw-para-index-3)#control-word enable
huawei(config-pw-para-index-3)#dyn-receive-label 10260
huawei(config-pw-para-index-3)#quit
huawei(config)#pw para pwindex 4
huawei(config-pw-para-index-4)#service-type vpls
huawei(config-pw-para-index-4)#pwid 4
huawei(config-pw-para-index-4)#peer-address 10.4.4.4
huawei(config-pw-para-index-4)#pw-type ethernet tagged
huawei(config-pw-para-index-4)#control-word enable
huawei(config-pw-para-index-4)#dyn-receive-label 10270
huawei(config-pw-para-index-4)#quit
```

Step 7 Bind PW and VSI.

Dynamically bind PW 1 and PW 4 in spoke mode, and dynamically bind PW 2 and PW 3 to the VSI named **enterprise_vpn** to establish the VPLS PW service. The

spoke mode is used to identify the peer is a user-side PE, and split horizon is not performed between PWs.

```
huawei(config)#vsi enterprise_vpn
huawei(config-vsi-enterprise_vpn)#pwsignal ldp
huawei(config-vsi-enterprise_vpn-ldp)#vsi-pw-binding pwindex 1 spoke
huawei(config-vsi-enterprise_vpn-ldp)#vsi-pw-binding pwindex 2
huawei(config-vsi-enterprise_vpn-ldp)#vsi-pw-binding pwindex 3
huawei(config-vsi-enterprise_vpn-ldp)#vsi-pw-binding pwindex 4 spoke
```

Step 8 Configure VPLS PW protection.

Configure PW2 and PW3 as a PW protection group named **pg_pw**. Set the working mode to master-slave and enable the dual receiving function for PWs. In the protection group enabled with dual receiving, two PWs are always allowed to receive traffic. In this way, when the remote device performs traffic switching, the traffic will not be dropped.

```
huawei(config)#vsi enterprise_vpn
huawei(config-vsi-enterprise_vpn)#pwsignal ldp
huawei(config-vsi-enterprise_vpn-ldp)#protect-group pg_pw
huawei(config-vsi-enterprise_vpn-ldp-group-pg_pw)#pw-protect primary-pw pwindex 2 secondary-pw pwindex 3
huawei(config-vsi-enterprise_vpn-ldp-group-pg_pw)#protect-mode master
huawei(config-vsi-enterprise_vpn-ldp-group-pg_pw)#stream-dual-receiving
```

Step 9 Bind AC and VSI.

Bind QinQ VLAN 100 to the VSI named enterprise_vpn, so that the enterprise private line service packets can be forwarded in the VSI.

```
huawei(config-vsi-enterprise_vpn)#vsi-ac-binding vlan 100
```

----End

Result

As shown in [Figure 9-55](#), the private networks distributed in different branches can establish point-to-multipoint communication with each other and various services can be provisioned between these private networks. When a PE which branch C is connected to is faulty, services can be automatically switched to another PE and therefore services are not affected.

9.4 VRF

Virtual route forwarding instance (VRF) is a mechanism in which a device works as multiple virtual routing devices. After the Layer 3 interfaces of the device are divided into different VRFs, multiple route forwarding instances can be emulated on the device.

9.4.1 Introduction to VRF

Definition

The key of the virtual route forwarding (VRF) lies in VR, which is equivalent to implementing the functions of multiple virtual routing devices one routing device. VRF is suitable for GPON users.

Purpose

The MA5800 categorizes VRFs by VLANs to provide L3VPN solutions. All the packets or related protocols on the Layer 3 interface of a VRF are processed only in this VRF, which is unrelated to other VRFs. In this way, the services or users can be isolated, and the IP addresses can be saved.

Multiple virtual routing devices can be created on the MA5800. That is, multiple L3VPNs can be established to implement the Layer 3 isolation and independent packet forwarding among different VRFs. Moreover, in different VRFs, the IP address can be reused, and also DHCP relay multi-instances, routing multi-instances, and independent route forwarding tables are supported.

VRF has two application scenarios:

- When the triple play service is provisioned to GPON access users, different services are isolated from each other by VRF, and all services of the device are carried and go upstream by the same physical link. One VR can be bound to each VLANIF interface, and the upstream port belongs to multiple Layer 3 interfaces. Different VRs are bound to different VLANIF interfaces, and each VR forwards data according to the route learned by this VR.
- When the triple play service is provisioned to GPON access users, different services are isolated from each other by VRF, and all services of the device are carried and go upstream by two or more physical links. The links in this case are in the Layer 3 mode, and different services are isolated from each other by VRF.

The difference of the two scenarios is that dual or multiple links are adopted for upstream transmission in scenario 2, where the effect of different VRs going different "ways" is more vivid.

9.4.2 VRF Principle

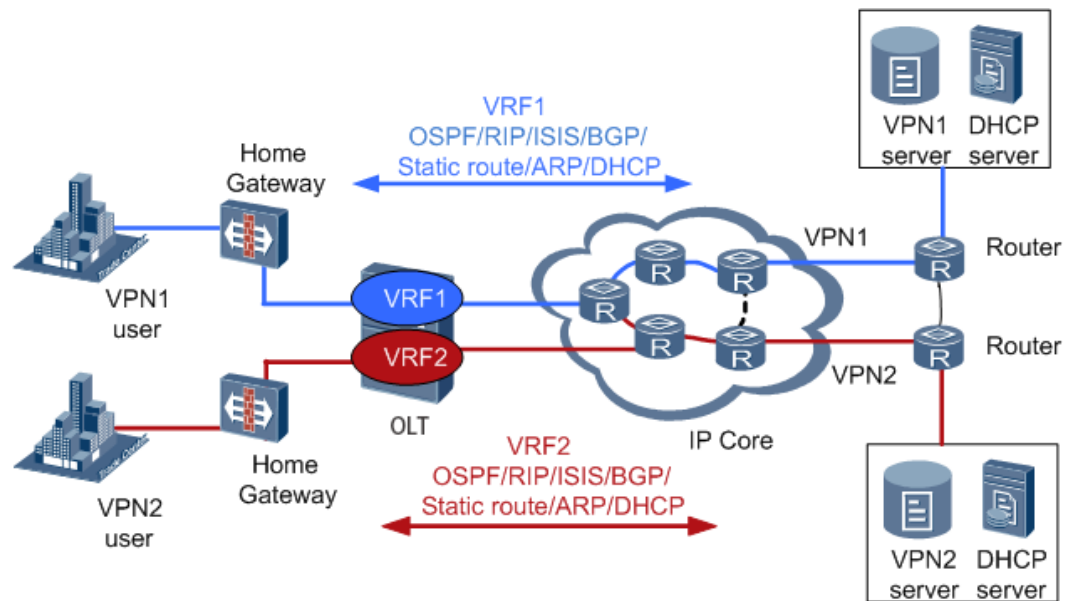
VRF Compatibility

The VRF architecture is compatible with the virtual private routed network (VPRN) architecture as defined in RFC2764.

VRF Architecture

VRF is an architecture of IP networks, as shown in [Figure 9-56](#). When users are isolated by service types or ISPs, or the users of different VPNs are prohibited from communicating with each other, multiple L3VPNs must be established in an IP network.

Figure 9-56 VRF architecture



The MA5800 VRF supports the following functions:

- Creating a VRF instance
You can create a VRF instance and set the name of the VRF as the reference flag through the CLI.
- Adding the VLAN Layer 3 interface and the loopback interface into a VRF instance
 - The MA5800 differentiates VRFs by the VLAN Layer 3 interfaces. A VRF contains one or more VLAN Layer 3 interfaces. When receiving or transmitting packets, any VLAN Layer 3 interface that belongs to the VRF must use the Layer 3 route forwarding table of the VRF. Moreover, the packets in the VRF must be forwarded between these VLAN Layer 3 interfaces and cannot be forwarded to any other VLAN Layer 3 interfaces that do not belong to the VRF.
 - After a loopback interface is bound with the VRF instance, the loopback interface can process all the routing protocols in the VRF.
 - The IP addresses configured in the VLAN Layer 3 interfaces of different VRFs can be identical, but the IP addresses in the same VRF cannot be identical.
- Isolating ARP in a VRF
The ARP in different VRFs is isolated, but the user IP addresses in different VRFs can be identical.
- Supporting independent ISIS, OSPF, RIP, or BGP routing protocol process for different VRFs
- Supporting the Layer 3 DHCP relay or DHCP proxy in a VRF
The MA5800 supports the DHCP configuration based on the VLAN to implement the DHCP relay or DHCP proxy function in the VRF.
- Supporting the ping and trace route functions in a VRF
 - Ping and trace route are the basic network maintenance means.

- The ping function is used to check the connectivity and reachability of a remote host by sending the ping packets to the host.
- The trace route function is used to check the network connectivity and locate the network faults by testing the route that the data packets pass through from the host to the destination.

9.4.3 Configuring IPv4 in VPN

This topic describes how to categorize virtual private network (VPN) instances by VLANs, and realize the virtual IPv4 static route forwarding in different VPN instances.

Context

A VPN instance is also called a VPN Routing and Forwarding (VRF) table. VRF is a Layer 3 virtual private network (L3 VPN). VRF is a mechanism in which a device works as multiple virtual routing devices. After the Layer 3 interfaces of the device are divided into different VRFs, multiple route forwarding instances can be emulated on the device.

Multiple virtual routing devices can be created on the access node. That is, multiple L3VPNs can be established to implement the Layer 3 isolation and independent packet forwarding among different VRFs. The access node supports the following VRF functions:

- In different VRF instances, the IP address can be reused. It means that the IP addresses of the Layer 3 interfaces which belong to different VRF instances can be the same.
- The ping and trace route functions are supported in a VRF.
- The users of different VRF instances can obtain the IP addresses through the Dynamic Host Control Protocol (DHCP) relay or the DHCP proxy.
- The static routes and the dynamic routes in a VRF instance do not affect each other, and the routing entry in each VRF instance supports the routing function independently.

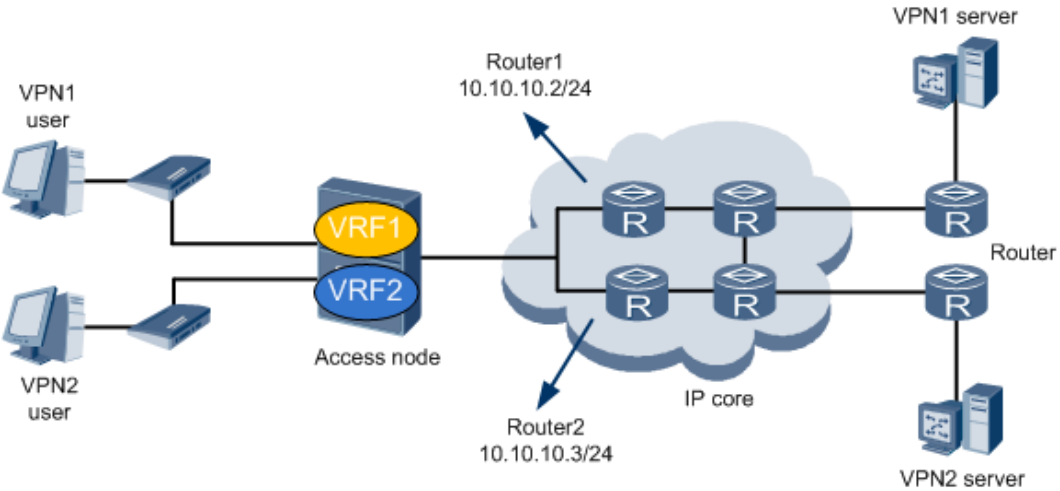
Networking

Figure 9-57 shows an example network for configuring IPv4 in VPN.

The access node categorizes VRF instances by VLANs to provide L3 VPN solutions. In this example, VPN instance VRF1 is categorized by virtual local area network (VLAN) 200, and IPv4 static routes are added in the virtual route forwarding entries of VRF1. The access node selects the routes for the users of VPN1 by querying the routing entries of VRF1. Similarly, VPN instance VRF2 is categorized by VLAN 300 and is used to select the routes for the users of VPN2. The access node implements the Layer 3 isolation and independent packet forwarding through different VRF instances.

This example describes how to configure the function of virtual static route forwarding by adding IPv4 static routes application on the instance. The function of virtual dynamic route forwarding can be realized by enabling the process of the dynamic routing protocols such as the open shortest path first (OSPF), Routing Information Protocol (RIP), intermediate system to intermediate system (IS-IS), and Border Gateway Protocol (BGP) in a VRF instance.

Figure 9-57 Example network for configuring IPv4 in VPN



Data Plan

Table 9-12 provides the data plan for configuring IPv4 in VPN.

Table 9-12 Data plan for configuring IPv4 in VPN

Item	Data
VRF1 (for VPN1)	Name of the VPN instance: vpn1 Route distinguisher (RD) of the VPN instance: 100:1
	Upstream port: 0/9/0 VLAN ID: 200 VLAN type: Smart VPN1 user: - Gigabit-capable passive optical network (GPON) port: 0/2/0 - ONT ID: 0 - GEM Port ID: 0
	IP address of the Layer 3 interface of VLAN 200: 10.10.10.1/24 IP address of router1: 10.10.10.2/24 IP address of the VPN1 server: 10.10.20.1/24
VRF2 (for VPN2)	Name of the VPN instance: vpn2 RD of the VPN instance: 100:2

Item	Data
	Upstream port: 0/9/0 VLAN ID: 300 VLAN type: Smart VPN2 user: • GPON port: 0/2/1 • ONT ID: 1 • GEM Port ID: 1
	IP address of the Layer 3 interface of VLAN 300: 10.10.10.1/24 IP address of router2: 10.10.10.3/24 IP address of the VPN2 server: 10.10.30.1/24

Procedure

- Configure VRF1 (for VPN1).
 - a. Create a VPN instance of the IPv4 address family.

```
huawei(config)#ip vpn-instance vpn1
huawei(config-vpn-instance-vpn1)#ipv4-family
```
 - b. Configure the RD of the VPN instance.

```
huawei(config-vpn-instance-vpn1-af-ipv4)#route-distinguisher 100:1
huawei(config-vpn-instance-vpn1-af-ipv4)#quit
huawei(config-vpn-instance-vpn1)#quit
```
 - c. Create a smart VLAN and add the upstream port and the service port to it.

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/9 0
huawei(config)#service-port vlan 200 gpon 0/2/0 ont 0 gempport 0 multi-service user-8021p
0 user-vlan 200 rx-cttr 5 tx-cttr 5
```
 - d. Associate the Layer 3 interface with the VPN instance.

```
huawei(config)#interface vlanif 200
huawei(config-if-vlanif200)#ip binding vpn-instance vpn1
```

Info: All IPv4 and IPv6 related configurations on this interface are removed.
 - e. Configure the IP address of the VLAN Layer 3 interface.

```
huawei(config-if-vlanif200)#ip address 10.10.10.1 24
huawei(config-if-vlanif200)#quit
```
 - f. Configure the IPv4 static route.

```
huawei(config)#ip route-static vpn-instance vpn1 10.10.20.0 24 10.10.10.2
```
 - g. Save the data.

```
huawei(config)#save
```
- Configure VRF2 (for VPN2).
 - a. Create a VPN instance of the IPv4 address family.

```
huawei(config)#ip vpn-instance vpn2
huawei(config-vpn-instance-vpn2)#ipv4-family
```
 - b. Configure the RD of the VPN instance.

```

huawei(config-vpn-instance-vpn2-af-ipv4)#route-distinguisher 100:2
huawei(config-vpn-instance-vpn2-af-ipv4)#quit
huawei(config-vpn-instance-vpn2)#quit

```

- c. Create a smart VLAN and add the upstream port and the service port to it.

```

huawei(config)#vlan 300 smart
huawei(config)#port vlan 300 0/9 0
huawei(config)#service-port vlan 300 gpon 0/2/1 ont 1 gemport 1 multi-service user-8021p
0 user-vlan 300 rx-cttr 6 tx-cttr 6

```

- d. Associate the Layer 3 interface with the VPN instance.

```

huawei(config)#interface vlanif 300
huawei(config-if-vlanif300)#ip binding vpn-instance vpn2
Info: All IPv4 and IPv6 related configurations on this interface are removed.

```

- e. Configure the IP address of the VLAN Layer 3 interface.

```

huawei(config-if-vlanif300)#ip address 10.10.10.1 24
huawei(config-if-vlanif300)#quit

```

- f. Configure the IPv4 static route.

```

huawei(config)#ip route-static vpn-instance vpn2 10.10.30.0 24 10.10.10.3

```

- g. Save the data.

```

huawei(config)#save

```

----End

Result

Run the **display ip vpn-instance** command to query the VPN configuration.

```

huawei(config)#display ip vpn-instance
{ <cr>|import-vt<K>|interface<K>|tunnel-info<K>|verbose<K>|vpn-instance-name<S><
Length 1-31>|vpn1|vpn2||<K> }:

```

Command:

```
display ip vpn-instance
```

Total VPN-Instances configured : 2

Total IPv4 VPN-Instances configured : 2

Total IPv6 VPN-Instances configured : 0

VPN-Instance Name	RD	Address-family
vpn1	100:1	IPv4
vpn2	100:2	IPv4

Run the following commands to verify that the VRF instances are configured successfully. The two IPv4 static routes are added to the IP routing table of VPN1 and VPN2.

```

huawei(config)#display ip routing-table vpn-instance vpn1
{ <cr>|ip-prefix<K>|prefix<I><X.X.X.X>|protocol<K>|route-number<K>|statistics<K>|table-name<K>|time-
range<K>|verbose<K>||<K> }:

```

Command:

```
display ip routing-table vpn-instance vpn1
```

Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route

Routing Tables: vpn1

Destinations : 3 Routes : 3

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.10.10.0/24	Direct	0	0	D	10.10.10.1	vlanif200
10.10.10.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
10.10.20.0/24	Static	60	0	D	10.10.10.2	vlanif200

```
huawei(config)#display ip routing-table vpn-instance vpn2
{ <cr>|ip-prefix<K>|prefix<I><X.X.X.X>|protocol<K>|route-number<K>|statistics<K>|table-name<K>|time-
range<K>|verbose<K>|<K> }:
```

Command:

```
display ip routing-table vpn-instance vpn2
```

Route Flags: R - relay, D - download to fib, T - to vpn-instance, B - black hole route

Routing Tables: vpn2

Destinations : 3 Routes : 3

Destination/Mask	Proto	Pre	Cost	Flags	NextHop	Interface
10.10.10.0/24	Direct	0	0	D	10.10.10.1	vlanif300
10.10.10.1/32	Direct	0	0	D	127.0.0.1	InLoopBack0
10.10.30.0/24	Static	60	0	D	10.10.10.3	vlanif300

Run the **ping** and **tracert** commands to check the VPN connectivity.

The MA5800 categorizes VRF instances by VLANs to provide L3 VPN solutions, realizing the Layer 3 isolation of users or services.

- For the users of VPN1, the MA5800 selects the routes by querying the routing entries of VPN1. For example, for the packets to be sent to the VPN1 server (with IP address 10.10.20.1), the MA5800 selects its next hop router (with IP address 10.10.10.2) to forward the packets.
- For the users of VPN2, the MA5800 selects the routes by querying the routing entries of VPN2. For example, for the packets to be sent to the VPN2 server (with IP address 10.10.30.1), the MA5800 selects its next hop router (with IP address 10.10.10.3) to forward the packets.
- For the users outside the VPNs, the route to the VPN1 server or the VPN2 server is not available.

Configuration File

Only the configuration files related to the VPN are listed.

```
ip vpn-instance vpn1
ipv4-family
route-distinguisher 100:1
quit
quit
ip vpn-instance vpn2
ipv4-family
route-distinguisher 100:2
quit
quit
interface vlanif200
ip binding vpn-instance vpn1
ip address 10.10.10.1/24
quit
interface vlanif300
ip binding vpn-instance vpn2
ip address 10.10.10.1/24
quit
ip route-static vpn-instance vpn1 10.10.20.0 24 10.10.10.2
ip route-static vpn-instance vpn2 10.10.30.0 24 10.10.10.3
```

9.4.4 Configuring IPv6 in VPN

This topic describes how to categorize virtual private network (VPN) instances by virtual local area networks (VLANs), and implement the virtual IPv6 static route forwarding in different VPN instances.

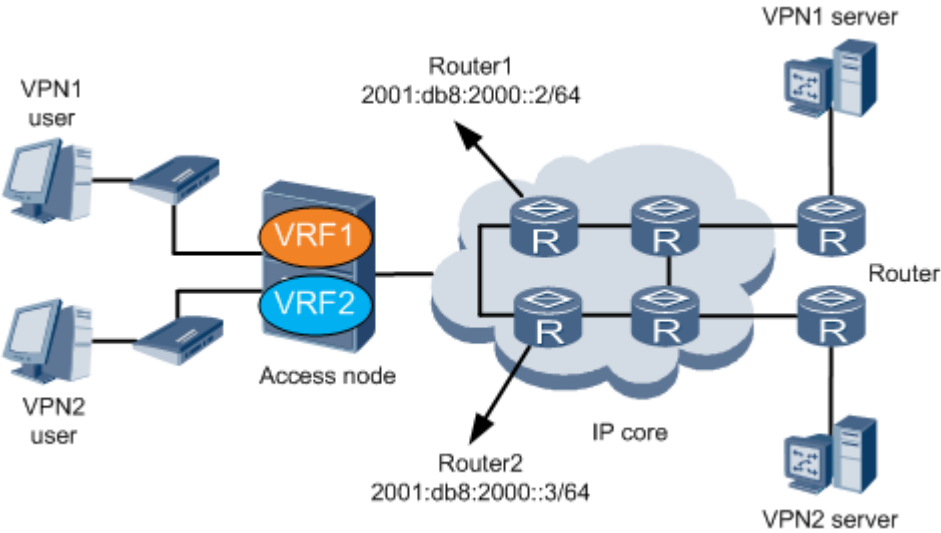
Networking

The access node supports virtual route forwarding (VRF) in the IPv6 network. The VRF principle and functions in the IPv6 network are the same as those in the IPv4 network. [9.4.4 Configuring IPv6 in VPN](#) shows an example network for configuring IPv6 in VPN.

The access node categorizes VRF instances by VLANs to provide L3 VPN solutions. In this example, VPN instance VRF1 is categorized by virtual local area network (VLAN) 200, and IPv6 static routes are added in the virtual route forwarding entries of VRF1. The access node selects the routes for the users of VPN1 by querying the routing entries of VRF1. Similarly, VPN instance VRF2 is categorized by VLAN 300 and is used to select the routes for the users of VPN2. The access node implements the Layer 3 isolation and independent packet forwarding through different VRF instances.

This example describes how to configure the function of virtual static route forwarding by adding IPv6 static routes to a VRF routing table. In addition, virtual dynamic route forwarding can be implemented in a VPN by using BGP4+.

Figure 9-58 IPv6 in VPN networking diagram



Data Plan

[Table 9-13](#) provides the data plan for configuring IPv6 in VPN.

Table 9-13 Data plan for configuring IPv6 in VPN

Item	Data
VRF1 (for VPN1)	Name of the VPN instance: vpn1 Route distinguisher (RD) of the VPN instance: 100:1

Item	Data
	Upstream port: 0/9/0 VLAN ID: 200 VLAN type: Smart VPN1 user: • Gigabit-capable passive optical network (GPON) port: 0/2/0 • ONT ID: 0 • GEM Port ID: 0
	IPv6 address of the Layer 3 interface of VLAN 200: 2001:db8:2000::1/64 IPv6 address of router1: 2001:db8:2000::2/64 IPv6 address of the VPN1 server: 2001:db8:2001::1/64
VRF2 (for VPN2)	Name of the VPN instance: vpn2 Route distinguisher (RD) of the VPN instance: 100:2
	Upstream port: 0/9/0 VLAN ID: 300 VLAN type: Smart VPN2 user: • GPON port: 0/2/1 • ONT ID: 1 • GEM Port ID: 1
	IPv6 address of the Layer 3 interface of VLAN 300: 2001:db8:2000::1/64 IPv6 address of router2: 2001:db8:2000::3/64 IPv6 address of the VPN2 server: 2001:db8:2002::1/64

Procedure

- Configure VRF1 (for VPN1).
 - a. Create a VPN instance of the IPv6 address family.

```
huawei(config)#ip vpn-instance vpn1
huawei(config-vpn-instance-vpn1)#ipv6-family
```
 - b. Configure the RD of the VPN instance.

```
huawei(config-vpn-instance-vpn1-af-ipv6)#route-distinguisher 100:1
```
 - c. (Optional) Configure the IPv6 routing specifications of the VPN instance.

```
huawei(config-vpn-instance-vpn1-af-ipv6)#prefix limit 1000 simply-alert
huawei(config-vpn-instance-vpn1-af-ipv6)#quit
huawei(config-vpn-instance-vpn1)#quit
```
 - d. Create a smart VLAN and add the upstream port and the service port to it.

```
huawei(config)#vlan 200 smart
huawei(config)#port vlan 200 0/9 0
```

```
huawei(config)#service-port vlan 200 gpon 0/2/0 ont 0 gemport 0 multi-service user-8021p  
0 user-vlan 200 rx-cttr 5 tx-cttr 5
```

- e. Associate the Layer 3 interface with the VPN instance.

```
huawei(config)#interface vlanif 200  
huawei(config-if-vlanif200)#ip binding vpn-instance vpn1  
Info: All IPv4 and IPv6 related configurations on this interface are removed.
```

- f. Configure the IPv6 address of the VLAN Layer 3 interface.

```
huawei(config-if-vlanif200)#ipv6 enable  
huawei(config-if-vlanif200)#ipv6 address 2001:db8:2000::1 64  
huawei(config-if-vlanif200)#quit
```

- g. Configure the IPv6 static route.

```
huawei(config)#ipv6 route-static vpn-instance vpn1 2001:db8:2001:: 64 2001:db8:2000::2
```

- h. Save the data.

```
huawei(config)#save
```

- Configure VRF2 (for VPN2).

- a. Create a VPN instance of the IPv6 address family.

```
huawei(config)#ip vpn-instance vpn2  
huawei(config-vpn-instance-vpn2)#ipv6-family
```

- b. Configure the RD of the VPN instance.

```
huawei(config-vpn-instance-vpn2-af-ipv6)#route-distinguisher 100:2
```

- c. (Optional) Configure the IPv6 routing specifications of the VPN instance.

```
huawei(config-vpn-instance-vpn2-af-ipv6)#prefix limit 1000 simply-alert  
huawei(config-vpn-instance-vpn2-af-ipv6)#quit  
huawei(config-vpn-instance-vpn2)#quit
```

- d. Create a smart VLAN and add the upstream port and the service port to it.

```
huawei(config)#vlan 300 smart  
huawei(config)#port vlan 300 0/9 0  
huawei(config)#service-port vlan 300 gpon 0/2/1 ont 1 gemport 1 multi-service user-8021p  
0 user-vlan 300 rx-cttr 6 tx-cttr 6
```

- e. Associate the Layer 3 interface with the VPN instance.

```
huawei(config)#interface vlanif 300  
huawei(config-if-vlanif300)#ip binding vpn-instance vpn2  
Info: All IPv4 and IPv6 related configurations on this interface are removed.
```

- f. Configure the IPv6 address of the VLAN Layer 3 interface.

```
huawei(config-if-vlanif300)#ipv6 enable  
huawei(config-if-vlanif300)#ipv6 address 2001:db8:2000::1 64  
huawei(config-if-vlanif300)#quit
```

- g. Configure the IPv6 static route.

```
huawei(config)#ipv6 route-static vpn-instance vpn2 2001:db8:2002:: 64 2001:db8:2000::3
```

- h. Save the data.

```
huawei(config)#save
```

----End

Result

Run the **display ip vpn-instance** command to query the VPN configurations.

```
huawei(config)#display ip vpn-instance  
{ <cr>|import-vt<K>|interface<K>|tunnel-info<K>|verbose<K>|vpn-instance-name<S><  
Length 1-31>|vpn1|vpn2|<K> }:
```

```
Command:  
display ip vpn-instance
```

```
Total VPN-Instances configured : 2
Total IPv4 VPN-Instances configured : 0
Total IPv6 VPN-Instances configured : 2
```

VPN-Instance Name	RD	Address-family
vpn1	100:1	IPv6
vpn2	100:2	IPv6

Run the following commands to verify that the configurations are successful and the IPv6 static route is added to the IPv6 routing table of VPN1 and VPN2.

```
huawei(config)#display ipv6 routing-table vpn-instance vpn1
{ <cr>|ipv6-prefix<K>|ipv6prefix<IPv6><X:X::X:X>|protocol<K>|route-number<K>|sta
tistics<K>|time-range<K>|verbose<K>||<K> };
```

Command:

```
display ipv6 routing-table vpn-instance vpn1
```

Routing Table : vpn1

Destinations : 4 Routes : 4

```
Destination : 2001:db8:2000::      PrefixLength : 64
NextHop : 2001:db8:2000::1      Preference : 0
Cost : 0      Protocol : Direct
RelayNextHop : ::      TunnelID : 0x0
Interface : vlnif200      Flags : D
```

```
Destination : 2001:db8:2000::1      PrefixLength : 128
NextHop : ::1      Preference : 0
Cost : 0      Protocol : Direct
RelayNextHop : ::      TunnelID : 0x0
Interface : InLoopBack0      Flags : D
```

```
Destination : 2001:db8:2001::      PrefixLength : 64
NextHop : 2001:db8:2000::2      Preference : 60
Cost : 0      Protocol : Static
RelayNextHop : ::      TunnelID : 0x0
Interface : vlnif200      Flags : RD
```

```
Destination : FE80::      PrefixLength : 10
NextHop : ::      Preference : 0
Cost : 0      Protocol : Direct
RelayNextHop : ::      TunnelID : 0x0
Interface : null0      Flags : D
```

```
huawei(config)#display ipv6 routing-table vpn-instance vpn2
{ <cr>|ipv6-prefix<K>|ipv6prefix<IPv6><X:X::X:X>|protocol<K>|route-number<K>|sta
tistics<K>|time-range<K>|verbose<K>||<K> };
```

Command:

```
display ipv6 routing-table vpn-instance vpn2
```

Routing Table : vpn2

Destinations : 4 Routes : 4

```
Destination : 2001:db8:2000::      PrefixLength : 64
NextHop : 2001:db8:2000::1      Preference : 0
Cost : 0      Protocol : Direct
RelayNextHop : ::      TunnelID : 0x0
Interface : vlnif200      Flags : D
```

```
Destination : 2001:db8:2000::1      PrefixLength : 128
NextHop : ::1      Preference : 0
Cost : 0      Protocol : Direct
RelayNextHop : ::      TunnelID : 0x0
Interface : InLoopBack0      Flags : D
```

```
Destination : 2001:db8:2002::      PrefixLength : 64
NextHop : 2001:db8:2000::3      Preference : 60
Cost : 0      Protocol : Static
RelayNextHop : ::      TunnelID : 0x0
Interface : vlnif300      Flags : RD
```

Destination : FE80::	PrefixLength : 10
NextHop : ::	Preference : 0
Cost : 0	Protocol : Direct
RelayNextHop : ::	TunnelID : 0x0
Interface : null0	Flags : D

Run the **ping ipv6** and **tracert ipv6** commands to check the VPN connectivity.

The MA5800 categorizes VRF instances by VLANs to provide L3 VPN solutions, realizing the Layer 3 isolation of users or services.

- For the users of VPN1, the MA5800 selects the routes by querying the routing entries of VPN1. For example, for the packets to be sent to the VPN1 server (with IPv6 address 2001:db8:2001::1), the MA5800 selects its next hop router (with IPv6 address 2001:db8:2000::2) to forward the packets.
- For the users of VPN2, the MA5800 selects the routes by querying the routing entries of VPN2. For example, for the packets to be sent to the VPN2 server (with IPv6 address 2001:db8:2002::1), the MA5800 selects its next hop router (with IPv6 address 2001:db8:2000::3) to forward the packets.
- For the users outside the VPNs, the route to the VPN1 server or the VPN2 server is not available.

Configuration File

Only the configuration files related to the VPN are listed.

```
ip vpn-instance vpn1
ipv6-family
route-distinguisher 100:1
routing-table limit 1000 simply-alert
prefix limit 1000 simply-alert
quit
quit
ip vpn-instance vpn2
ipv6-family
route-distinguisher 100:2
routing-table limit 1000 simply-alert
prefix limit 1000 simply-alert
quit
quit
interface vlanif200
ip binding vpn-instance vpn1
ipv6 enable
ipv6 address 2001:db8:2000::1/64
quit
interface vlanif300
ip binding vpn-instance vpn2
ipv6 enable
ipv6 address 2001:db8:2000::1/64
quit
ipv6 route-static vpn-instance vpn1 2001:db8:2001:: 64 2001:db8:2000::2
ipv6 route-static vpn-instance vpn2 2001:db8:2002:: 64 2001:db8:2000::3
```

9.5 BGP/MPLS IP VPN

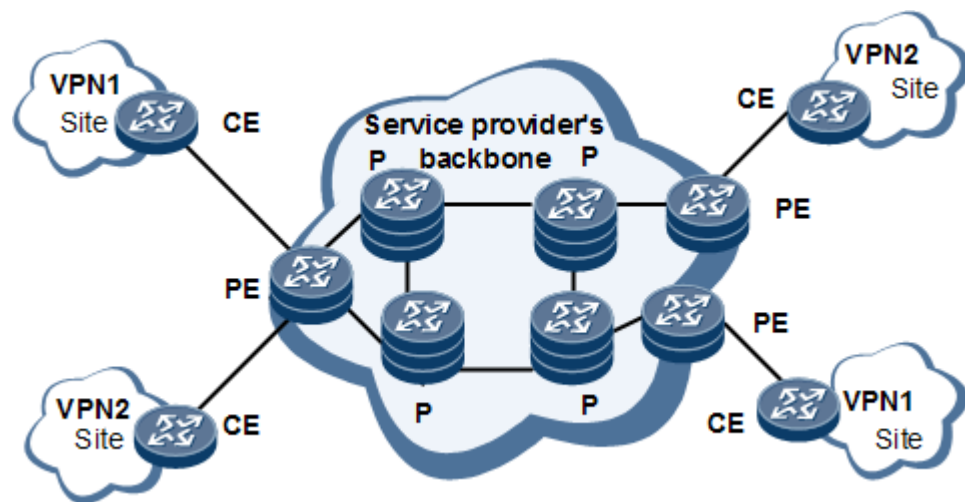
9.5.1 Introduction to BGP/MPLS IP VPN

Definition

A BGP/MPLS IP VPN is a Layer 3 virtual private network (L3VPN), which uses BGP to advertise VPN routes and uses MPLS to forward VPN packets on the IP backbone networks of service providers (SPs).

[Figure 9-59](#) shows the basic model of BGP/MPLS IP VPN.

Figure 9-59 BGP/MPLS IP VPN



As shown in [Figure 9-59](#), a BGP/MPLS IP VPN consists of the following roles:

- **CE:** An edge device on a customer network. A CE provides interfaces that are directly connected to the SP network. A CE can be a router, a switch, or a host. Usually, a CE is unaware of the VPN and does not need to support MPLS.
- **PE:** An edge device on an SP network. A PE is directly connected to a CE. On an MPLS network, PEs process all VPN services. The requirements on the performance of PEs are rather high.
- **P:** A backbone device on an SP network. A P is not directly connected to a CE. Ps only need to possess basic MPLS forwarding capabilities and do not maintain VPN information.

PEs and Ps are managed by SPs. CEs are managed by users, except that the users trust SPs with the management rights.

A PE can connect to multiple CEs. A CE can connect to multiple PEs of the same SP or of different SPs.

Purpose

- MPLS seamlessly integrates the flexibility of IP routing and simplicity of ATM label switching. A connection-oriented control plane is introduced into an MPLS IP network, which enriches the means of managing and operating the

network. On IP networks, MPLS TE has become an important tool in managing network traffic, reducing network congestion, and ensuring QoS.

The VPNs using MPLS IP networks as the backbone networks are highly valued by carriers, and have become an important means of providing value-added services.

- Unlike the IGP, BGP focuses on controlling route transmission and choosing optimal routes instead of discovering and calculating routes. VPNs use public networks to transmit VPN data, and the public networks use an IGP to discover and calculate their routes. The key to constructing a VPN is to control the transmission of VPN routes and choose the optimal routes between two PEs.

BGP uses TCP (with port number 179) as the transport layer protocol, enhancing transmission reliability. VPN routes can be directly exchanged between two PEs with routers located between them.

BGP can append any information to a route as optional BGP attributes. The information is transparently forwarded by BGP devices that cannot identify those attributes. Therefore, VPN routes can be conveniently transmitted between PEs.

When routes are updated, BGP sends only updated routes rather than all routes. This implementation saves the bandwidth consumed by route transmission, making the transmission of a great number of routes over a public network possible.

As an Exterior Gateway Protocol (EGP), BGP is best suited for VPNs that cross the networks of multiple carriers.

9.5.2 BGP/MPLS IP VPN Reference Standards and Protocols

The following table lists the references.

Document No.	Document Name	Protocol Compliance
RFC 2764	A Framework for IP Based Virtual Private Networks	Fully compliant
RFC 2917	A Core MPLS IP VPN Architecture	Fully compliant
RFC 3392	Capabilities Advertisement with BGP-4	Fully compliant
RFC 4026	Provider Provisioned Virtual Private Network (VPN) Terminology	Fully compliant
RFC 4271	BGP-4	Fully compliant
RFC 4364	BGP/MPLS IP Virtual Private Networks (VPNs)	Partially compliant. The Carrier's Carrier is not supported.
RFC 4382	MPLS/BGP Layer 3 Virtual Private Network (VPN) Management Information Base	Fully compliant

Document No.	Document Name	Protocol Compliance
RFC 4577	OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs)	Fully compliant
RFC 4659	BGP-MPLS VPN Extension for IPv6 VPN	Partially compliant. The Carrier's Carrier is not supported.
RFC 4760	Multiprotocol Extensions for BGP-4	Fully compliant
RFC 5668	4-Octet AS Specific BGP Extended Community	Fully compliant

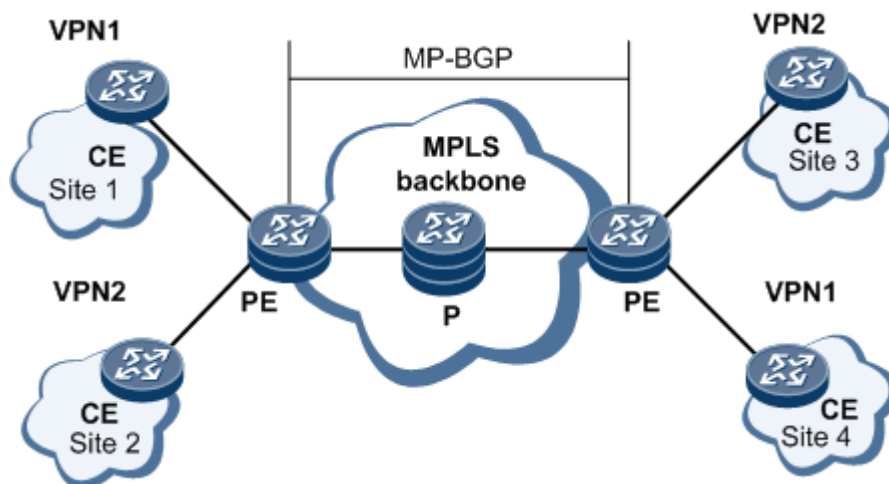
9.5.3 Basic BGP/MPLS IP VPN

Definition

A basic BGP/MPLS IP VPN is an L3VPN network that covers only one carrier's network, which is an MPLS backbone network that does not span multiple ASs, as shown in [Figure 9-60](#). A basic BGP/MPLS IP VPN has the following characteristics:

- Transmits packets using extended BGP.
- Encapsulates and transmits VPN packets over MPLS LSPs serving as public network tunnels.
- Allows a device that can play PE, P, and CE roles to play only one role at a time.

Figure 9-60 Basic BGP/MPLS IP VPN networking



Benefits

BGP/MPLS IP VPN offers the following benefits:

- Enables users to communicate with each other over networks of geographically different regions.
- Ensures the security of VPN user data during transmission over the public network.

9.5.4 Related Concepts for BGP/MPLS IP VPN

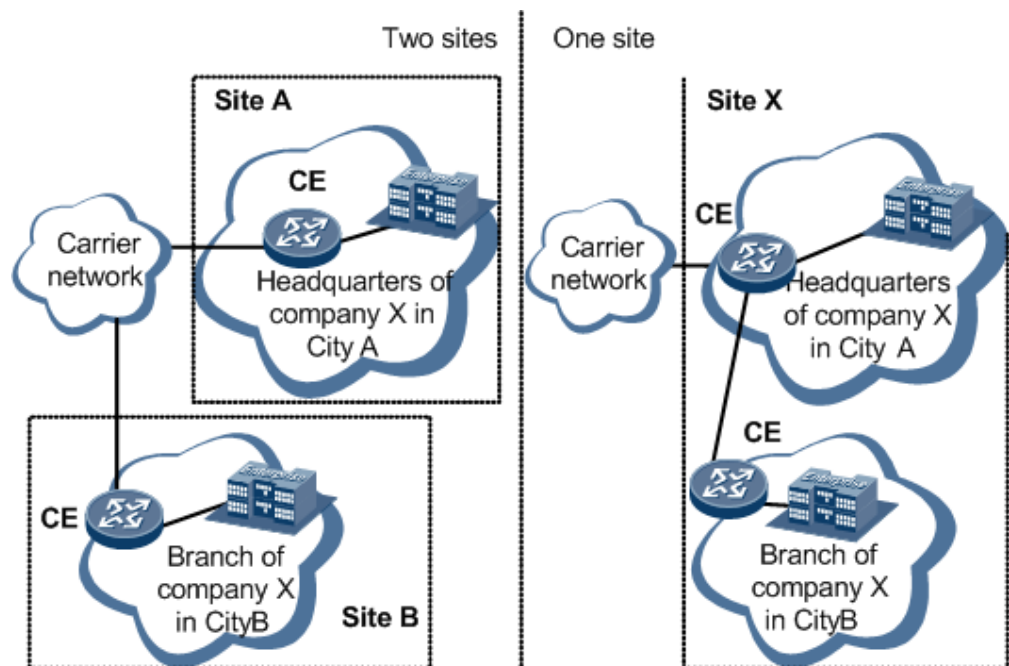
Site

The concept of "site" is frequently mentioned in the VPN technology. The following describes a site from different aspects:

- A site is a group of IP systems that can communicate without using carrier networks.

As shown in [Figure 9-61](#), on the networks of the left side, the headquarters network of company X in City A is a site; the branch network of company X in City B is another site. IP devices within each site can communicate without using the SP network.

Figure 9-61 Schematic diagram of sites



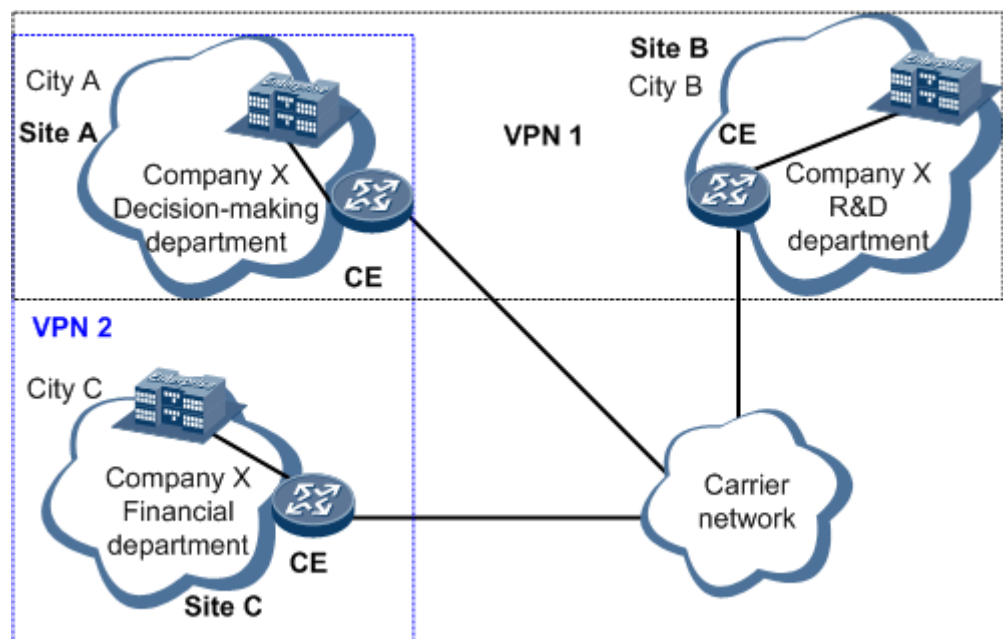
- Sites are classified based on the topological relationships between devices rather than the geographical locations of devices, although devices in a site are geographically adjacent to each other in general. If two geographically separated IP systems are connected over a leased line instead of a carrier network, the two systems compose a site.

As shown in [Figure 9-61](#), if the branch network in City B connects to the headquarters network in City A over a leased line instead of a carrier network, the branch network and the headquarters network compose a site.

- The devices at a site may belong to multiple VPNs. In other words, a site may belong to more than one VPN.

As shown in [Figure 9-62](#), the decision-making department of company X in City A (Site A) is allowed to communicate with the R&D department in City B (Site B) and the financial department in City C (Site C). Site B and Site C are not allowed to communicate with each other. In this case, two VPNs, VPN1 and VPN2, can be established, with Site A and Site B belonging to VPN1 and Site A and Site C belonging to VPN2. In this manner, Site A is configured to belong to multiple VPNs.

Figure 9-62 One site belonging to multiple VPNs



- A site connects to a carrier network through the CE and may contain more than one CE, but a CE belongs only to one site.

It is recommended that you determine the devices to be used as CEs based on the following principles:

If the site is a host, use the host as the CE.

If the site is a subnet, use switches as CEs.

If the site comprises multiple subnets, use routers as CEs.

Sites connecting to the same carrier's network can be categorized into different sets based on configured policies. Only sites that belong to the same set can access each other, and this set is a VPN.

Address space overlapping

As a private network, a VPN independently manages an address space. Address spaces of different VPNs may overlap. For example, if both VPN1 and VPN2 use addresses on network segment 10.110.10.0/24, address space overlapping occurs.

NOTE

VPNs can use overlapped address spaces in the following situations:

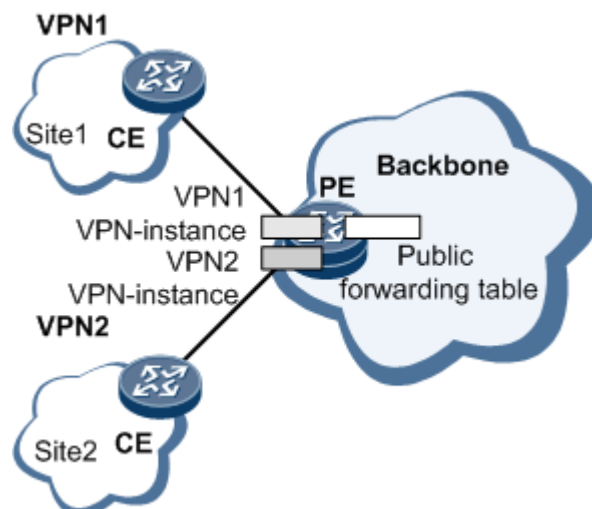
- Two VPNs do not cover the same site.
- Two VPNs cover the same site, but devices at the site and devices using addresses in overlapped address spaces in the VPNs do not access each other.

VPN instance

CEs are user-side devices and need to send only local VPN routes to PEs, irrespective of whether the PEs connect to the public network or other VPNs. PEs are network-side devices, and a PE generally connects to multiple CEs from different VPNs. A PE may receive routes from different VPNs. Because address spaces used by different VPNs may overlap, routes sent from different VPNs may carry the same destination address. If a PE maintains only one routing and forwarding table, this table will accept only one of the routes from different VPNs but with the same destination address. To prevent this problem, the VPN technology uses VPN instances.

A VPN instance is also called a VPN routing and forwarding (VRF) table. A PE maintains multiple routing and forwarding tables, including a public routing and forwarding table and one or more VRF tables. In other words, a PE has multiple instances, including a public network instance and one or more VPN instances, as shown in [Figure 9-63](#). Each VPN instance maintains routes from the corresponding VPN. The public network instance maintains public network routes. This enables a PE to keep all routes from VPNs, irrespective of whether their address spaces overlap.

Figure 9-63 Schematic diagram of VPN instances



The differences between a public routing and forwarding table and a VRF table are as follows:

- A public routing table contains the IPv4 routes of all PEs and Ps. These IPv4 routes are static routes configured on the backbone network or are generated by routing protocols configured on the backbone network.
- A VPN routing table contains the routes of all sites that belong to the corresponding VPN instance. The routes are obtained through exchange of VPN routes between PEs or between CEs and PEs.
- According to route management policies, a public forwarding table contains the minimum forwarding information extracted from the corresponding routing table, whereas a VPN forwarding table contains the minimum forwarding information extracted from the corresponding VPN routing table.

The VPN instances on a PE are independent of each other. They are also independent of the public routing and forwarding table.

Each VPN instance can be regarded as a virtual router, which maintains an independent address space and has one or more interfaces connected to the router.

In RFC 4364 (BGP/MPLS IP VPNs), a VPN instance is called a per-site forwarding table. As the name suggests, one VPN instance corresponds to one site. To be specific, every connection between a CE and a PE corresponds to a VPN instance, but this is not a one-to-one mapping. The VPN instance is manually bound to the PE interface that directly connects to the CE.

A VPN instance uses an RD to identify an independent address space and uses VPN targets to manage VPN memberships and routing principles of directly connected sites and remote sites.

Relationships between VPNs, sites, and VPN instances

The relationships between VPNs, sites, and VPN instances are as follows:

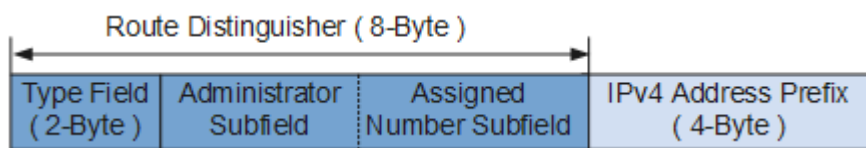
- A VPN consists of multiple sites. A site may belong to multiple VPNs.
- A site is associated with a VPN instance on a PE. A VPN instance integrates the VPN member relationships and routing principles of its associated sites. Multiple sites form a VPN based on VPN instance rules.

RD and VPN-IPv4 address

Traditional BGP cannot process the routes of VPNs with overlapped address spaces. Assume that VPN1 and VPN2 use addresses on the network segment 10.110.10.0/24, and each of them advertises a route destined for this network segment. The local PE identifies the two VPN routes based on VPN instances and sends them to the remote PE. Because routes from different VPNs cannot work in load-balancing mode, the remote PE adds only one of the two routes to its VRF table based on BGP route selection rules.

This is because BGP cannot distinguish VPN routes with the same IP address prefix. To solve this problem, BGP/MPLS IP VPN uses the VPN-IPv4 address family.

A VPN-IPv4 address consists of 12 bytes. The first eight bytes represent the RD and the last four bytes represent the IPv4 address prefix, as shown in [Figure 9-64](#).

Figure 9-64 VPN-IPv4 address

RDs are used to distinguish IPv4 prefixes using the same address space. The format of RDs enables carriers to allocate RDs independently. An RD, however, must be unique on the entire network to ensure correct routing if CEs are dual-homed to PEs. IPv4 addresses with RDs are called VPN-IPv4 addresses. After receiving IPv4 routes from a CE, a PE converts the routes to globally unique VPN-IPv4 routes and advertises the routes on the public network.

VPN target

The VPN target, also called the route target (RT), is a 32-bit BGP extended community attribute. BGP/MPLS IP VPN uses VPN targets to control the advertisement of VPN routing information.

A VPN instance is associated with one or more VPN targets, which are of the following types:

- Export VPN target: After learning an IPv4 route from a directly connected site, a PE converts the route to a VPN-IPv4 route and sets the export VPN target for the route. As an extended community attribute, the export VPN target is advertised with the route.
- Import VPN target: After receiving a VPN-IPv4 route advertised by another PE, the local PE checks the export VPN target of the route. If the export VPN target is identical with the import VPN target of a VPN instance on the PE, the PE adds the route to the VPN instance.

The VPN target defines the sites that can receive a VPN route, and the sites from which the PE can receive routes.

After receiving a route from a directly connected CE, a PE sets the export VPN targets of the route. The PE then uses BGP to advertise the route with export VPN targets to related PEs. After receiving the route, the related PEs compare the export VPN targets with the import VPN targets of all their VPN instances. If an export VPN target is identical with an import VPN target, the route is added to the corresponding VPN instance.

The reasons for using VPN targets instead of RDs as the extended community attributes are as follows:

- A VPN-IPv4 route has only one RD, but can be associated with multiple VPN targets. With multiple extended community attributes, BGP can greatly improve network flexibility and expansibility.
- VPN targets are used to control route advertisement between different VPNs on a PE. After being configured with matching VPN targets, different VPN instances on a PE can import routes from each other.

On a PE, different VPNs have different RDs, but the extended community attributes allowed by BGP are limited. Using RDs for route importing limits network expansibility.

On a BGP/MPLS IP VPN, VPN targets can be used to control exchange of VPN routes between sites. Export VPN targets and import VPN targets are independent of each other and can be configured with multiple values, ensuring flexible VPN access control and diversified VPN networking modes.

Multiprotocol Border Gateway Protocol (MP-BGP)

Traditional BGP-4 defined in RFC 1771 can manage IPv4 routes, but not the routes of VPNs with overlapped address spaces.

To correctly process VPN routes, VPNs use MP-BGP defined in RFC 4760 (Multiprotocol Extensions for BGP-4). MP-BGP supports multiple network layer protocols. Network layer protocol information is contained in the Network Layer Reachability Information (NLRI) field and the Next Hop field of an MP-BGP Update message.

MP-BGP uses the address family to differentiate network layer protocols. An address family can be a traditional IPv4 address family or any other address family such as a VPN-IPv4 address family or an IPv6 address family. For the values of address families, see RFC 3232 (Assigned Numbers).

9.5.5 BGP/MPLS IP VPN Principles

Route Advertisement on a Basic BGP/MPLS IP VPN

On a basic BGP/MPLS IP VPN, CEs and PEs are responsible for advertising VPN routes, whereas Ps only need to maintain backbone network routes without knowing VPN routing information. Generally, a PE maintains the routes of VPNs that the PE accesses, rather than all VPN routes. VPN route advertisement consists of the following phases: Route advertisement from the local CE to the ingress PE Route advertisement from the ingress PE to the egress PE Route advertisement from the egress PE to the remote CE After the process of route advertisement is complete, the local and remote CEs can set up reachable routes, and VPN routing information can be advertised on the backbone network. The following describes the three phases of route advertisement in detail:

1. Route advertisement from the local CE to the ingress PE

After the peer relationship is set up between a CE and the directly connected PE, the CE advertises the local IPv4 routes to the PE. The CE can communicate with the PE over static routes or routes established using Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Intermediate System to Intermediate System (IS-IS), or BGP. Routes advertised by the CE to the PE are standard IPv4 routes, regardless of which routing protocol is used.

VPN instances on a PE are isolated from each other and independent of the public routing and forwarding table, so as to prevent problems caused by **address space overlapping**. After learning routes from CEs, a PE decides to which routing and forwarding table the routes should be installed. Common static routes and routing protocols do not have this capability, and manual configuration is required.

2. Route advertisement from the ingress PE to the egress PE

Route advertisement from the ingress PE to the egress PE consists of the following phases:

- After learning VPN routes from a CE, a PE stores these routes in corresponding VRFs and adds **RDs** to these standard IPv4 routes. The VPN-IPv4 routes are then generated.
- The ingress PE advertises VPN-IPv4 routes to the egress PE by sending **MP-BGP** Update messages. The MP-BGP Update messages also contain **VPN targets** and MPLS labels.

Before the next-hop PE receives the VPN-IPv4 routes, the routes are first filtered by BGP routing policies, including the export policy configured on the VPN instance and the peer export policy.

After these routes arrive at the egress PE, if they match the BGP peer import policy and their next hops are reachable or they can be iterated, the egress PE performs local route crossing and filters these routes based on a VRF import policy. The egress PE then decides which routes are to be added to its VPN routing tables. Routes received from other PEs are added to a VPN routing table based on **VPN targets**. The egress PE stores the following information for subsequent packet forwarding:

- Values of MPLS labels contained in MP-BGP Update messages
- Tunnel IDs generated after tunnel iteration

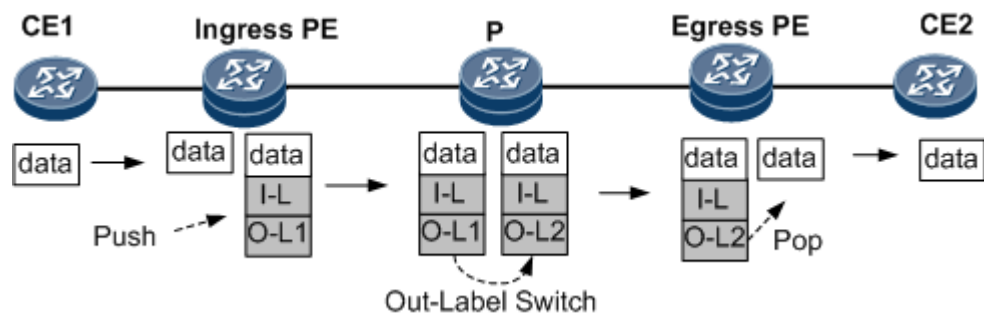
3. Route advertisement from the egress PE to the remote CE

A remote CE can learn VPN routes from an egress PE over static routes or routes established using RIP, OSPF, IS-IS, or BGP. Route advertisement from the egress PE to a remote CE is similar to that from a local CE to the ingress PE. The details are not described here. Note that the routes advertised by the egress PE to the remote CE are standard IPv4 routes.

After a PE receives routes of different VPNs from a local CE, if the next hops of these routes are reachable or these routes can be iterated, the PE matches the export VPN targets of these routes with the import VPN targets of its local VPN instances. This process is called local route crossing. During local route crossing, the PE filters these routes based on a VRF import policy and modifies the attributes of eligible routes.

Packet Forwarding on a BGP/MPLS IP VPN

On a BGP/MPLS IP VPN backbone network, a P does not know VPN routing information. VPN packets are forwarded between PEs over tunnels. **Figure 9-65** shows an example of packet forwarding on a BGP/MPLS IP VPN. A packet is transmitted from CE1 to CE2. I-L indicates an inner label, and O-L indicates an outer label. The outer label directs the packet to the BGP next hop, and the inner label identifies the outbound interface for the packet or the VPN to which the packet belongs.

Figure 9-65 Forwarding of a VPN packet from CE1 to CE2

The forwarding process is as follows:

1. CE1 sends a VPN packet to the ingress PE.
2. After receiving the packet from an interface bound to a VPN instance, the ingress PE performs the following steps:
 - Searches the corresponding VPN forwarding table based on the RD of the bound VPN instance.
 - Matches the destination IPv4 address with forwarding entries and searches for the corresponding tunnel ID.
 - Adds an I-L to the packet and finds the tunnel to be used based on the tunnel ID.
 - Adds an outer label to the packet and sends the packet over the tunnel. In this example, the tunnel is an LSP, and the outer label is an MPLS label.
 - Transmits the double-tagged packet over the backbone network. Each P on the forwarding path swaps the outer label of the packet.
3. After receiving the packet, the egress PE removes the outer label of the packet.

NOTE

In this example, the final outer label of the packet is O-L2. If PHP is configured, O-L2 is removed on the penultimate hop, and the egress PE receives a packet with the inner label only.

4. The egress PE removes the inner label residing at the bottom of the label stack.
5. The egress PE sends the packet from the corresponding outbound interface to CE2. After its labels are removed, the packet becomes a pure IP packet.

In this manner, the packet is sent from CE1 to CE2. CE2 forwards the packet to the destination in the way it sends other IP packets.

9.5.6 Hub & Spoke

The Hub & Spoke networking can be used to enable an access control device on a VPN to control the mutual access of other users. The site where the access control device locates is called a Hub site, and other sites are called Spoke sites. At the Hub site, a device that accesses the VPN backbone network is called a Hub-CE; at a Spoke site, a device that accesses the VPN backbone network is called a Spoke-

CE. On the VPN backbone network, a device that accesses the Hub site is called a Hub-PE; a device that accesses a Spoke site is called a Spoke-PE.

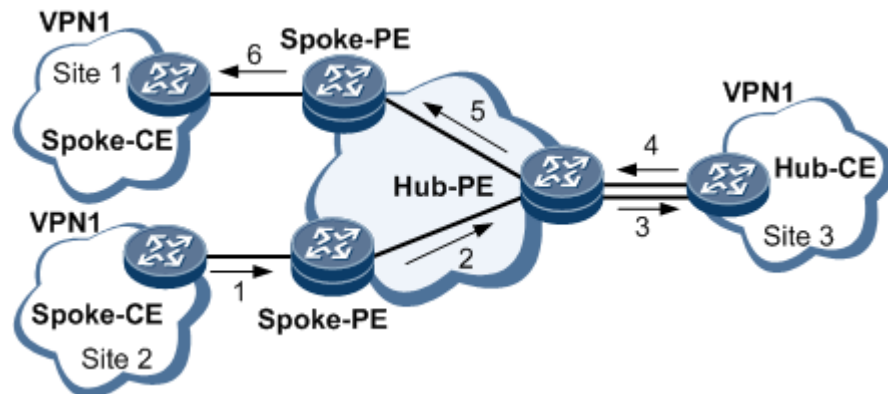
A Spoke site advertises routes to the Hub site, and the Hub site then advertises the routes to other Spoke sites. No direct route exists between the Spoke sites. The Hub site controls the communication between the Spoke sites.

In the Hub & Spoke networking model, two VPN targets are configured to stand for Hub and Spoke respectively.

The configuration of a VPN target on a PE must comply with the following rules:

- The export target and the import target of the Spoke-PE at a Spoke site are Spoke and Hub respectively. The import target of a Spoke-PE is different from the export targets of other Spoke-PEs.
- A Hub-PE requires two interfaces or sub-interfaces. One interface or sub-interface receives routes from Spoke-PEs, and the import target of the VPN instance on the interface is Spoke. The other interface or sub-interface advertises the routes to Spoke-PEs, and the export target of the VPN instance on the interface is Hub.

Figure 9-66 Route advertisement from Site 2 to Site 1 in Hub & Spoke networking

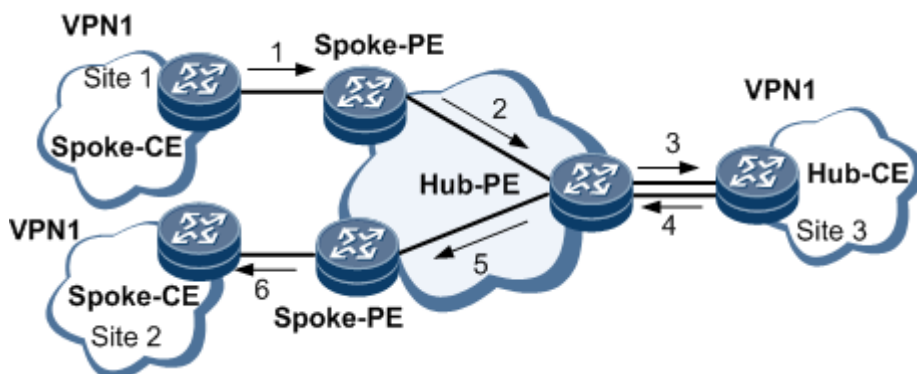


As shown in [Figure 9-66](#), the communication between Spoke sites is controlled by the Hub site. The lines with arrowheads show the process of advertising a route from Site 2 to Site 1.

- The Hub-PE can receive the VPN-IPv4 routes advertised by all the Spoke-PEs.
- All the Spoke-PEs can receive the VPN-IPv4 routes advertised by the Hub-PE.
- The Hub-PE advertises the routes learned from the Spoke-PEs to the Hub-CE, and advertises the routes learned from the Hub-CE to all the Spoke-PEs. The Spoke sites can access each other through the Hub site.
- The import target of a Spoke-PE is different from the export targets of other Spoke-PEs. Two Spoke-PEs cannot directly advertise VPN-IPv4 routes to each other. As a result, the Spoke sites cannot access each other.

The transmission path between Site 1 and Site 2 is shown in [Figure 9-67](#). The lines with arrowheads indicate the path from Site 2 to Site 1.

Figure 9-67 Path of data transmission from Site 1 to Site 2



Networking Description

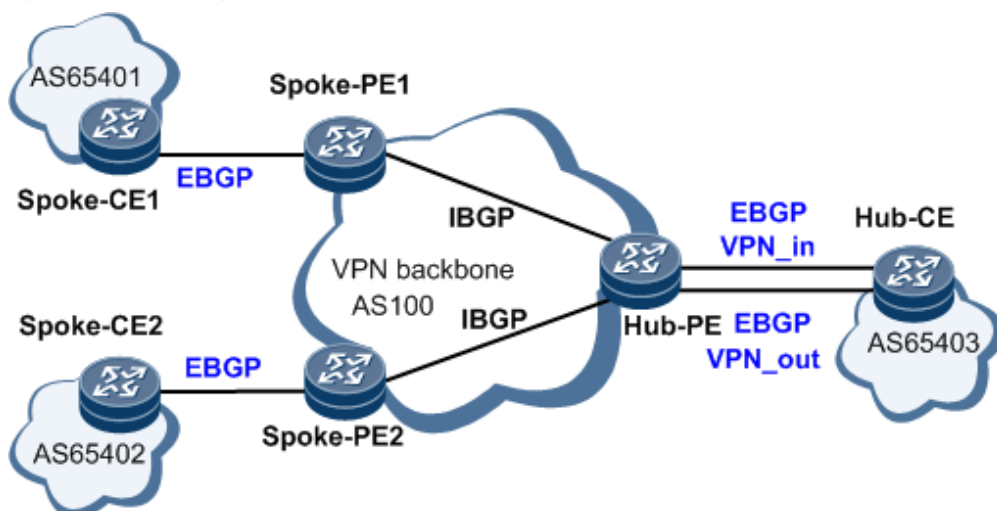
Hub & Spoke networking schemes include:

- External Border Gateway Protocol (EBGP) running between the Hub-CE and Hub-PE, and between Spoke-PEs and Spoke-CEs
- IGP running between the Hub-CE and Hub-PE, and between Spoke-PEs and Spoke-CEs
- EBGP running between the Hub-CE and Hub-PE, and IGP running between Spoke-PEs and Spoke-CEs

The following describes these networking schemes in detail:

- EBGP running between the Hub-CE and Hub-PE, and between Spoke-PEs and Spoke-CEs

Figure 9-68 EBGP running between the Hub-CE and Hub-PE, and between Spoke-PEs and Spoke-CEs

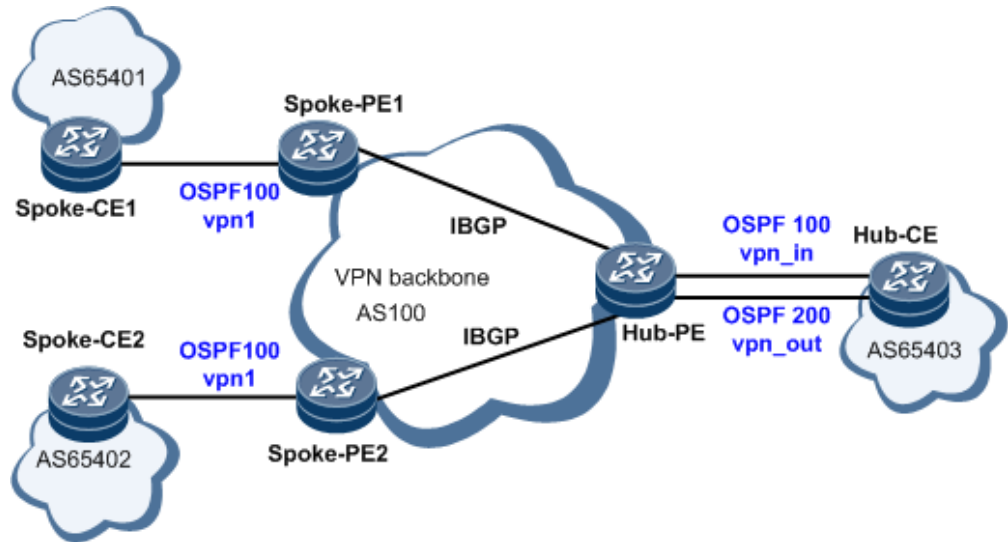


As shown in [Figure 9-68](#), the routing information advertised by a Spoke-CE is forwarded to the Hub-CE before being transmitted to other Spoke-PEs. If

EBGP runs between the Hub-PE and Hub-CE, the Hub-PE performs the AS-Loop check on the route. If the Hub-PE detects its own AS number in the route, it discards the route. In this case, to implement the Hub & Spoke networking, the Hub-PE must be configured to permit the existence of repeated local AS numbers.

- IGP running between the Hub-CE and Hub-PE, and between Spoke-PEs and Spoke-CEs

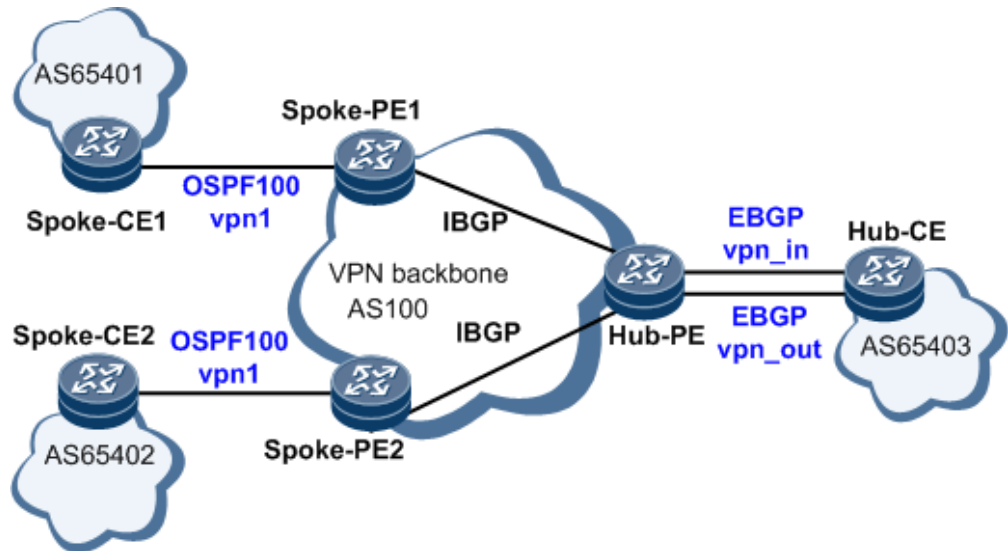
Figure 9-69 IGP running between the Hub-CE and Hub-PE, and between Spoke-PEs and Spoke-CEs



Because all PEs and CEs exchange routing information through IGP and IGP routes do not contain the AS_Path attribute, the AS_Path field of BGP VPNv4 routes is null.

- EBGP running between the Hub-CE and Hub-PE, and IGP running between Spoke-PEs and Spoke-CEs

Figure 9-70 EBGP running between the Hub-CE and Hub-PE, and IGP running between Spoke-PEs and Spoke-CEs



The networking topology is similar to that shown in [Figure 9-68](#). The AS_Path attribute of the route forwarded by the Hub-CE to the Hub-PE contains the AS number of the Hub-PE. Therefore, the Hub-PE must be configured to permit the existence of repeated local AS numbers.

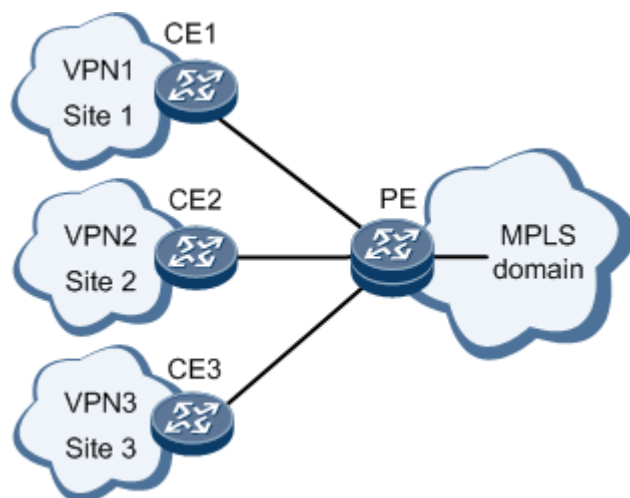
9.5.7 MCE

The multi-VPN-instance customer edge (MCE) technology provides logically independent VPN instances and address spaces on a CE, allowing multiple VPN users to share the same CE. The MCE technology provides an economical and easy-to-use solution to solve problems concerned with VPN service isolation and security.

Background

VPN services are becoming increasingly refined, and the demand for VPN service security is growing. Carriers must isolate different types of VPN services on networks to meet this demand. As shown in [Figure 9-71](#), the traditional BGP/MPLS IP VPN technology isolates VPN services by deploying one CE for each VPN, bringing in high costs and complicated network deployment. If multiple VPNs use the same CE to access upper-layer devices, these VPNs will share the same routing and forwarding table, and data security for these VPNs cannot be ensured. The MCE technology addresses conflicts between network costs and data security problems caused by multiple VPNs sharing the same CE.

Figure 9-71 Networking diagram for VPN service isolation using BGP/MPLS IP VPN

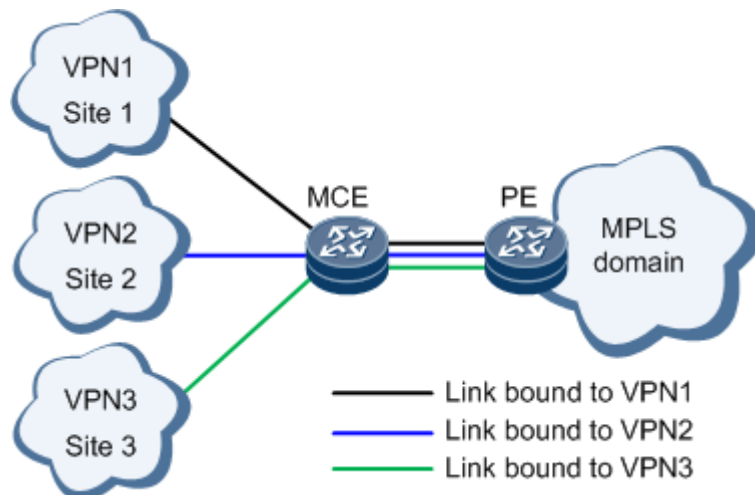


Implementation

The MCE technology creates a VPN instance for each VPN service to be isolated. Each VPN uses an independent routing protocol to communicate with the MCE to which these VPNs are connected. A VPN instance is bound to each link between the MCE and the PE to which the MCE is bound. As a result, an independent channel is established for each VPN service, and different VPN services are isolated.

As shown in [Figure 9-72](#), three VPN instances are configured on the MCE: VPN1, VPN2, and VPN3. To be specific, three independent VPN routing and forwarding tables are created on the MCE. VPN1 is bound to the link between the MCE and Site1 and a link between the MCE and PE, VPN2 is bound to the link between the MCE and Site2 and a link between the MCE and PE, and VPN3 is bound to the link between the MCE and Site3 and a link between the MCE and PE. These configurations allow VPN services to be isolated using only one MCE.

Figure 9-72 MCE networking



Benefits

The MCE technology enables CEs to provide PE functions. MCEs avoid the practice of deploying one CE for each VPN while isolating VPN services, significantly reducing maintenance costs and expenditure on devices.

9.5.8 BGP/MPLS IP VPN Label Distribution Modes

Background

On a BGP/MPLS IP VPN, a private network label (MPLS label) is assigned for each VPN route by default. If a large number of VPN routes exist, MPLS label resources may be insufficient. Other label distribution modes can be used to save MPLS label resources. [Table 9-14](#) compares the label distribution modes which are currently available.

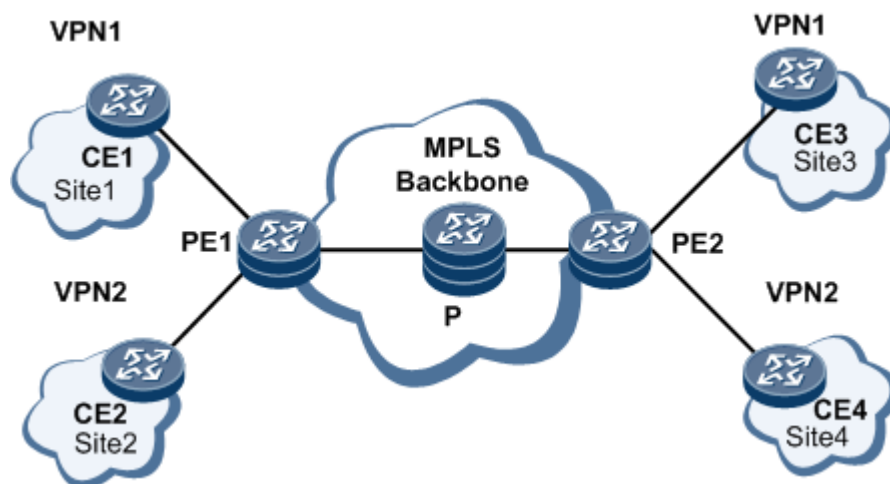
Table 9-14 Comparison among label distribution modes

Label Distribution Mode	Description	Applicable Networking	Configuration Position
One label per instance	All the VPN routes from a VPN instance are assigned the same private network label.	All types of BGP/MPLS IP VPNs	Devices on which VPN instances are configured
One label per next hop	All the VPN routes with the same next hop and outgoing label are assigned the same private network label.	Inter-AS VPN Option B	ASBRs

Implementation

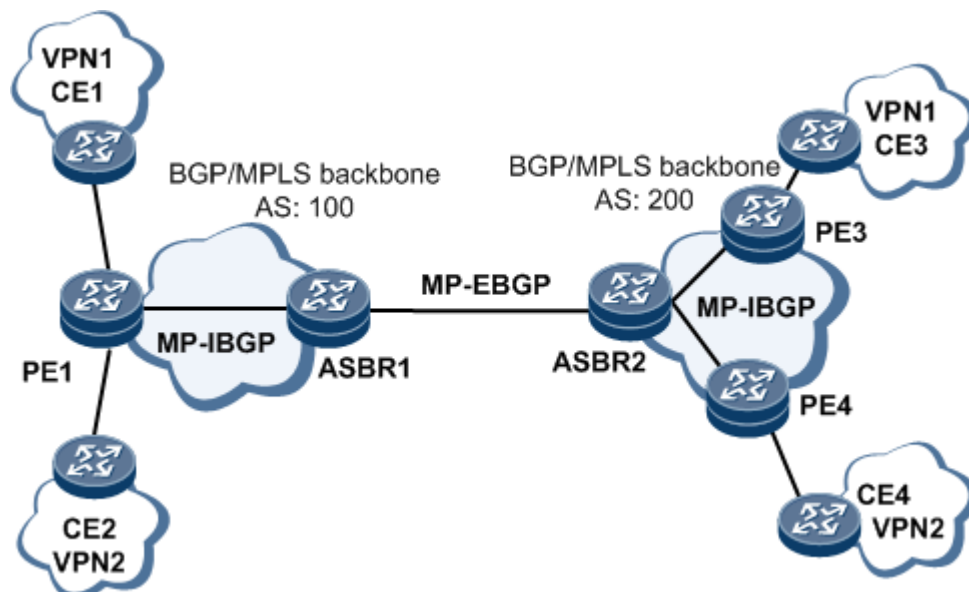
One Label per Instance

After one-label-per-instance label distribution is configured in the IPv4 or IPv6 address family of a VPN instance, all the VPN routes from the corresponding address family of the VPN instance share the same private network label. On the network shown in [Figure 9-73](#), PE1 has two VPN instances: VPN1 and VPN2. If PE1 receives 10,000 VPN routes from VPN1 and VPN2, respectively, PE1 assigns 20,000 private network labels to these routes by default. After one-label-per-instance label distribution is configured, PE1 assigns only one label to the 10,000 VPN routes received from VPN1 and one label to the 10,000 VPN routes received from VPN2.

Figure 9-73 One label per instance

One label per next hop

By default, an ASBR assigns a private network label to each VPN route. You can also configure an ASBR to distribute labels based on next hops. After one-label-per-next-hop label distribution is configured on an ASBR, the ASBR re-advertises an MP-BGP Update packet to its peers. The MP-BGP Update packet carries VPNv4 routes and their labels that are re-assigned based on next hops. After a peer receives the MP-BGP Update packet, the peer updates its local label forwarding table and re-establishes LSPs. After the ASBR and its peers update their label forwarding tables, packets are forwarded based on the updated label forwarding tables.

Figure 9-74 One label per next hop

In the inter-AS VPN Option B scenario shown in [Figure 9-74](#), two VPN instances named VPN1 and VPN2 are configured on PE1 that uses one-label-per-instance label distribution. If one-label-per-next-hop label distribution is not configured on ASBR1, ASBR1 assigns 20,000 labels to the 20,000 VPN routes imported from CE1 and CE2 over PE1 before advertising these routes to ASRB2. After one-label-per-next-hop label distribution is configured on ASBR1, ASBR1 only needs to assign one label to VPN routes with the same next hop and outgoing label. In other words, ASBR1 assigns only two labels to the 20,000 routes imported from CE1 and CE2 over PE1 before advertising these routes to ASRB2.

NOTE

One-label-per-route label distribution and one-label-per-next-hop label distribution can be flexibly switched to each other. During label distribution mode switching, service packets are lost for a short period due to the update of label forwarding tables.

In an inter-AS VPN Option B scenario, be sure to configure one-label-per-instance label distribution on PEs if you configure one-label-per-next-hop label distribution on ASBRs.

Benefits

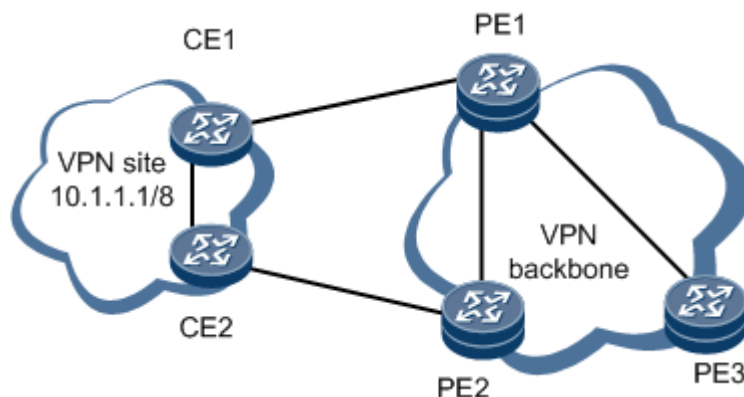
Using an appropriate label distribute mode saves label resources.

9.5.9 BGP Site of Original (SoO)

If multiple CEs in a VPN site access different PEs, VPN routes sent from CEs to PEs may return to this VPN site after traveling across the backbone network. This may cause routing loops in the VPN site.

After the SoO attribute is configured on a PE, the PE adds the SoO attribute to the route sent from a CE and then advertises the route to other PE peers. Before advertising the VPN route to the connected CE, the PE peers check the SoO attribute carried in the VPN route. If the PE peers find that this SoO attribute is the same as the locally configured SoO attribute, the PE peers do not advertise this VPN route to the connected CE.

On the network shown in [Figure 9-75](#), CE1 and CE2 belong to the same VPN site and can advertise routes to each other. CE1 advertises the route destined for 10.1.1.1/8 in the VPN site to PE1, and PE1 advertises the route to PE2 by using Multiprotocol Internal Border Gateway Protocol (MP-IBGP). PE2 then advertises the route to CE2 by using BGP. As a result, the route returns to the original VPN site from which the route is advertised, which may cause a routing loop in the VPN site.

Figure 9-75 Networking diagram for BGP SoO application

To avoid routing loops in a VPN site, you can configure an SoO attribute on PE1 for CE1. The SoO attribute identifies the site where the CE1 resides. The routes advertised by CE1 to PE1 then carry this SoO attribute, and PE1 advertises the routes with the SoO attribute to other PEs across the backbone network. Before advertising the received routes to its peer CE2, PE2 checks whether the routes carry the SoO attribute specified for the site where CE2 resides. If a route carries this SoO attribute, this route is advertised from the site where CE2 resides. PE2 then refuses to advertise such a route to CE2, avoiding routing loops in the site.

9.5.10 Terms, Acronyms, and Abbreviations for BGP/MPLS IP VPN

Terms

Term	Definition
CE	Customer edge equipment that is directly connected to the service provider. On an MPLS VPN, a CE can be a router, switch, or even a host.
Address space	An address realm managed by a VPN.
L2TP	A Layer 2 tunneling protocol that is drafted by the IETF and involves the participation of companies such as Microsoft. L2TP combines the advantages of both PPTP and L2F.
MP-BGP	A multi-protocol extension of BGP-4. MP-BGP supports multiple network layer protocols and identifies the protocols based on address families. MP-BGP transmits VPN composition information and VPN-IPv4 routes between PEs.
P	A backbone router that is located on the service provider network. A P is indirectly connected to CEs. Ps only need to possess basic MPLS forwarding capabilities and do not maintain information about a VPN.

Term	Definition
PE	A router that is located on the backbone network of the MPLS VPN structure. A PE is responsible for VPN user management, establishment of LSPs between PEs, and exchange of routing information between sites of the same VPN. During the process, a PE performs the mapping and forwarding of packets from the private network to the public channel and then from the public channel to the private network. A PE can be a UPE, an SPE, or an NPE.
RD	A route identifier, which is an 8-byte field in a VPN IPv4 address. An RD and a 4-byte IPv4 address prefix construct a VPN IPv4 address, which is used to differentiate the IPv4 prefixes using the same address space.
Site	A group of IP systems with IP connectivity, which can be achieved independent of SP networks.
Tunnel	A channel through which a packet switching network transmits service traffic between PEs. In VPN, a tunnel is an information transmission channel between two entities. The tunnel provides security for transparent transmission of VPN information. In most cases, a tunnel is an MPLS tunnel.
Tunnel iteration	A process in which a route is iterated to a tunnel.
Tunnel key	A group of information, including the token, slot number of an outgoing interface, tunnel type, and location method.
VPN	A recently-developed technology that implements the private network over a public network. It is a network that only logically exists.
VPN instance	An entity that is set up and maintained by PEs for directly-connected sites. Each site has its VPN instance on a PE. A VPN instance is also called a VRF table. A PE has multiple forwarding tables, including a public-network routing table and one or more VRF tables.
VPN target	A BGP extended community attribute that is also called route target. In BGP/MPLS IP VPN, VPN targets are used to control VPN routing information. The VPN target attribute defines that a VPN IPv4 route can be received by which sites and a PE device can receive routes from which site.

Acronyms and Abbreviations

Acronym and Abbreviation	Full Name
AMB	active main board

Acronym and Abbreviation	Full Name
AS	autonomous system
ASG	access service gateway
BSC	base station controller
BTS	base transceiver station
DCN	data communication network
EBGP	External Border Gateway Protocol
EGP	Exterior Gateway Protocol
FMC	fixed-mobile convergence
GR	graceful restart
HA	high availability
HoPE	hierarchy of PE
IBGP	Internal Border Gateway Protocol
IS-IS	Intermediate System to Intermediate System
L3VPN	Layer 3 virtual private network
LSDB	link state database
LTE	Long Term Evolution
MCE	multi-VPN-instance customer edge
MME	mobility management entity
MBGP	Multiprotocol Border Gateway Protocol
MP-EBGP	Multiprotocol External Border Gateway Protocol
MP-IBGP	Multiprotocol Internal Border Gateway Protocol
NLRI	Network Layer Reachability Information
NSF	non-stop forwarding
NSR	non-stop routing
OSPF	Open Shortest Path First
PSTN	public switched telephone network
RIP	Routing Information Protocol
RIPng	Routing Information Protocol next generation
RM	routing management

Acronym and Abbreviation	Full Name
RNC	radio network controller
RP	route processor
RR	route reflector
RSG	radio service gateway
RSVP	Resource Reservation Protocol
RT	route target
SP	service provider
SMB	standby main board
TCP	Transport Control Protocol
VRF	VPN routing and forwarding

9.6 GRE

9.6.1 Introduction to GRE

Definition

Generic Routing Encapsulation (GRE) is a common routing encapsulation protocol that can encapsulate network layer protocols, such as IPX, ATM, IPv6/IPv4, and AppleTalk, inside virtual point-to-point links over an Internet Protocol network.

GRE provides a transmission channel in which one network layer protocol is encapsulated in another network layer protocol. This channel is called a GRE tunnel.

Feature Value

- Allows one network layer protocol to be encapsulated in another network layer protocol to traverse heterogeneous networks.
- Provides a workaround for networks that support a limited number of hops.
- Sets up a VPN across two physically separate networks.
- Carries IPv4 packets on private or public networks.
- Lowers requirements on device performance and sets up tunnels between devices that do not support Multiprotocol Label Switching (MPLS).

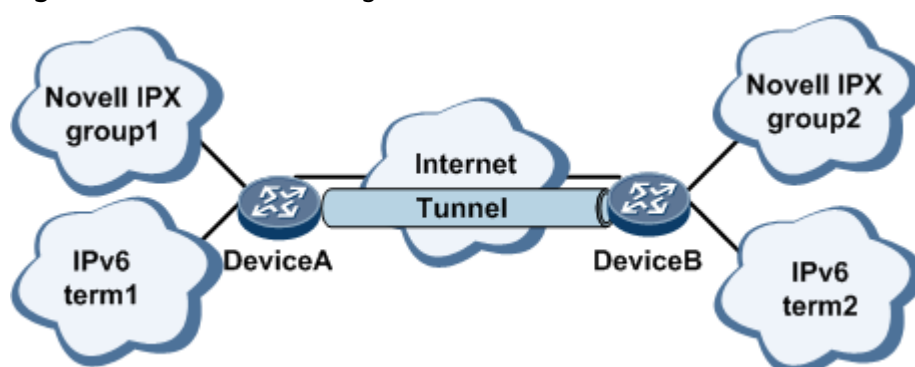
9.6.2 GRE Basic Principles

Background

A single network protocol, such as IPv4, is used to transmit packets on a backbone network, whereas other protocols, such as Internetwork Packet Exchange (IPX), Asynchronous Transfer Mode (ATM), IPv6, may be used on non-backbone networks. Because the backbone and non-backbone networks use different protocols, packets cannot be transmitted between the non-backbone networks over the backbone network. Generic Routing Encapsulation (GRE) resolves this issue by encapsulating one network protocol inside another.

On the network shown in [Figure 9-76](#), groups 1 and 2 are the non-backbone networks running Novell IPX, and teams 1 and 2 are the non-backbone networks running IPv6. The backbone network is an IPv4 network. To transmit packets between groups 1 and 2 and between teams 1 and 2 over the backbone network, GRE is used to establish a tunnel between DeviceA and DeviceB. When DeviceA receives a packet from group 1 or team 1, DeviceA encapsulates the packet into a GRE packet. The GRE packet is then encapsulated into an IPv4 packet for forwarding.

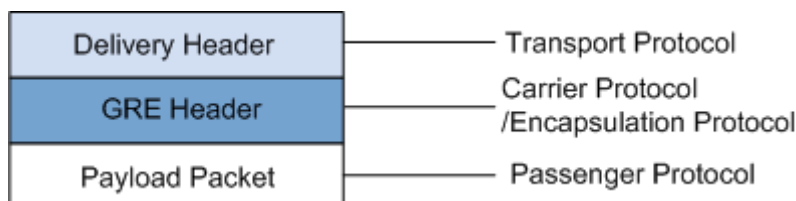
Figure 9-76 GRE networking



Related Concepts

- GRE packet format
After receiving a packet of network layer protocol, the system adds a GRE header to the packet and encapsulates the packet into another protocol, such as IP. Then, the IP protocol forwards the packet. [Figure 9-77](#) shows the format of a GRE packet.

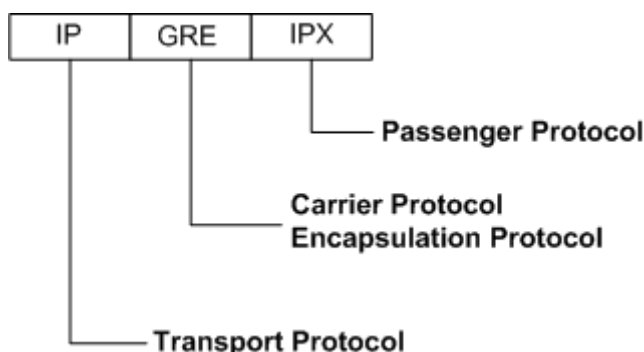
Figure 9-77 Format of a GRE packet



- Payload: is received by the system and needs to be encapsulated and routed.
- Passenger protocol: is used by the packet before encapsulation.
- Encapsulation protocol: is used to encapsulate the passenger protocol. It is also called the carrier protocol.
- Transport or delivery protocol: is responsible for forwarding the encapsulated packets.

The following shows the format of an IPX packet encapsulated for transmission over an IP tunnel.

Figure 9-78 Format of an IPX packet transmitted over an IP tunnel



NOTE

For an IPv4 GRE tunnel:

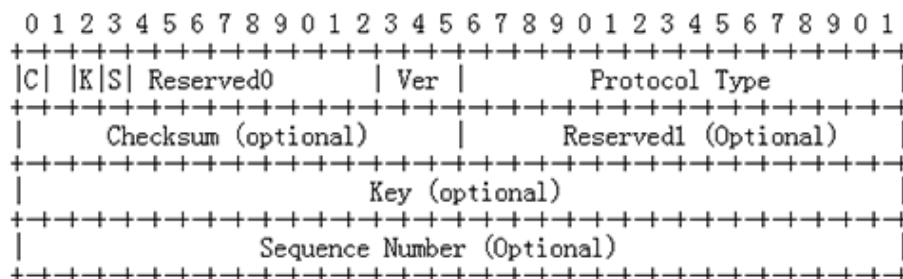
- The packet transmission protocol is IPv4.
- Only IPv4 packets can be encapsulated and routed.

• GRE packet header

RFC 1701, RFC 2784, and RFC 2890 define the GRE packet format. This feature is implemented according to RFC 2784 and RFC 2890 and is partially compatible with RFC 1701.

Figure 9-79 shows the format of the GRE header defined in RFC 2890.

Figure 9-79 Format of the GRE packet header defined in RFC 2890

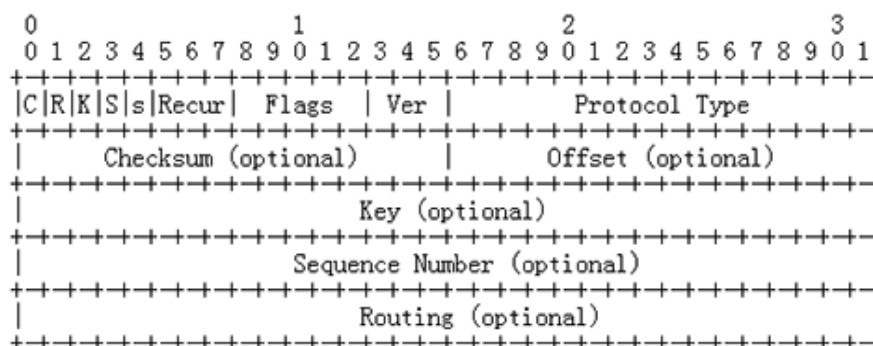


Each field is described as follows:

- C: indicates checksum. If its value is 1, the checksum field is inserted into the GRE header. If its value is 0, the GRE header does not contain the checksum field.
- K: indicates keyword. If its value is 1, the key field is inserted into the GRE header. If its value is 0, the GRE header does not contain the key field. This bit in RFC 2890 is used to identify the type of traffic in a GRE tunnel. The meaning of a keyword can be defined by customers. For example, it can be used to identify a virtual private network (VPN) to which the traffic inside a GRE tunnel belongs.
- S: indicates the sequence number. If its value is 1, the sequence number field is inserted into the GRE header. If its value is 0, the GRE header does not contain the sequence number field. If a received packet is out of sequence, it might be discarded.
- Reserved0: indicates the reserved bit, filled with 0.
- Ver: indicates the version field, which must be set to 0. Ver 1 is used for RFC 2637 PPTP.
- Protocol Type: indicates the negotiated passenger protocol type.
- Checksum: indicates the checksum field in the GRE header and payload. This field is filled in when the C bit is 1.
- Key: indicates the keyword. This field is filled in when K bit is 1.

Figure 9-80 shows the format of the GRE header defined in RFC 1701.

Figure 9-80 Format of the GRE packet header defined in RFC 1701



Each field is described as follows:

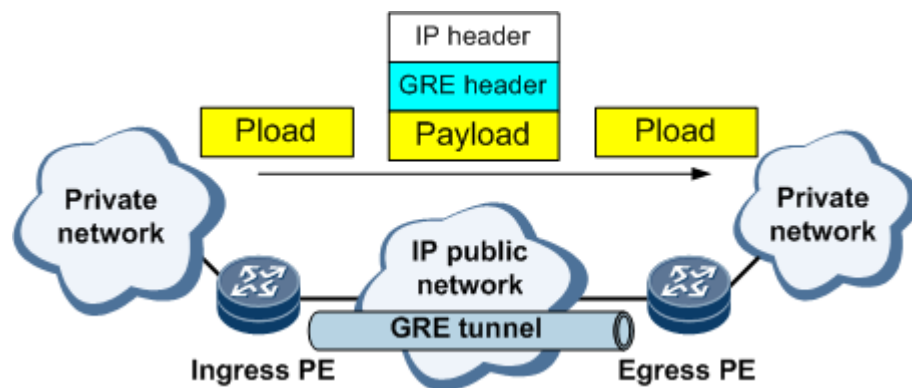
- R: indicates the routing present bit. If its value is 1, the Routing field is filled in.
- s: indicates the strict source route field. If its value is 1, Routing contains Strict Source Route.
- Recur: Indicates the recursion bit, which is used to indicate the number of GRE packet encapsulation layers. If its value is 0, there is only one-layer GRE encapsulation. Its value is increased by 1 for every GRE encapsulation. If the number of encapsulation layers is greater than 3, the packet is dropped. This field prevents a packet from being encapsulated for infinite times.

- Flags: reserved. It must be set to 0 currently.
- K: indicates the keyword, which is used by the receiver of a tunnel to verify received packets.

Transmission of Packets over a GRE Tunnel

The transmission of packets over a GRE tunnel can be divided into two phases: encapsulation and decapsulation. On the network shown in [Figure 9-81](#), a private network packet is encapsulated on the ingress PE and decapsulated on the egress PE.

Figure 9-81 Interconnection of private networks over a GRE tunnel



- Encapsulation

Upon receiving a private network packet, the ingress PE delivers the packet to the private network protocol module.

The protocol module checks the destination address field in the packet header, searches the routing table or forwarding table of the private network for the outgoing interface, and determines how to route this packet. If the outgoing interface is a GRE tunnel interface, the protocol module sends the packet to the tunnel module.

Upon receiving the packet, the tunnel module processes the packet as follows:

- Adds a GRE header to the packet according to the protocol type of the passenger protocol and the Key parameter configured for the current GRE tunnel.
- Adds a transport protocol header to the packet based on the configuration. For example, if the transport protocol is IP, the source and destination addresses carried in the IP header are the source and destination addresses of the tunnel.
- Delivers the packet to the IP module. Based on the destination address in the IP header, the IP module searches the public network routing table for the outgoing interface and sends the packet. The encapsulated packet is then transmitted on the public IP network.

- Decapsulation

The decapsulation process is opposite to the encapsulation process. Upon receiving a packet, the egress PE analyzes the IP header. After determining

that the destination of the packet is itself and the Protocol Type field is 47, which indicates that the protocol is GRE (see RFC 1701 and RFC 2784), the egress PE delivers the packet to the GRE module. The GRE module removes the IP and GRE headers and learns from the Protocol Type field in the GRE header that the passenger protocol is the protocol running on the private network. The GRE module then delivers the packet to the module corresponding to this protocol, which forwards the packet.

9.6.3 GRE Principles

9.6.3.1 Keepalive Detection

Principles

GRE does not support link status detection. If the remote interface is unreachable, the tunnel cannot immediately close the tunnel connection. As a result, the source continues forwarding packets to the peer.

However, link status detection can be provided by the keepalive function, which can be enabled on tunnel interfaces to detect the status of the remote interface.

Implementation

After the keepalive function is enabled, the source GRE tunnel periodically sends probe packets to the peer. If the peer is reachable, the source tunnel interface can receive a reply. The details are as follows:

1. After the keepalive function is enabled on the source GRE tunnel interface, the interface starts a timer, periodically sends probe packets, and starts a probe packet counter, which increases by 1 each time a probe packet is sent.
2. The peer sends a reply to the source after receiving a probe packet.
3. If the source receives a reply before the counter reaches the preset value, the source considers the peer reachable and resets the counter. Otherwise, the source considers the peer unreachable and closes the tunnel connection.

NOTE

If the keepalive function is enabled on a tunnel interface, the remote tunnel interface sends a reply upon receiving a probe packet, regardless of whether the keepalive function is enabled.

Benefits

The keepalive function prevents data loss when the peer becomes unreachable, ensuring data transmission reliability.

9.6.3.2 GRE Security Mechanism

Remote GRE Header Querying

The trace-counter function can capture packets from the remote device to check the generic routing encapsulation (GRE) header and verify whether the packet information is correct during packet transmission and encapsulation.

- **GRE Keyword Authentication**

GRE supports keyword authentication, a security mechanism defined in RFC 1701 for authenticating tunnel interfaces. This security mechanism prevents tunnel interfaces from incorrectly identifying and receiving packets from other routers.

As defined in RFC 1701, if the K bit in the GRE header is set to 1, the Key field is inserted to the GRE header, and both the receiver and sender perform key authentication.

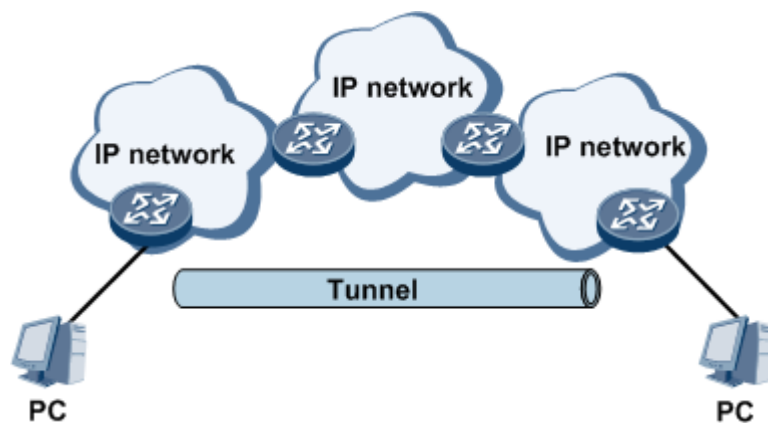
The Key field contains a four-byte number, which is inserted into the GRE header during packet encapsulation. Packets of the same traffic flow have the same Key field. When decapsulating packets, a tunnel endpoint identifies packets of the same traffic flow based on the Key field.

The authentication succeeds only if the Key fields set on both endpoints of the tunnel are the same. Otherwise, the packet is discarded. "Same" means that the Key field is not set on either endpoint, or is set to the same value on both endpoints.

9.6.4 GRE Applications

Workaround for Networks that Support a Limited Number of Hops

Figure 9-82 Enabling communication in a larger network scope



On the network shown in [Figure 9-82](#), the IP protocol runs on the network. Assume that the hop limit of the IP protocol is 255. If the hop count between two PCs is greater than 255, the PCs cannot communicate. After a tunnel is used on the network, the intermediate hops between the two tunnel endpoints are hidden so that the data can traverse a larger network scope.

Setting Up a VPN Across Physically Separate Networks

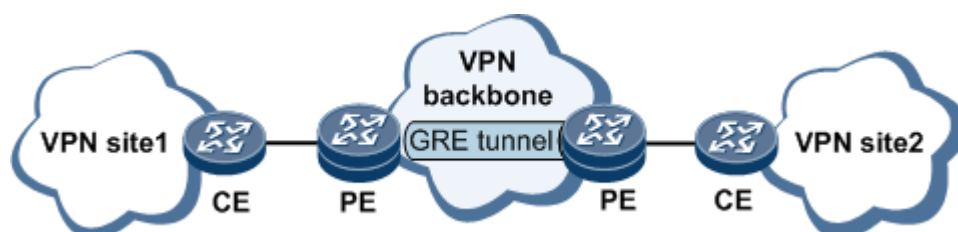
With GRE tunnels, you can set up a VPN across networks physically separated by a WAN.

Assume that Site 1 and Site 2 are deployed in different cities. By setting up a GRE tunnel between the PEs, you can connect the two separate networks to establish a VPN.

GRE, which applies to both L2VPNs and L3VPNs, can be used in either CPE-based VPNs or network-based VPNs:

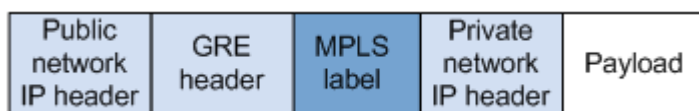
In a network-based VPN scenario, both ends of the GRE tunnel reside on PEs, as shown in [Figure 9-83](#).

Figure 9-83 GRE in a network-based VPN



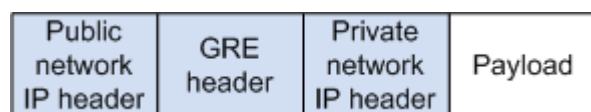
Usually, the VPN backbone network uses label switched paths (LSPs) as public network tunnels. If the core devices (P devices) on the backbone network do not support MPLS, LSPs cannot be used as public network tunnels. Then, you can use the GRE tunnel in place of the LSP to provide Layer 3 or Layer 2 VPN solutions at the core network. [Figure 9-84](#) shows the format of a private network packet transmitted on the VPN backbone network.

Figure 9-84 Format of a GRE packet that contains an MPLS label



GRE tunnels can also be used as non-MPLS VPN backbone tunnels. In this case, private network packets cannot contain MPLS labels when being transmitted on the VPN backbone network. [Figure 9-85](#) shows the format of such a packet.

Figure 9-85 Format of a GRE packet that does not contain an MPLS label

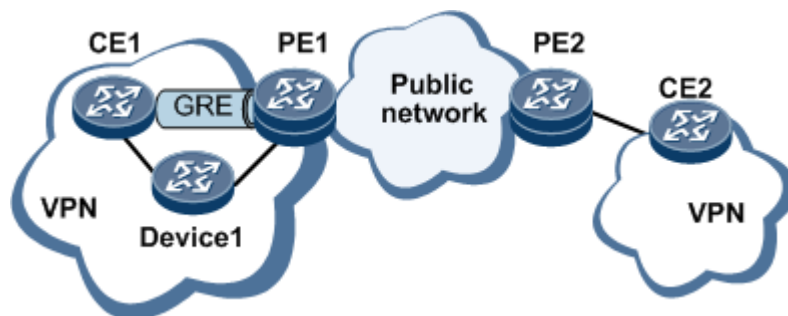


Communication Across a WAN

Static routes can be used to connect a private network to a public network or another physically separate private network. This configuration applies to only IPv4 networks.

GRE on a LAN

Figure 9-86 GRE on a LAN

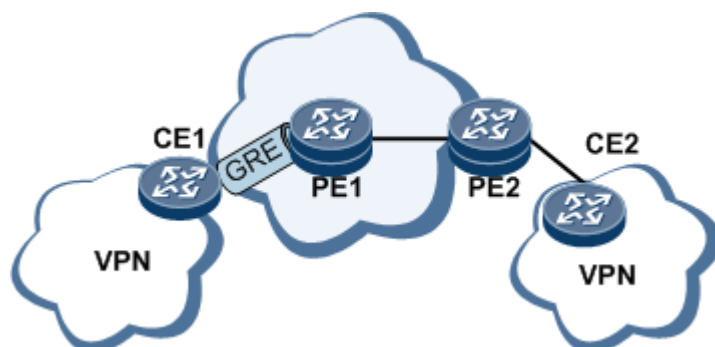


As shown in [Figure 9-86](#), both the source and destination addresses of the GRE tunnel are private addresses for PE1.

GRE Across a WAN

In this networking, CEs and PEs must have public addresses. In addition, CE1 and PE1 must have a route to each other.

Figure 9-87 GRE across a WAN



The traffic destined from the LAN connected to CE1 for remote networks must pass through the GRE tunnel. Therefore, in the routing table on CE1, the outgoing interface must be set to the source interface of the GRE tunnel for all routes pointing to remote sites, and the next hop must be set to the remote tunnel interface. If multiple LANs are connected to CE1, you can select a LAN to bind it to the source tunnel interface.

9.6.5 GRE Configuration

This section describes how to configure GRE.

9.6.5.1 Example for Configuring a Static Route for GRE

This section describes how to configure a static route for generic routing encapsulation (GRE) to transmit user traffic over the GRE tunnel. A static route is required between the device and its connected client.

Context

As shown in [Figure 9-88](#), DeviceA (OLT), DeviceB (OLT), and DeviceC (router) belong to the backbone VPN and Open Shortest Path First (OSPF) runs between them.

A direct link is required between DeviceA and DeviceC. To meet such a requirement, configure a GRE tunnel between DeviceA and DeviceC, create a static route, and specify the tunnel interface as the outgoing interface of the static route so that PC1 and PC2 can communicate with each other.

PC1 and PC2 use DeviceA and DeviceC respectively as their default gateways.

Figure 9-88 Networking of configuring a static route for GRE

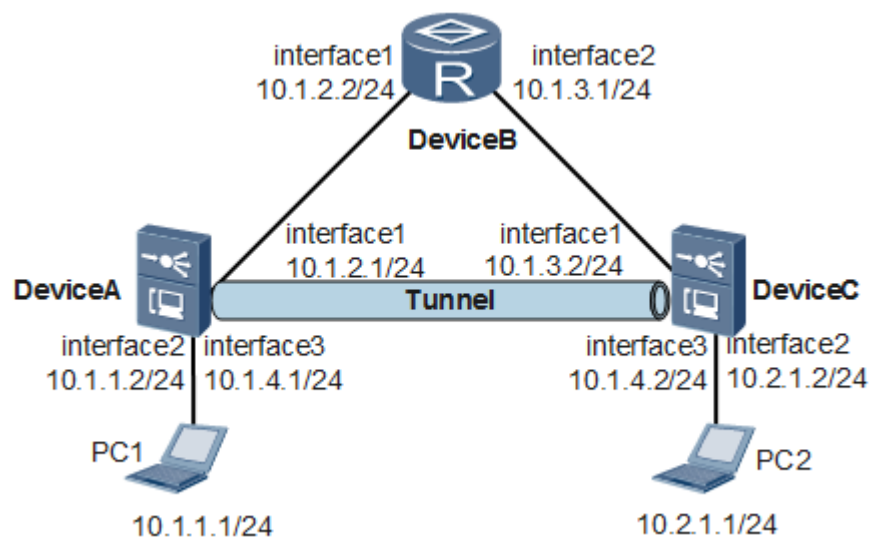


Table 9-15 Data planning

Configuration Item	Parameter	Value
Layer 3 interface	VLAN port	vlan 10 vlan 2

Configuration Item	Parameter	Value
OSPF route	Device IP address	DeviceA: 10.1.2.1 DeviceB (interface 1): 10.1.2.2 DeviceB (interface 2): 10.1.3.1 DeviceC: 10.1.3.2
GRE tunnel	Tunnel IP address	10.1.4.1 10.1.4.2
	Address of the device at each end of the tunnel	DeviceA: 10.1.2.1 DeviceC: 10.1.3.2

Prerequisite

To complete the configuration, you need the following data:

- Data required for running OSPF by referring to [11.12.6.3 Configuration Example of OSPF](#).
- Source and destination addresses and IP address of the tunnel interface at each end of the GRE tunnel.

Procedure

- Step 1** Configure the interfaces and routes.
- Step 2** Configure OSPF by referring to Configuration Example of OSPF to ensure connectivity between NEs.
- Step 3** Configure a GRE tunnel on DeviceA and DeviceC.
- Step 4** Configure GRE binding and paths.

----End

Example

1. Configure the interfaces and routes.
Configure the route between DeviceA and DeviceC because GRE tunnel transmission is based on Layer 3 IP forwarding.
 - Configure a VPN on DeviceA.

```
huawei(config)#ip vpn-instance vpn1
huawei(config-upn-instance-vpn1)#ipv4-family
huawei(config-upn-instance-vpn1-af-ipv4)#quit
huawei(config-upn-instance-vpn1)#quit
```
 - Configure a Layer 3 interface on DeviceA.

```
huawei(config)#vlan 10 smart
huawei(config)#port vlan 10 0/9 1
huawei(config)#interface vlanif 10
huawei(config-if-vlanif10)#ip address 10.1.2.1 24
huawei(config-if-vlanif10)#quit
```

- Configure OSPF on DeviceA.

```
huawei(config)#router id 10.10.10.10
huawei(config)#ospf
huawei(config-ospf-1)#area 0
huawei(config-ospf-1-area-0.0.0.0)#network 10.1.2.1 0.0.0.255
huawei(config-ospf-1-area-0.0.0.0)#quit
huawei(config-ospf-1)#quit
```
 - Configure a VPN on DeviceC.

```
huawei(config)#ip vpn-instance vpn1
huawei(config-upn-instance-vpn1)#ipv4-family
huawei(config-upn-instance-vpn1-af-ipv4)#quit
huawei(config-upn-instance-vpn1)#quit
```
 - Configure a Layer 3 interface on DeviceC.

```
huawei(config)#vlan 10 smart
huawei(config)#port vlan 10 0/9 1
huawei(config)#interface vlanif 10
huawei(config-if-vlanif10)#ip address 10.1.3.2 24
huawei(config-if-vlanif10)#quit
```
 - Configure OSPF on DeviceC.

```
huawei(config)#router id 10.20.20.20
huawei(config)#ospf
huawei(config-ospf-1)#area 0
huawei(config-ospf-1-area-0.0.0.0)#network 10.1.3.2 0.0.0.255
huawei(config-ospf-1-area-0.0.0.0)#quit
huawei(config-ospf-1)#quit
```
 - On DeviceB, set the address of the interface connected to DeviceA to 10.1.2.2 and that of the interface connected to DeviceC to 10.1.3.1.
Then, configure routes on DeviceB. For details, see *Router Configuration*.
2. Configure OSPF by referring to [11.12.6.3 Configuration Example of OSPF](#) to ensure connectivity between NEs.
 3. Configure a GRE tunnel on DeviceA and DeviceC.
 - Configure a GRE tunnel on DeviceA.

```
huawei(config)#interface tunnel 11
huawei(config-if-tunnel11)#ip binding vpn-instance vpn1
huawei(config-if-tunnel11)#tunnel-protocol gre
huawei(config-if-tunnel11)#ip address 10.1.4.1 255.255.255.0
huawei(config-if-tunnel11)#source 10.1.2.1
huawei(config-if-tunnel11)#destination 10.1.3.2
```
 - Configure a GRE tunnel on DeviceC.

```
huawei(config)#interface tunnel 11
huawei(config-if-tunnel11)#ip binding vpn-instance vpn1
huawei(config-if-tunnel11)#tunnel-protocol gre
huawei(config-if-tunnel11)#ip address 10.1.4.2 255.255.255.0
huawei(config-if-tunnel11)#source 10.1.3.2
huawei(config-if-tunnel11)#destination 10.1.2.1
```
 4. Configure GRE binding and paths.
 - Create a VLAN and implement GRE binding on DeviceA.

```
huawei(config)#vlan 2 smart
huawei(config)#port vlan 2 0/9 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip binding vpn-instance vpn1
huawei(config-if-vlanif2)#ip address 10.1.1.2 24
huawei(config-if-vlanif2)#quit
```
 - Set the next hop to tunnel 11 on DeviceA. The destination network is 10.2.1.0.

```
huawei(config)#ip route-static 10.2.1.0 255.255.255.0 tunnel 11
```
 - Create a VLAN and implement GRE binding on DeviceC.

```
huawei(config)#vlan 2 smart
huawei(config)#port vlan 2 0/9 0
huawei(config)#interface vlanif 2
huawei(config-if-vlanif2)#ip binding vpn-instance vpn1
huawei(config-if-vlanif2)#ip address 10.2.1.2 24
huawei(config-if-vlanif2)#quit
```

- Create a VPN route and set the next hop to tunnel 11 on DeviceC. The destination network is 10.1.1.0.

```
huawei(config)#ip route-static 10.1.1.0 255.255.255.0 tunnel 11
```

9.6.5.2 Example for Configuring a L3VPN over GRE Tunnel

L3VPN over GRE uses public GRE tunnels to carry L3VPN services. L3VPN/MPLS uses label switched paths (LSPs) as the public network tunnels. If the core router (P router) in the backbone network does not support MPLS, the LSPs cannot be used as the public network tunnels. In such a case, GRE tunnels can be used to implement L2VPN or L3VPN solutions in the core network.

Networking

As shown in [Figure 9-89](#):

- PEs distribute private routes carrying labels through the Multiprotocol Extensions for BGP (MP-BGP) protocol.
- VPN packets can be transmitted to the peer PE after GRE encapsulation and two-layer inner labels.
- Tunnel policies are applied on the PE and GRE tunnels are specified for VPN packet forwarding.

Figure 9-89 Networking of configuring a L3VPN over GRE tunnel

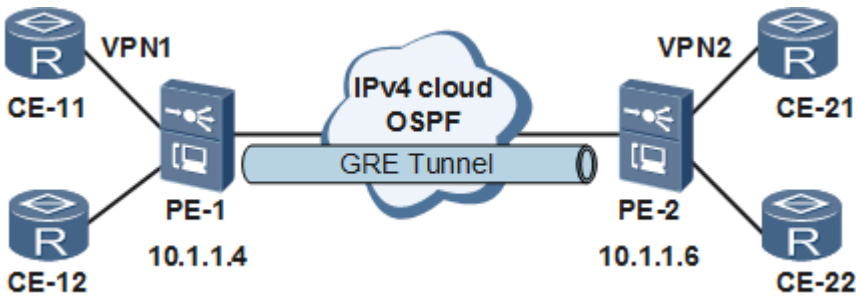


Table 9-16 Data planning

Configuration Item	Parameter	Value
Tunnel policy	Tunnel policy name	policy1
IP address	PE1 IP address	10.1.1.4
	PE2 IP address	10.1.1.6
GRE tunnel	GRE tunnel	tunnel11

Prerequisite

To complete the configuration, you need the following data:

- GRE license that has been applied for and installed
- Source and destination addresses of the GRE tunnel
- Name of the VPN instance created on the PE

Procedure

- Step 1** Configure GRE tunnels by referring to "Example for Configuring a Static Route for GRE".
- Step 2** Create a VPN and tunnel policy, and bind the VPN instance to the tunnel policy.
- Step 3** Set up the adjacency relationship between PE devices through the BGP protocol.
- Step 4** Set up the tunnel by using the adjacency relationship. The source and destination addresses of the tunnel must be the same as those of the BGP peers.
- Step 5** Create a Layer 3 interface and bind it to a VPN.

----End

Example

1. 1. Configure a VPN and tunnel policy.

- Create a tunnel policy.

```
huawei(config)#tunnel-policy policy1
huawei(config-tunnel-policy-policy1)#tunnel select-seq gre load-balance-number 1
huawei(config-tunnel-policy-policy1)#quit
```

- Create a VPN and bind it to the tunnel policy.

```
huawei(config)#ip vpn-instance vpn1
huawei(config-vpn-instance-vpn1)#ipv4-family
huawei(config-vpn-instance-vpn1-af-ipv4)#route-distinguisher 77:1
huawei(config-vpn-instance-vpn1-af-ipv4)#tnl-policy policy1
huawei(config-vpn-instance-vpn1-af-ipv4)#vpn-target 300:11 export-extcommunity
huawei(config-vpn-instance-vpn1-af-ipv4)#vpn-target 400:22 import-extcommunity
huawei(config-vpn-instance-vpn1-af-ipv4)#quit
huawei(config-vpn-instance-vpn1)#quit
```

2. Set up the adjacency relationship between PE devices through the BGP protocol.

- Configure the BGP protocol on the Layer 3 interface of PE1.

```
huawei(config)#interface loopback 0
huawei(config-if-loopback0)#ip address 10.1.1.4 255.255.255.255
huawei(config-if-loopback0)#quit
huawei(config)#bgp 2345
huawei(config-bgp)#peer 10.1.1.6 as-number 2345
huawei(config-bgp)#peer 10.1.1.6 connect-interface loopback 0
huawei(config-bgp)#ipv4-family unicast
huawei(config-bgp-af-ipv4)#peer 10.1.1.6 enable
huawei(config-bgp-af-ipv4)#quit
huawei(config-bgp)#ipv4-family vpnv4
huawei(config-bgp-af-vpnv4)#policy vpn-target
huawei(config-bgp-af-vpnv4)#peer 10.1.1.6 enable
huawei(config-bgp-af-vpnv4)#quit
huawei(config-bgp)#ipv4-family vpn-instance vpn1
huawei(config-bgp-vpn1)#import-route direct
huawei(config-bgp-vpn1)#quit
huawei(config-bgp)#quit
```

- Configure the BGP protocol on the Layer 3 interface of PE2.

```

huawei(config)#interface loopback 0
huawei(config-if-loopback0)#ip address 10.1.1.6 255.255.255.255
huawei(config-if-loopback0)#quit
huawei(config)#bgp 2345
huawei(config-bgp)#peer 10.1.1.4 as-number 2345
huawei(config-bgp)#peer 10.1.1.4 connect-interface loopback 0
huawei(config-bgp)#ipv4-family unicast
huawei(config-bgp-af-ipv4)#peer 10.1.1.4 enable
huawei(config-bgp-af-ipv4)#quit
huawei(config-bgp)#ipv4-family vpnv4
huawei(config-bgp-af-vpnv4)#policy vpn-target
huawei(config-bgp-af-vpnv4)#peer 10.1.1.4 enable
huawei(config-bgp-af-vpnv4)#quit
huawei(config-bgp)#ipv4-family vpn-instance vpn1
huawei(config-bgp-vpn1)#import-route direct
huawei(config-bgp-vpn1)#quit
huawei(config-bgp)#quit

```

3. Configure a GRE tunnel.

- Configure a GRE tunnel on PE1.

```

huawei(config)#interface tunnel 11
huawei(config-if-tunnel11)#tunnel-protocol gre
huawei(config-if-tunnel11)#ip address 10.1.4.1 255.255.255.0
huawei(config-if-tunnel11)#source 10.1.1.4
huawei(config-if-tunnel11)#destination 10.1.1.6
huawei(config-if-tunnel11)#quit

```

- Configure a GRE tunnel on PE2.

```

huawei(config)#interface tunnel 11
huawei(config-if-tunnel11)#tunnel-protocol gre
huawei(config-if-tunnel11)#ip address 10.1.4.2 255.255.255.0
huawei(config-if-tunnel11)#source 10.1.1.6
huawei(config-if-tunnel11)#destination 10.1.1.4
huawei(config-if-tunnel11)#quit

```

4. Configure OSPF by referring to [11.12.6.3 Configuration Example of OSPF](#).

5. Bind the Layer 3 interface to the VPN.

```

huawei(config)#vlan 100 smart
huawei(config)#interface vlanif 100
huawei(config-if-vlanif100)#ip binding vpn-instance vpn1
huawei(config-if-vlanif100)#ip address 10.10.10.10 255.255.255.0
huawei(config-if-vlanif100)#quit

```