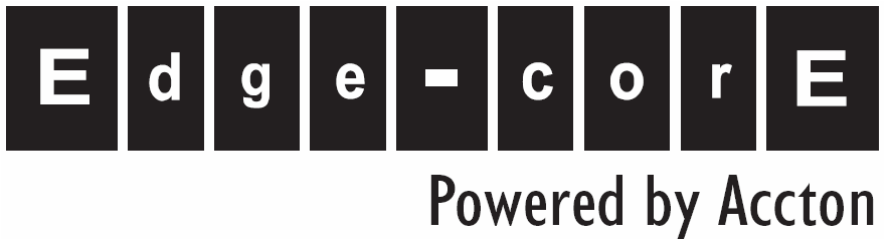

ES4704(10)BD MPLS
Management Guide

www.edge-core.com

Content

Chapter 1 MPLS Overview

1.1 MPLS Overview

MPLS (Multiprotocol Label Switching), originating from IPv4, was first designed for improving the forwarding speed. Its core technology can be extended into multiple network protocols, including IPv6 (Internet Protocol version 6), IPX (Internet Packet Exchange), Appletalk, DECnet, CLNP (Connectionless Network Protocol) and etc, since the “Multiprotocol” in MPLS means supporting multiple protocols. MPLS technology is a combination of fast switch and L3 route forwarding hence can satisfy the network requirement of various new applications.

1.1.1 MPLS Introduction

Forwarding Equivalence Class

MPLS, as a class-based forwarding technology, will put packets with the same forwarding mode into a class named as FEC (Forwarding Equivalence Class). The same FEC group will be treated with the same way in MPLS networks. FEC is a group of L3 messages, which will be forwarded along the same path, at the same priority level, and in the same mode. There are two steps to finish the forwarding process:

- ☞ Analyze the packet header and divide packets into FEC
- ☞ Map the FEC to the next-hop

In traditional IP forwarding networks, each router will process the same packet with the above two steps. FEC can include one or more FEC units. All of them are L3 message packets that can be mapped to the same LSP.

At present, there are two types of FEC:

- ☞ Address Prefix: Use the Address Prefix to identify a FEC unit, whose length ranges from 0 to the full address length. Each Address Prefix FEC unit corresponds with a destination subnet.
- ☞ Host Address: Use the Host Address to identify a FEC unit, as each unit corresponds with a host address.

The division rules of FEC is very flexible, which can be any combination of source address, destination address, source port, destination port, protocol type, VPN and etc. For instance, in the traditional IP forwarding using the Longest Prefix Match Algorism, all packets targeted at the same destination address belong to one FEC.

Label

In MPLS networks,,each specific FEC will be encoded at the edge LSR into a label - a short, fixed-length value, which will be added to the head of packets and turn them into label packets, before they are forwarded. Besides a segment identifying FEC, labels also include a COS segment, and thus representing FEC, precedence, and service class as a whole. LSR will divide packets reaching different ports into different FEC to establish the foundation of VPN. When a LSR creates a new FEC, it will also create a corresponding label, and advertise it to all peers. LSR maintain both incoming and outgoing labels. To implement load sharing, one FEC may correspond with multiple labels, but one label can only represent one FEC.

Labels, being carried in packet header, don't include topology information, and is only locally meaningful. The label length is 4 bytes. The figure demonstrates its encapsulation structure:

Fig 1-1 The Encapsulation Structure of a Label

There are 4 fields in a label:

- Label：The label value, whose length is 20 bits, a pointer for forwarding.
- Exp：3bits, used by QoS.
- S：1bit, the label's layered structure supported by MPLS, that is, there are multiple label layers. The value 1 represents the bottom-most layer of label.
- TTL：8bits, serves the same purpose as the TTL (Time To Live) in IP packets.

The label, like VPI/VCI of ATM and DLCI of Frame Relay, is identification for connections. If there is a label field in the link-layer protocol, such as VPI/VCI of ATM and DLCI of Frame Relay, the label will be encapsulated in these fields, otherwise, in a transitional layer between the link layer and the IP layer. Thus, labels can be supported by any link layer protocol.

Label Space

LSR can distribute a different label for a FEC according to its ingress port. As a result, packets from different ports can be forwarded independently, which is the basic foundation of VPN. To enhance the utilization efficiency of labels, MPLS provides the concept of label space, which is a label prefix. By allocating FECs belonging to different label spaces with the same label, the boundary of label is actually expanded. The label space is only meaningful when allocating labels, but not when forwarding them.

Label Switching

There is no need to analyze packet header in non-edge LSRs, instead, the label will be used as a pointer to the next-hop egress port and a new label. The label packet will

replace the old label with the new one and then be forwarded through the specified egress port. Label switching will simplify and accelerate the forwarding process, and realize applications like VPN, QoS, traffic engineering and etc.

Label Switching Router

LSR (Label Switching Router) is the basic element of a MPLS network, with all LSRs supporting MPLS technology.

LSR is a device able to forwarding packets according to their label value. A LSR connecting an IP route network and a MPLS switching network is called an Edge LSR. Such a LSR is able to adding labels to IP messages and forwarding data according to LSP, or deleting MPLS packet labels and forwarding data according to the IP routes. Each LSR must be distributed a global-alone LSR ID, usually get an interface IP address of LSR. Assume that, LSR Ru and Rd agree on the map between the label L and the FEC F. Packets can be forwarded from Ru to Rd based on the label L, in which case, Ru is the upstream LSR, and Rd the downstream LSR, that is to say, the forwarding of packets id always from the upstream LSR to the downstream one.

Label Switched Path

The path a FEC follows in the MPLS network is called a LSP (Label Switched Path). Two adjacent LSRs in a LSP are separately called the upstream and downstream LSR, along the direction of data transmission. In the next figure, R2 is the downstream LSR of R1,while R1 is the upstream LSR of R2.

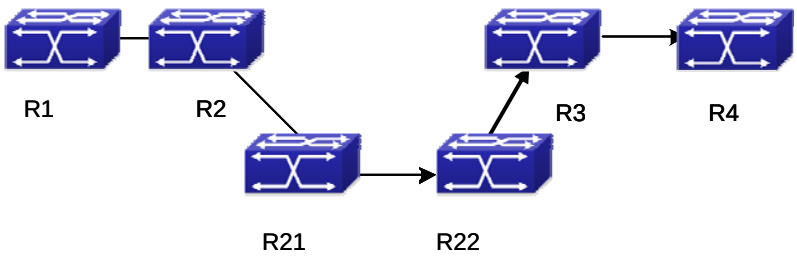

Fig 1-2 Label Switched Path LSP

The function of LSP, the same as the virtual circuit of ATM and Frame Relay, is a unidirectional path form the ingress of a MPLS network to its egress. Each router along the LSP is a LSR.

When downstream LSRs advertise labels to their upstream LSRs, all labels as a series and the LSR sequence compose a LSP. LSP will map the IP layer route information to a link layer switched path. LSP is a unidirectional packet forwarding path, along which, packets are always forwarded form an upstream LSR to a downstream one. To forward packets in the opposite direction, creating an entirely new and independent LSP is necessary. LSP always relates FEC with LSP. This relationship between FEC and LSP is

called mapping packets to LSP.

1. The rules of mapping packets to LSP:
   (1) If there is only one LSP, which includes a host-address FEC unit with the same destination address as the packet, map the packet to it;
   (2) If there is more than one LSP satisfying condition 1, map the packet to any one of them.
   (3) If there is only one LSP, whose address-prefix FEC unit can match the packet, map the packet to it.
   (4) If there is more than one LSP satisfying condition 3, choose a LSP based on the Longest Prefix Match principle;
   (5) If a packet will definitely pass through a specific egress LSR, and there is a LSP, the prefix FEC unit bounded to which is the address of that egress LSR, map the packet to this LSP.
2. Additional Rules:
   (1) If the destination address of the packet matches no LSP, the packet will be sent along the LSP with the same address as its Egress Router, as long as the LSP has an Address-prefix FEC unit.
   (2) If a packet matches two LSPs, one of which includes a host-address FEC unit, and the other an address-prefix FEC unit, always map the packet to the first one.
   (3) If the packet matches no LSP with a host-address FEC unit, it should not be sent along a LSP even if whose host-address FEC unit is the same as the packet's egress router address.
   (4) The creation of LSP is based on connections, which are the result of topology information rather than the demand of data flow. That is to say, no matter data forwarded by this router exist or not, the LSP will always be created.

Label Merging

With the LSR mapping multiple incoming labels to the same FEC, all these incoming labels will correspond with the same outgoing label and egress port. As a result, when packets with different labels reach the LSR, all outgoing packets will carry the same label. This process is called Label Merging. Label Merging can decrease the label number in the MPSL domain, but maybe at the cost of losing ingress port information of the packets.

If the LSR doesn't support label merging, when there are multiple label requests, it will initiate a new label request to the downstream LSR once for each of them, no matter they have the same FEC or not. Otherwise, only one label request will be implemented.

Label Distribution Protocol

LDP (Label Distribution Protocol) is the MPLS control protocol, like singling protocols in traditional networks, whose function includes classifying FEC, distributing labels, creating and maintaining LSP and etc.

MPSL supports multiple label distribution protocols, including protocols specially designed for distributing labels, like LDP, CR-LDP (Constraint-Based Routing using LDP), and existing ones capable of it after extension, like BGP (Border Gateway Protocol), RSVP (Resource Reservation Protocol). Besides, manually configured static LSP is allowed.

LSP Tunnel Technology

MPLS supports LSP tunnel technology. Even if the path between an upstream LSR and a downstream LSR in a LSP is not provided by the routing protocol, MPLS allows creating a new LSP connecting the two, making them the start and end of it separately. This new LSP is a LSP tunnel, which avoids encapsulating the tunnel via traditional network layer.

If the routes passed by a tunnel are the same as those from the routing protocol, this tunnel is Hop-by-Hop Routed Tunnel; or, it is an Explicitly Routed Tunnel.

Multi-layer Label Stack

If a packet is transmitted in more than one layer of LSP tunnel, it will carry multiple layers of labels – Label Stack. At the ingress and egress of each tunnel, MPLS will PUSH or POP a label accordingly.

The label stack follows the “Last-In-First-Out” principle, so MPLS will process labels from the stack top.

MPLS sets no limit to the label stack depth. If the label stack depth of a packet is m, the label at the stack bottom is level 1, and the one at the stack top will be level m. A packet without pushing any label will be treated as having an empty label stack (the label stack depth is 0).

1.1.2 MPLS Network Introduction

MPSL Network Structure

As demonstrated in the next figure, the basic unit composing the MPLS network is LSR; and a network consists of LSR is called a MPLS domain.

The LSR at the edge of a MPLS domain, connecting other customer networks is called LER (LER，Label Edge Router) , and the internal LSR is a core LSR. Core LSRs can either be routers supporting MPLS or ATM-LSR upgraded from ATM routers. LSRs in the domain communicate with each other via MPLS, while the MPLS domain edge is adapted via LER and traditional IP technologies.

Packets will be transmitted along a LSP composed of a series of LSRs after the ingress LER pushes a label to it. The ingress LER is called Ingress, egress LER called Egress, and routers in the middle called Trasit.

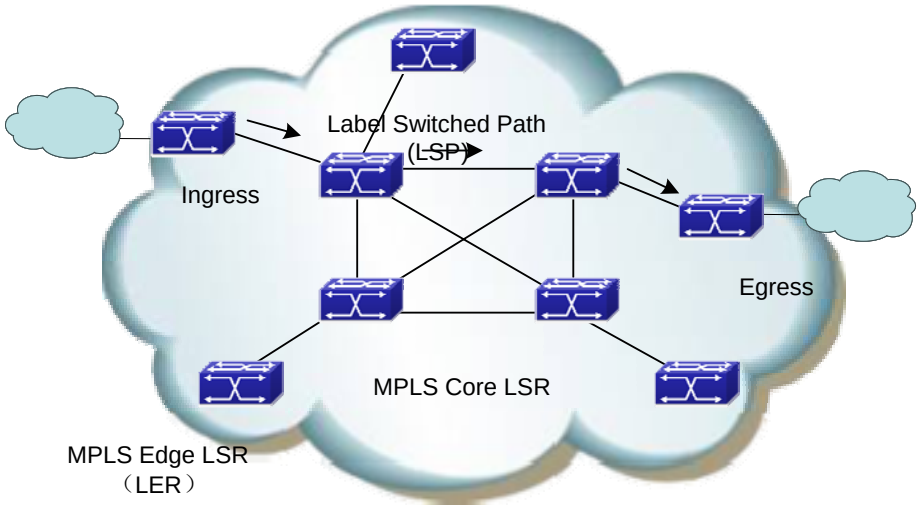

Fig 1-3 The MPLS Network Structure

The basic working process of MPLS based on the above figure :

First, LDP, together with traditional routing protocols (like OSPF, ISIS, etc) create route tables and LIB (Label Information Base) for FEC demanding services;

The ingress LER receives packets, completes L3 function, determines the FEC of the packets, labels them, and thus generates MPLS label packets.

Then, LSR in the network will forward packets according to their labels and LFIB (Label Forwarding Information Base) without implementing any L3 processing.

Finally, the egress LER of the MPLS will remove the label from the packet before the following IP forwarding.

To sum up, MPLS is neither a service or an application, but a tunnel technology, and a routing and switching technology platform integrated with label switching forwarding and network layer routing technology. This platform can support various high-level protocols and services with a certain guarantee of information security in the transmission.

1.1.3 Introduction to MPLS and Routing Protocols

When LDP creates LSP in hop-by-hop mode, it determines the next-hop based on the information from the forwarding table of each LSR along it. Since the information from forwarding tables are collected by routing protocols like IGP and BGP, LDP indirectly relates with them.

Besides, existing protocols like BGP and RSVP, can also distribute MPLS labels after extension.

Sometimes, it is necessary to extend some routing protocols in MPLS applications. For example, MPLS-based VPN requires extension to BGP, so that, BGP can distribute

the VPN (Virtual Private Network) route information; MPLS-based TE (Traffic Engineering) requires extension to OSPF or IS-IS protocol, to carry link status information.

1.1.4 MPLS Application Introduction

MPLS technology originally combines L2 switching and L3 routing technology to enhance the route lookup speed. As ASIC (Application-Specific Integrated Circuit) develops, route lookup speed has no longer been the bottleneck of network development. As a result, MPLS's advantage in accelerating forwarding disappears.

However, combining the powerful L3 switching function of IP networks and efficient forwarding mechanism of traditional L2 networks, MPLS uses connection-oriented method at the forwarding plane, similar to the current L2 network. As a result, it can easily achieve seamless convergence of IP and L2 networks like ATM and Frame Relay, and provide better solutions for applications like QoS, TE and VPN.

MPLS-based VPN

Traditional VPN transmits private data in the public network via tunnel protocols like GRE, L2TP, and PPTP. Since LSP is a public network tunnel itself, MPLS is innately advantageous in implementing VPN.

MPLS-based VPN will connect different branches of a private network via LSP to form an integrated one. It also supports the intercommunication control between different VPN.

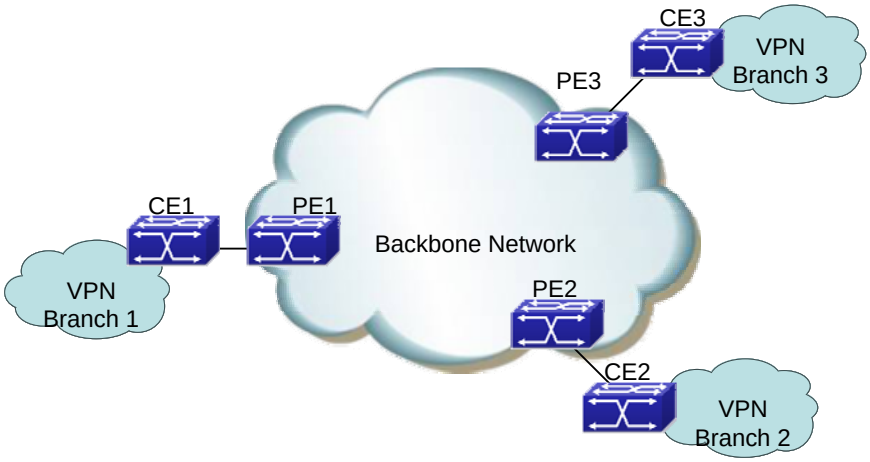

Fig 1-4 MPLS-based VPN

The above figure demonstrates the basic structure of MPLS-based VPN: CE (Customer Edge), a router, a switch or a host; PE (Provider Edge), in the backbone network.

PE manages VPN customers, establishes LSP connections between different PE and distributes routes to different branches of a VPN customer. The route distribution between PE is usually achieved via LDP or extended BGP.

MPLS-based VPN supports IP address multiplexing of different branches, and the intercommunication between different VPN. Different with traditional routes, VPN route contains extra identification of branches and VPN, making BGP extension a necessity, in order to carry VPN route information.

MPLS-based TE

MPLS-based TE and the Diff-serv feature can provide data flow at different precedent level with different service while ensuring a high network utility efficiency, and hence, be able to provide low-delay, low packet loss rate services with a guaranteed bandwidth to various data flows like voice and video.

Considering the difficulty of deploying TE over the whole network, the Diff-serv model is usually the method of implementing QoS in real networking resolutions.

The basic mechanism of Diff-Serv is mapping a service to a certain service class at the network edge, according to the required service quality. The service is uniquely identified via the DS segment (originated from ToS field) of IP packet. According to the segment, the routers in the backbone network will apply pre-configured service policy to different services, ensuring the service quality.

The service quality class mechanism and the label mechanism of Diff-Serv are similar to the label distribution mechanism of MPLS. In fact, the MPLS-based Diff-Serv is implemented via the combination of the DS distribution and MPLS label distribution.

1.1.5 MPLS PHP

In the MPLS network, the core LSR will forward packets according to their labels. The Egress router (Egress LER) will remove the label before implementing IP forwarding.

In fact, in simple MPLS applications, where the Egress routers only implement IP forwarding, labels will become useless. In such cases, popping the labels out via the Penultimate Hop Popping feature at the penultimate router will stop the Egress router from processing the labels.

1.2 Commands for MPLS

1.2.1 mpls egress-ttl

Command：mpls egress-ttl <*0-255*>

no mpls egress-ttl

Function: Set the TTL value of IP messages through the egress LSR of LSP; the no operation will cancel the configured value.

Parameters: <***0-255***>: the TTL value.

Default: None.

Command Mode: Global Mode

Usage Guide: The egress-ttl configuration of the LSR will be the TTL of all IP messages forwarded through this egress LSR.

Example: Set the egress TTL as 45.

Switch#config terminal

Switch(config)#mpls egress-ttl 45

Related Commands: mpls ingress-ttl

1.2.2 mpls enable

Command：mpls enable

no mpls enable

Function: Enable mpls protocol; the no command will disable the protocol.

Parameters: None.

Default: The mpls protocol is disabled by default.

Command Mode: Global Mode.

Usage Guide: Implementing this command will enable the mpls protocol.

Example:

Switch(config)#mpls enable

1.2.3 mpls ingress-ttl

Command：mpls ingress-ttl <*0-255*>

no mpls ingress-ttl

Function: Set the TTL value of IP messages through the ingress LSR of LSP; the no operation will cancel the configured value.

Parameters: <***0-255***>: the TTL value.

Default: None.

Command Mode: Global Mode

Usage Guide: The ingress-ttl configuration of the ingress LSR will be the TTL value in the

top label of all MPLS messages entering this LSP through the LSP ingress router.

Example: Set the ingress TTL as 45.

Switch#config terminal

Switch(config)#mpls ingress-ttl 45

Related Commands: mpls egress-ttl

1.2.4 show mpls

Command: show mpls

Function: Display all label data.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Implementing this command will display all label data.

Example: Display all label data.

Switch#show mpls

Minimum label configured: 16

Maximum label configured: 1048575

Per label-space information:

Label-space 0 is using minimum label: 16 and maximum label: 1048575

Custom ingress TTL configured: none

Custom egress TTL configured: none

Display	Explanation
Minimum label configured	The configured minimum label
Maximum label configured	The configured maximum label
Per label-space information	The space information of each label
Label-space 0 is using minimum label	The minimum label can be used by label-space 0.
Label-space 0 is using maximum label	The maximum label can be used by label-space 0.
Custom ingress TTL configured	The ingress TTL configured by users
Custom egress TTL configured	The egress TTL configured by users

1.2.5 show mpls enable

Command: show mpls enable

Function: Display whether the mpls is enabled.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Implementing this command will display whether the mpls is enabled.

Example: Display whether the mpls is enabled.

Switch#show mpls enable

Switch#MPLS enable has been on

Related Commands: mpls enable

1.2.6 show mpls forwarding-table

Command: show mpls forwarding-table

Function: Display the information of all LSP created by the switch as an ingress router, and FTN (FEC to Next-Hop-Label-Forwarding-Entry) marked as selected.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Implementing this command will display the information of all LSP created by the switch as an ingress router, and FTN marked as selected.

Example: Display the information of all LSP created by the switch as an ingress router.

Switch#show mpls forwarding-table

Codes: > - selected FTN, B - BGP FTN, C - CR-LDP FTN, K - CLI FTN,

L - LDP FTN, R - RSVP-TE FTN, S - SNMP FTN, U - unknown FTN

Code	FEC	FTN-ID	Pri	Nexthop	Out-Label	Out-Intf
L>	200.200.1.2/32	1	Yes	202.200.1.1	640	Vlan3
L>	202.200.1.0/24	2	Yes	0.0.0.0	3	Vlan3
L>	202.200.2.0/24	3	Yes	202.200.1.1	3	Vlan3

Display	Explanation
Code	Type
FEC	The FEC Address
FTN-ID	The FTN ID
Pri	The Primary lsp label
Nexthop	The next-hop address
Out-Label	The Out label
Out-Intf	The Out interface

1.2.7 show mpls ftn-table brief

Command: show mpls ftn-table brief

Function: Display brief information of public network FTN routers created by MPLS on the switch.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Implementing this command will display brief information of public network FTN routers created by MPLS on the switch.

Example:

Switch#show mpls ftn-table brief

FTN Entry Brief Information

FEC	Out-Label	Out-intf	Next hop	Oper-code	Op-State	Vrf
100.1.1.0/24	3	Vlan10	0.0.0.0	Push	Up	0

1.2.8 show mpls ftn-table detail

Command: show mpls ftn-table detail

Function: Display detailed information of public network FTN router created by MPLS on the switch.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Implementing this command will display detailed information of public network FTN routers created by MPLS on the switch.

Example:

Switch#show mpls ftn-table detail

FTN ID : 1
VrfIndex : 0
Fec : 100.1.1.0/24
Nexthop addr : 0.0.0.0
Owner : LDP
Primary : Yes

Row Status : Active
Exp-bits : 0X0
Incoming DSCP : none
Tunnel ID : 0
Protected LSP id : 0
QoS Resource id : 0
In-Label : 0
In-Interface : N/A
Out-Label : 3
Out-Interface : Vlan10
Admin Status : Up
Oper Status : Up
Oper Code : Push

Display	Explanation
FTN ID	The FEC ID
VrfIndex	The Vrf Index
Fec	The Fec Address
Nexthop addr	The next-hop address
Owner	The protocol creating the cross-link table
Primary	Whether it is primary or not.
Row Status	The Row status
Exp-bits	The experiment bits
Incoming DSCP	Differentiated Services CodePoint.
Tunnel ID	The Tunnel ID
Protected LSP id	The id of protected LSP
QoS Resource id	The ID of Qos Resource
in label	The in label
In-Interface	The in interface
Out-Label	The out label
Out-Interface	The out interface
Admin Status	The administration status
Oper Status	The operation status
Oper Code	The operation code

1.2.9 show mpls ilm-table

Command: show mpls ilm-table

Function: Display the information of ILM routers created by MPLS on the switch.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Implementing this command will display the information of ILM routers created by MPLS.

Example:

Switch#show mpls ilm-table

In-Label	Out-Label	In-Intf	Out-Intf	Nexthop	FEC
640	3	Vlan1	Vlan2	24.1.1.2	2.2.2.2/32
641	3	Vlan2	Vlan1	14.1.1.1	1.1.1.1/32

Display	Explanation
In-Label	The in label
Out-Label	The out label
In-Intf	The in interface
Out-Intf	The our interface
Nexthop	The next-hop address
FEC	The fec address

1.2.10 show mpls vrf-table

Command: show mpls vrf-table [vrf-name]

Function: Display the detailed information of all configured VRP ingresses.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Implementing this command will display the detailed information of all configured VRP ingresses. If there is a specified VRF in the parameter, only details about this ingress will be displayed.

Example:

Switch#show mpls vrf-table

Output for VRF table with id: 1

FTN ID : 1
VrfIndex : 1
Fec : 10.1.1.0/24
Nexthop addr : 0.0.0.0
Owner : BGP
Primary : Yes
Row Status : Active
Exp-bits : 0X0
Incoming DSCP : none
Tunnel ID : 0
Protected LSP id : 0
QoS Resource id : 0
In-Label : 0
In-Interface : N/A
Out-Label : 0
Out-Interface : Vlan20
Admin Status : Up
Oper Status : Up
Oper Code : Deliver to IP

Display	Explanation
FTN ID	The FEC ID
VrfIndex	The Vrf Index
Fec	The Fec address
Nexthop addr	The next-hop address
Owner	The protocol creating the cross-link table
Primary	Whether it is primary or not
Row Status	The row status
Exp-bits	The experiment bits
Incoming DSCP	Differentiated Services CodePoint.
Tunnel ID	The tunnel ID
Protected LSP id	The ID of protected LSP
QoS Resource id	The ID of Qos resource
in label	The in label
In-Interface	The in interface
Out-Label	The out label
Out-Interface	The out interface
Admin Status	The administration status

Oper Status	The operation status
Oper Code	The operation code

Chapter 2 LDP

2.1 LDP Introduction

LDP protocol is used for label distribution in the MPLS label switching environment, and only applies to networks capable of label switching. LDP, integrated with traditional routing algorithm, distribute labels, advertise <label, FEC> map, create and maintain Label Forwarding Information Base and LSP, by transmitting various messages via TCP connections. LDP is used to distributing public network label in the MPLS VPN environment.

LDP doesn't create any route; instead, it obtains routes from the system, distributes labels for them and advertises the labels to its upstream router. At the same time, for the FEC having a downstream, LDP will receive a label from the downstream, take it as the outgoing label and create a label switched path, which means to create an entry of switching the incoming label as the outgoing one. If the label distributed by the downstream is 3, the LDP will create an entry of popping out the label.

LDP is defined in RFC3036; and its latest standard is RFC5036. It switches the map between labels and routes via the TCP connection between peers. Two neighbor discovery modes are supported by LDP: the basic mode (automatic discovery) and the extended mode (specified). The automatic discovery of peers is implemented via the UDP multicast messages to all routers (224.0.0.2), using the port 646 in both TCP and UDP messages.

The main process is as follows:

- Discover and maintain neighbors: after LDP is global enabled and interface enabled, it will send multicast Hello messages on the specified interface (unless it disables the multicast-based neighbor discovery) to advertise the network about its existence. The Hello messages will carry its transmission address, the address for TCP connections. The adjacency will be created when receiving Hello messages from other LSRs, and maintained by periodically sending Hello messages.
- Establish and maintain sessions: LDP sessions are TCP-based; First, compare the transmission address in the Hello message from the other end and that from this end, set the one with bigger value as ACTIVE and the other PASSIVE. The ACTIVE router will initiate a connect request to establish a TCP connection (to avoid the similar connection conflict problems suffered by BGP neighbors). Once the TCP connection is established, the two parts will send initialization messages

to negotiate session parameters. A session will be established once the negotiation succeeds. After that, the two neighbors will send the local interface address list and label information to each other. To hold the connection when there is no data, KEEPALIVE messages will be sent.

- ☞ Create and maintain LSP: a session is necessary for each pair of LSR peers to switch label information, which create LSP by switching FEC and label binding messages.
- ☞ Cancel sessions: Without any message from the other end for a long time, LDP will disconnect the session and notify the close of the session to the other end by sending a notification messages.

Please notice that, LDP won't distribute labels for default routes, or BGP routes (unless explicitly specified).

2.1.1 Basic Concept of LDP

LDP Peer

When distributing labels to FEC, LDP needs to advertise this label and its meaning in the MPLS network to create LSP. LSR is a LDP peer when switching label information via LDP. LDP peers obtain each other's label map and other messages.

LDP Session

Two LSR will create a LDP session between each other after exchanging LDP Discovery Hello messages. LSP relies on LDP sessions to exchange messages like label map, release.

Two steps to establish a LDP session

- ☞ Establish the transmission connection.
- ☞ Initialize the session

Two types of LDP session:

- ☞ Local LDP Session: the two LSR establishing the session are directly connected.
- ☞ Remote LDP Session: the two LSRs establishing the session are indirectly connected

LDP Message Type

Four types of LDP messages:

- ☞ Discover message: to advertise and maintain the existence of LSR in the network;
- ☞ Session message: to create, maintain and terminate the sessions between LDP peers;
- ☞ Advertisement message: to create, change and delete the map from label to FEC;

- Notification message: to provide advice messages and error notices.

To ensure the reliable sending of LDP messages, LDP uses TCP to send Session, Advertisement and Notification messages, and UDP to send Discovery ones.

2.1.2 Introduction to LDP Message Format

LDP PDU

LDP PDU includes a LDP header and several LDP messages. The LDP header format is as follows:

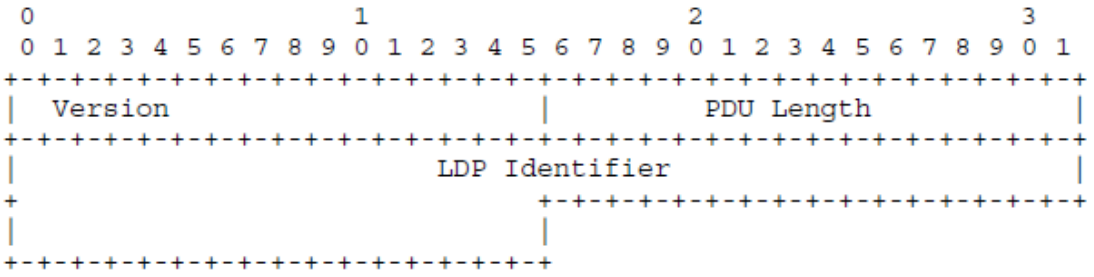

Fig 2-1 The LDP Header Format

- Version：The LDP version, I byte. The current LDP version is 1.
- PDU Length：The total length of the LDP message (in byte), 2 bytes.
- LDP ID：LDP ID, 6 bytes. The first 4 bytes is the globally unique LSR ID, and the rest 2 are label space ID, which is 0 when it comes to the global label space.

TLV Encoding

LDP encapsulates parameters in LDP messages via TLV (Type-Length-Value). The LDP TLV format is as follows:

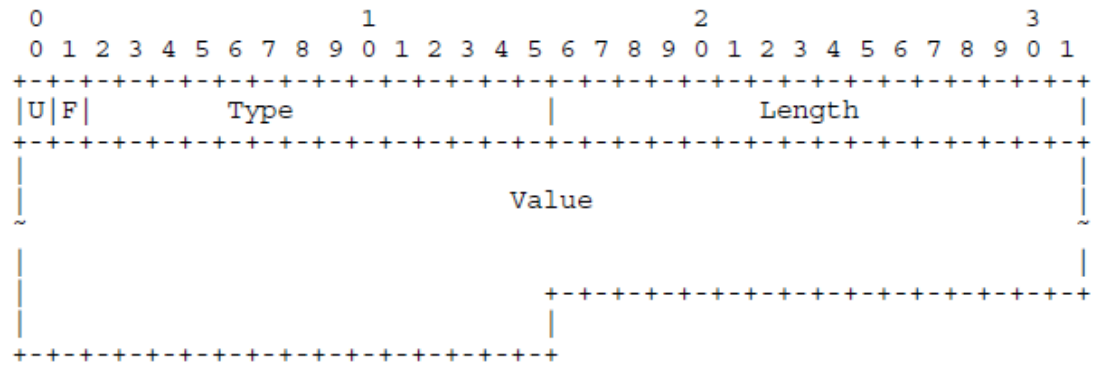

Fig 2-2 The TVL Format of LDP

- U bit：Unknown flag, I bit. If the U flag is 0, LSR should notify the source LSR of the packet and ignore the whole message; otherwise, ignore this TLV parameter

and analyze other ones normally.

- ☞ F bit：Forwarding unknown TLV flag, 1bit. This flag only applies to LDP messages with unknown TLV and a U bit set as 1. If the F flag is 0, stop forwarding unknown TLV parameters; otherwise, forward them;
- ☞ Type： Type, 14 bits.
- ☞ Length： Length, 1 byte. The length of TLV value segment.
- ☞ Value：The Value segment, whose length is defined by the parameter of “Length”.
- ☞ The Value segment of TLV can also contain TLV parameters, meaning that, TLV are embeddable. The first byte of TLV doesn’t need alignment.

Currently defined TLV types:

TLV	Type
FEC	0x0100
Address List	0x0101
Hop Count	0x0103
Path Vector	0x0104
Generic Label	0x0200
ATM Label	0x0201
Frame Relay Label	0x0202
Status	0x0300
Extended Status	0x0301
Returned PDU	0x0302
Returned Message	0x0303
Common Hello Parameters	0x0400
IPv4 Transport Address	0x0401
Configuration Sequence Number	0x0402
IPv6 Transport Address	0x0403
Common Session Parameters	0x0500
ATM Session Parameters	0x0501
Frame Relay Session Parameters	0x0502
Label Request Message ID	0x0600
Vendor-Private	0x3E00- 0x3EFF
Experimental	0x3F00- 0x3FFF

2.1.3 LDP Label Management

In the MPLS system, the downstream LSR determines the distribution of label to specific FEC, and notifies the upstream. That is to say the labels are specified by the

downstream and distributed from downstream to upstream.

Label Advertisement Mode

In the MPLS domain, packets will be forwarded to the downstream LSR with the downstream LSR label after the label switching process in the upstream LSR. The FEC labels distributed by the downstream LSR apply only to itself and the upstream LSR, and should be advertised to the upstream LSR. MPLS defines two label advertisement modes for the downstream LSR passing labels to its upstream LSR:

- DoD（Downstream On Demand）: LSR only distributes and advertises a label for the specified FEC after receiving a label request message from the upstream.
- DU（Downstream Unsolicited）: LSR distributes and advertises a label for the specified FEC without receiving a label request message from the upstream. It will automatically send label map information and notify the upstream LSR.

These two modes can be mixed, with each LSR interface configured independently to use one of them. During initialization, the upstream and downstream LSR have to exchange their label advertisement mode information to reach an agreement on the mode. Otherwise the creation of LSP will fail.

The figure demonstrates the process of LDP label advertisement:

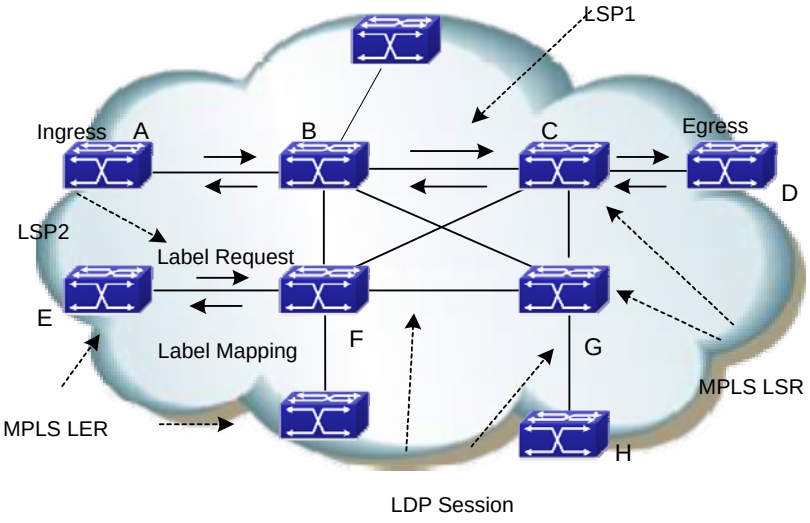

Fig 2-3The Process of Label Advertisement

For example, as for LSP1 in the above figure, LSR B is the upstream LSR of LSR C, while LSR C is the downstream LSR of LSR B.

The main difference of two label advertisement mode lies on whether the label advertisement is DoD or DU.

The following is the detailed label advertisement process of these two modes:

(1) DoD（downstream-on-demand）

The upstream LSR send a Label Request Message, which carries FEC description to its downstream LSR. The downstream LSR will distribute a label for this FEC, and respond to the upstream with the mapped label via a Label Mapping Message.

When will the downstream LSR respond the Label Mapping Message depends on the label advertisement mode it adopted.

1) In Ordered mode, it will send the Label Mapping Message to the upstream only after receiving a Label Mapping Message from its downstream.
2) In Independent mode, it will immediately send the Label Mapping Message to the upstream no matter it receives a Label Mapping Message from its downstream or not.

Usually, the upstream LSR chooses the downstream LSR based on the routing table. In the above figure, all LSR along the LSP1 work in the ordered mode, while LSR F in LSP2 in the Independent mode.

(2) DU（downstream unsolicited）

The downstream LSR will automatically advertise the label mapping message to its upstream LSR after the LDP session successfully created. The upstream LSR will save the message and process it according to its retention mode.

Label Distribution Control Mode

In the MPLS domain, LSR generate a LSP from the ingress router and the egress router via switching labels, based on the route-forwarding path created by IGP in the MPLS domain. Only a complete path is useful for pack forwarding. The creation of LSP is the LSR label advertisement process; hence, controlling the creation of LSP is controlling the LSR label advertisement. MPLS defines two LSP control modes to determine when the downstream LSR will advertise labels to the upstream LSR:

- Ordered Mode: For a FEC label mapping of a LSR, the LSR only advertise the mapping to its upstream when it already has the label mapping of the FEC next-hop, or when it is the egress router of the FEC. The label advertisement of a flow starts from the egress router of this FEC flow, binding routers from downstream to upstream, thus to guarantee the mapping between labels and the flow is complete and coherent in the whole network. The ordered mode can prevent loop more effectively.
- Independent Mode: LSR doesn't have to wait for the label of the FEC next-hop to advertise labels to its peer. It can notify label mapping to the LSR connected to it at any time. This mode may cause the LSR advertise a label to its upstream before receiving one from its downstream. This mode can accelerate the creation and aggregation of LSP.

Requirements for LSR to be an Egress router:

- The FEC quotes the LSR address;

- The FEC next-hop router locates outside the label switching network;
- The FEC unit passes the route area, such as another OSPF SUMMAERY domain, or another autonomy system of OSPF, BGP.

Label Retention Mode

Label Retention Mode determines how the LSR handles the currently useless mapping from label to FEC it received. In DU mode, the upstream LSR may receive a large number of <FEC, label> map sets from the downstream LSR, in which case, only when the FEC in the map set is the local FEC next-hop of the upstream LSR, this map set is meaningful for the label forwarding. MPLS defines two label retention modes to determine the processing of currently useless map set.

- Conservative Mode: the LSR will reserve the label mapping received from the neighbor LSR no matter the neighbor is its next-hop or not. The advantage of this mode is that it only creates and maintain the labels that meaningful for data forwarding, a very significant feature when the label space is limited (ATM switching).
- Liberal Mode: the LSR only save label maps from the neighbor LSR which is its next-hop. The advantage of this mode is that the expense of processing route changes is very low; and the disadvantage is many useless labels will be advertised and maintained.

In the Liberal label retention mode, LSR can adapt rapidly to route changes; in the Conservative mode, LSR can distribute and save relatively less labels. The Conservative retention mode, together with the DoD mode, usually applies to LSR with limited label space.

Some Basic Concepts of Label Switching

- NHLFE: Next Hop Label Forwarding Entry. It is used to describe the operation to the label, including Push and Swap.
- FTN (FEC to NHLFE map): the process of mapping FEC to NHLFE on the Ingress router.
- ILM (Incoming Label Map): the process of mapping received labels to NHLFE by LSR.

The Label Switching Process

The Ingress LER divides the packets entering the network into FECs. The packets belonging to the same FEC will follow the same path - LSP, in the MPLS domain. LSR will distribute a label for the incoming FEC packet and forward it through the corresponding interface.

The detailed process of label switch is as follows:

- All LSRs along the LSP will create an ILM first, the entries in which are the rule of mapping the incoming labels.

- ☞ LSR will map the labels of received packets to NHLFE;
- ☞ LSR will find the corresponding NHLFE in the LIB based on the label, replace it with the new label and then forward the label packet.

2.1.4 LDP Session

There are four steps to establish a LDP session:

- ☞ Discover
- ☞ Establish and maintain the session
- ☞ Create LSP
- ☞ Cancel the session

Discover

At this step, the LSR will send Hello messages periodically to adjacent LSRs, notifying them about its existence, in order to establish a session. In the basic discover mechanism, LSR will discover its LDP peers automatically via this process without manual configuration. There are two discover mechanisms:

- ☞ Basic Discover Mechanism

The Basic Discover Mechanism is used to discover local LDP peers – LSRs directly connected via the link layer, and create a local LDP session. In this mode, the LSR will send LDP Link Hello messages periodically via UDP messages to the multicast address marked as “all routers in the subnet”.

LDP Link Hello messages carry the LDP ID of the interface and other related information. If the LSR receives a LDP Hello Message at an interface, it means that there is a LDP peer at this interface (Link Layer).

- ☞ Extended Discover Mechanism

The extended discover mechanism is used to discover remote LDP peers – LSRs not directly connected via the link layer, and created remote LDP sessions. In this mode, the LSR will send LDP Targeted Hello messages periodically to the specified IP address via UDP messages.

LDP Targeted Hello messages carry the LDP ID of the interface and other related information. If the LSR receives a LDP Targeted Message at an interface, it means that there is a LDP peer at Network Layer.

Establish and Maintain the Session

After discovering a LDP peer, LSR will began to establish the session in two steps:

- ☞ Establish the transmission layer connection, that is, a TCP connection between LSRs;
- ☞ Initiate the session between the LSRs, negotiate all concerning parameters, such as the LDP version, the label advertisement mode, the timer value, the

label space. After the negotiation succeeds, the session is established between the LSRs.

The session will be maintained by Keepalive messages after established.

Create LSP

The process of creating LSP is mapping FEC and labels and advertising the maps to the adjacent LSRs along the LSP, which is realized via LDP. Take DoD mode as the example, the main steps are as follows:

(1) When the network routes change, if an edge router finds out a new destination address in its route table which belongs to none of the existing FECs, it needs to create a new FEC for this destination address. The edge LSR determines the route for the FEC, initiates a label request message to its downstream LSR, and specifies for which FEC this label request is.

(2) The downstream receiving the label request message will save this message, finds the corresponding FEC next-hop according to the local route table and then sends a label request message to its downstream.

(3) When the label request message reaches the destination router or the egress router of the MPLS network, if the router has available labels, and judges the label request messages as legal, it will distribute a label for the FEC, and send a label mapping message containing the label information to its upstream;

(4) The LSR receiving the label mapping message will check the state of label request messages saved locally. If there is a corresponding label request message of a FEC label mapping message in the data base, LSR will distribute a label for the FEC, and add a new entry in its LFIB, and then send the label mapping information to its upstream.

(5) When the ingress LSR receives a label mapping message, it also should add a corresponding entry in its LFIB, and thus finish the creation of LSP.

Cancel the session

LDP maintains adjacency by checking Hello messages. It also maintains session by checking Keepalive messages. If there is no Keepalive message received within a certain period of time, the LDP session will close the connection.

Each LDP session can include one or more Hello adjacencies. LDP maintains Hello adjacency via periodical Hello messages. If there is no LDP Discovery Hello message received within a certain period of time, the LDP session will close the Hello connection. When closing the last Hello adjacency in the LDP session, LDP will send notification messages, and close the transmission connection.

2.1.5 LDP Loop Detection

Creating LSP in the MPLS domain also needs to prevent loops. The LDP loop detection mechanism can detect LSP loops and avoid them.

To detect loops in the MPLS domain, all LSRs should be enabling the loop detection. But when establishing LDP sessions, the configurations of loop detection on the two parties don't have to be the same.

There are two LDP loop detection modes:

The maximum hop count

It is the number of LSR passed by the label messages (including label mapping and label request). When LSR transmits label information with the hop-count parameter, it will first increase the hop count by 1. When the hop count reaches the configured maximum value, it means that a loop exists, and the LSP creation will fail. If the hop count is 0, it means the hop count is unknown. The hop count of label messages is always 0. The default maximum hop count is 255.

Path Vector

It is used to record the path information in label mapping or label request messages. At each hop, the LSP checks whether its LSR ID is in the record. The following two conditions mean the existence of a loop and the failure of the LSP creation.

- ☞ There is a record of this LSR in the path vector record;
- ☞ The hop count of the path exceeds the configured maximum value.

If no record of its LSR ID is found, a new one will be added. The maximum value of path vector is the same as that of the hop count.

2.2 LDP Configuration

LDP Configuration Task Sequence:

1. Enable MPLS Globally (Necessary)
2. Enable LDP (Necessary)
   (1) Enable/Disable the LDP module
   (2) Enable/Disable label-switching on the interface
   (3) Enable/Disable LDP module on the interface
3. Configure the LDP parameters (optional)
   (1) Configure the LDP label management mode
      1) Configure the LDP label retention mode
      2) Configure the LDP label advertisement mode
      3) Configure the LDP label control mode
   (2) Configure the LDP loop detection
      1) Enable/Disable the LDP loop detection
      2) Set the maximum hop count of the LDP loop detection

(3) Configure the LDP specified peers

(4) Configure other LDP parameters

1) Configure the aging time or interval of each timer

2) ID Configure the LDP router ID

3) Configure the TCP interface address of LDP

4) Configure the LDP to discover peers via multicast Hellos or not.

5) Configure the LDP to import BGP routes or not.

6) Enable/Disable the LDP label merging capability

7) Configure the LDP to transmit release messages or not.

8) Configure the LDP to retry or not when the label request is rejected.

9) Hello Configure the LDP to receive Hello from specified targets

4. Clear LDP connections or adjacencies.

1. Globally enable MPLS

Command	Explanation
Global Mode	
mpls enable **no mpls enable**	necessary Enable MPLS; the no operation will disable MPLS.

2. Enable LDP

It is easy to implement basic configurations of LDP. Usually users only have to enable the LDP switch, and enable it on the interface where the LDP will work. Please notice that, the interface with LDP enabled should enable label switching.

Command	Explanation
Global Mode	
[no] router ldp	Necessary LDP Enable/disable LDP; disabled by default
Interface Configuration Mode	
[no] label-switching	Necessary Enable/disable label-switching; disabled by default
ldp {enable|disable}	Necessary LDP Enable/disable LDP on the interface; disabled by default

3. Configure the LDP parameters

(1) Configure the LDP label management mode

1) Configure the LDP label retention mode

2) Configure the LDP label advertisement mode

3) Configure the LDP label control mode

Command	Explanation
Router Configuration Mode	
label-retention-mode {conservative|liberal}	Optional Configure the global label retention mode: Conservative or Liberal; it is liberal by default
advertisement-mode {downstream-on-demand|downstream-unsolicited}	Optional Configure the global label advertisement mode: **downstream-on-demand** or **downstream-Unsolicited.** This mode relates with the other two. The change of it will change the label retention mode and the global label path control mode at the same time. It is **downstream-unsolicited** by default
control-mode {ordered|independent}	Optional Configure the global label retention mode: Ordered or **independent**; it is **independent** by default
Interface Configuration Mode	
ldp label-retention-mode {conservative | liberal}	Optional Configure the label retention mode of the interface; the default value is the same as the global configuration. If the configuration differs with the global one, the interface configuration will take effect.
ldp advertisement-mode {downstream-on-demand|downstream-unsolicited}	Optional Configure the label advertisement mode of the interface; the default value is the same as the global configuration. If the configuration differs with the global one, the interface configuration will take effect.

(2) Configure LDP loop detection

1) Enable/disable LDP loop detection

2) Configure the maximum hop count of LDP loop detection

Command	Explanation
Router Configuration Mode	
[no] loop-detection	Optional Enable LDP loop detection, the no operation will disable it.

[no] loop-detection-count <*count*>	optional Configure the maximum hop count of LDP loop detection, whose default value is 255, the no operation will restore the default value.

(3) Configure the LDP specified peers

Command	Explanation
Router Configuration Mode	
[no] targeted-peer <*ip-addr*>	optional Configure the remote peer of the LDP targeted destination.

(4) Configure other LDP parameters

1) Configure the aging time or interval of each LDP timer
2) ID Configure LDP router ID
3) Configure the TCP interface address of LDP
4) Configure the LDP to discover peers via multicast Hellos or not,
5) Configure the LDP to import BGP routes or not.
6) Configure the LDP to enable label merging capability or not.
7) Configure the LDP to transmit release messages or not.
8) Configure the LDP to retry or not when the label request is rejected
9) Hello Configure the LDP to receive Hello from the specified targets

Command	Explanation
Route Configuration Mode	
[no] keepalive-interval <*interval*>	Optional Configure the interval of sending LDP keepalive messages, whose default value is 10 seconds; the no operation will restore the default value
[no] keepalive-timeout <*time-val*>	Optional Configure the LDP keepalive timeout, whose default value is 30 seconds; the no operation will restore the default value
[no] Hello-interval <*Hello-interval*>	Optional Configure the interval of sending multicast HELLO messages, whose default value is 5 seconds; the no operation will restore the default value

[no] hold-time <*hold-time* >	Optional Configure the LDP multicast peer hold time, whose default value is 15 seconds; the no operation will restore the default value
[no] targeted-peer-Hello-interval <*Hello -interval*>	optional Configure the interval of sending HELLO to specified targets, whose default value is 15 seconds; the no operation will restore the default value
[no] targeted-peer-hold-time <*hold-time*>	optional Configure the LDP targeted peer hold time, whose default value is 45 seconds; the no operation will restore the default value
Interface Configuration Mode	
[no] ldp keepalive-interval <*interval*>	optional Configure the interval of sending LDP keepalive messages on a specified interface; the no operation will restore the default value
[no] ldp keepalive-timeout <*time-val*>	Optional Configure the LDP keepalive timeout on a specified interface; the no operation will restore the default value
[no] ldp Hello-interval <*Hello-interval*>	Optional Configure the interval of sending LDP multicast HELLO messages on a specified interface; the no operation will restore the default value
[no] ldp hold-time <*hold-time*>	optional Configure the LDP multicast peer hold time on a specified interface; the no operation will restore the default value
[no] ldp targeted-peer-Hello-interval <*Hello-interval*>	optional Configure the interval of sending LDP HELLO messages to specified targets on a specified interface; the no operation will restore the default value

[no] ldp targeted-peer-hold-time <*hold-time*>	optional Configure the LDP targeted peer hold time on a specified interface; the no operation will restore the default value
router configuration mode	
[no] router-id <*ip-addr*>	optional Configure the LDP router ID, which is obtained automatically by default. The no operation will cancel the manually configured router ID, and automatically obtain a valid interface IP address as the router ID.
[no] transport-address <*ip-addr*>	optional Configure the IP address of LDP for TCP connections. Please notice that this address has to be that of a loopback interface on the main VRF. The no operation will cancel the manual configuration and let LDP automatically choose the TCP address
[no] multicast-Hellos	optional Configure the LDP to discover peers via multicast HELLOs, the no operation will do the opposite. Using multicast HELLO is the default setting.
[no] import-bgp-routes	Optional Configure the LDP to import BGP routes; the no operation will do the opposite. Not importing BGP routes is the default setting.
[no] global-merge-capability {merge-capable|non-merge-capable}	optional Configure the LDP to enable global label merging capability or not, the no operation will restore the default value.
[no] propagate-release	optional Configure the LDP to advertise label release messages to peers, the no operation will do the opposite. Not transmitting label release messages is the default setting.

[no] request-retry	optional Configure the LDP to retry 5 times when the label request is rejected, the no operation will disable the retry.
[no] request-retry-timeout <*time-val*>	optional Configure the retry interval, whose default value is 5 second, the no operation will restore the default value.
[no] targeted-peer-Hello-receipt	optional Configure LDP to receive HELLOs from specified targets, even the targeted peer is not configured on the host. Not receiving such HELLOs is the default setting. The no operation will restore the default configuration. Please notice that, if targeted LDP peers are configured, targeted-peer-Hello-receipt should be too.

4. Clear the LDP connections or adjacencies

Command	Explanation
Admin Mode	
clear ldp adjacency {<*ip-addr*>|*}	Optional Clear specified LDP adjacencies, "*" means all.
clear ldp session {<*ip-addr*>|*}	optional Clear specified LDP sessions, "*"means all.

2.3 Commands for LDP

2.3.1 advertisement-mode

Command: advertisement-mode {downstream-on-demand | downstream-unsolicited}

no advertisement-mode {downstream-on-demand | downstream-unsolicited}

Function: Configure the advertisement mode of labels; the no operation will cancel the configuration.

Parameters: None.

Default: Downstream-unsolicited mode

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: The LDP label advertisement mode determines how the LDP protocol handles the label advertisement. The protocol supports two modes: the first one is downstream-on-demand, which means, only when the upstream propose a label request, will the switch advertise a label to it; the other one is downstream-unsolicited, which means, the switch will allocate labels for all upstreams no matter they need one or not. It is recommended to use this mode together with the label retention modes and label control modes: the downstream-unsolicited mode corresponds with the liberal retention mode and the liberal mode, while the downstream-on-demand mode with the conservative retention mode and the ordered mode. It is better not to configure other attributes separately. If the interface is in the label advertisement mode, this command will have no effect.

Example: Configure the label advertisement mode as downstream-unsolicited.

Switch(config)#router ldp

Switch(config-router)#advertisement-mode downstream-on-demand

Related Commands: ldp advertisement-mode， label-retention-mode， ldp label-retention-mode

2.3.2 clear ldp adjacency

Command: clear ldp adjacency {<*ip-addr*>|*}

Function: Cancel the LDP adjacency.

Parameters: <*ip-addr*> is the adjacent IP address, * means to clear all adjacencies.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Implementing this command will clear the adjacency between the switch and its neighbor. With all configurations staying the same, the switch will recreate an adjacency with the neighbor through negotiation.

Example: Clear the adjacency with the neighbor 10.10.10.1.

Switch#clear ldp adjacency 10.10.10.1

2.3.3 clear ldp session

Command: clear ldp session {<*ip-addr*> | *}

Function: Clear LDP sessions.

Parameters: <*ip-addr*> is the IP address of the neighbor, * means to clear all sessions.

Default: None.

Command Mode: Admin Mode

Usage Guide: Implementing this command will clear session procedures. With all configurations staying the same, the switch will restart the session again. Please pay attention to the relationship between session and adjacency: multiple adjacencies may be created in one session.

Example:

Switch#clear ldp session *

2.3.4 clear ldp statistics

Command: clear ldp statistics

Function: Clear the LDP statistics.

Parameters: None.

Default: None.

Command Mode: Admin Mode.

Usage Guide: Implementing this command will clear all statistics.

Example:

Switch#clear ldp statistics

2.3.5 control-mode

Command: control-mode {ordered | independent}

no control-mode

Function: Configure the LSP control mode; the no operation will cancel the configuration.

Parameters: None.

Default: The default mode is “independent”.

Command Mode: LDP Protocol Configuration Mode

Usage Guide: LSP provides two different control modes: independent and ordered. The independent mode means that, there is no need to acquire a label map of the FEC from the downstream, which is required in the ordered mode when a LSR is advertising to the upstream a label map related with the specified FEC (unless this LSR is the egress router of this FEC). Hop-by-hop route applications usually work in the independent LSP control mode, and choose DU mode as the label advertisement mode. The ordered mode should be used along with the DoD mode.

Example: Configure the LSPcontrol mode to ordered.

Switch(config)#router ldp

Switch(config-router)#control-mode ordered

Related Commands: advertisement-mode, ldp advertisement-mode

2.3.6 debug ldp all

Command: debug ldp all

no debug ldp all

Function: Display all debug information related with LDP; when it is disabled, all debug switches will be disabled too.

Parameters: None.

Default: No display of debug information.

Command Mode: Admin Mode.

Example: Enable all debug switches.

Switch#debug ldp all

2.3.7 debug ldp dsm

Command: debug ldp dsm

no debug ldp dsm

Function: Display debug information related with the LDP downstream state machine; the no operation will disable the debug information.

Parameters: None.

Default: No display of debug information.

Command Mode: Admin Mode.

Usage Guide: Implementing this command will display the debug information related with the LDP downstream state machine. With it is enabled, debug information will be displayed when any the LDP protocol change related with the downstream state machine happens.

Example: Enable the debug switch.

Switch#debug ldp dsm

2.3.8 debug ldp error

Command: debug ldp error

no debug ldp error

Function: Display debug information of LDP errors; the no operation will disable the debug information.

Parameters: None.

Default: No display of debug information.

Command Mode: Admin Mode.

Usage Guide: When there is any LDP error, corresponding debug information will be displayed with this command enabled.

Example: Enable the debug switch.

Switch# debug ldp error

2.3.9 debug ldp events

Command: debug ldp events

no debug ldp events

Function: Display debug information of LDP events; the no operation will disable the debug information.

Parameters: None.

Default: No display of debug information.

Command Mode: Admin Mode.

Usage Guide: With this command enabled, the corresponding debug information of LDP events will be displayed.

Example: Enable the debug switch.

Switch#debug ldp events

2.3.10 debug ldp fsm

Command: debug ldp fsm

no debug ldp fsm

Function: Display debug information related with the LDP session finite state machine; the no operation will disable the debug information.

Parameters: None.

Default: No display of debug information.

Command Mode: Admin Mode.

Usage Guide: Enable (Disable) the debug information related with the LDP session finite state machine.

Example: Enable the debug switch.

Switch#debug ldp fsm

2.3.11 debug ldp hexdump

Command: debug ldp hexdump

no debug ldp hexdump

Function: Display the debug information of LDP messages in hex; the no operation will disable the debug information.

Parameters: None.

Default: No display of debug information.

Command Mode: Admin Mode.

Usage Guide: Enable (Disable) the hex debug information of received and sent LDP message contents.

Example: Enable the debug switch

Switch#debug ldp hexdump

2.3.12 debug ldp nsm

Command: debug ldp nsm

no debug ldp nsm

Function: Enable the debug information switch of the message communication between NSM and LDP; the no operation will disable the switch.

Parameters: None.

Default: No display of the debug information.

Command Mode: Admin Mode.

Usage Guide: Enable (Disable) the debug information of NSM, mainly including interface changes, route changes, entry distribution and etc.

Example: Enable the debug switch

Switch#debug ldp nsm

2.3.13 debug ldp packet

Command: debug ldp packet [receive|send|detail]

no debug ldp packet [receive|send|detail]

Function: Display the debug information of LDP messages; the no operation will disable

the switch.

Parameters: None.

Default: No display of debug information.

Command Mode: Admin Mode.

Usage Guide: Enable (Disable) the debug information of LDP receiving and sending messages. All information about sending and receiving messages will be displayed with the switch enabled while no such information will be printed. receive|send|detail separately means information of receiving/sending and detailed information.

Example: Enable the debug switch.

Switch#debug ldp packet receive

2.3.14 debug ldp timer

Command: debug ldp timer

no debug ldp timer

Function: Display the debug information of the LDP timer; the no operation will disable the switch.

Parameters: None.

Default: No display of debug information.

Command Mode: Admin Mode.

Usage Guide: The debug information of the LDP timer will be displayed with this command enabled.

Example: Enable the debug switch.

Switch#debug ldp timer

2.3.15 debug ldp tsm

Command: debug ldp tsm

no debug ldp tsm

Function: Display the debug information of the LDP state machine.

Parameters: None.

Default: No display of debug information.

Command Mode: Admin Mode.

Usage Guide: Implementing this command will display the debug information of the LDP state machine.

Example: Enable the debug switch.

Switch#debug ldp tsm

2.3.16 debug ldp usm

Command: debug ldp usm

no debug ldp usm

Function: Display the debug information of the LDP upstream state machine.

Parameters: None.

Default: No display of debug information.

Command Mode: Admin Mode.

Usage Guide: Implementing this command will display the debug information of the LDP upstream state machine.

Example: Enable the debug switch.

Switch#debug ldp usm

2.3.17 ldp {enable|disable}

Command: ldp {enable|disable}

Function: Enable the LDP protocol on the interface.

Parameters: None.

Default: The LDP is disabled.

Command Mode: Interface Mode.

Usage Guide: The LDP protocol is a label switching protocol used when switching labels in the public network, which usually works in a BGP VPN environment. “router ldp” is used to globally enable the LDP protocol, however, in interfaces where the protocol is actually working, implementing “ldp enable” in the interface configuration mode is required, so does enabling Label-switching, which, in combination with this command, work as a whole to ensure the normal operation of the protocol.

Example:

Switch(config)#int vlan 9

Switch(Config-if-Vlan9)#ldp enable

Related Commands: router ldp，label-Switching

2.3.18 global-merge-capability

Command: global-merge-capability {merge-capable|non-merge-capable }

no global-merge-capability {merge-capable|non-merge-capable }

Function: Enable or disable globally the LDP label merging capability; the no operation will restore the default value.

Parameters: None.

Default: Enable the label merging capability globally.

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: The LSP map multiple in-labels to the same FEC, corresponding with the same out-label and out-interface, in which case, when packets with different labels enter the LSR, the output packets will bear the same label. This procedure is called label merging. If the label-merging capability on the interface changes, the switch will reboot.

Example:

Switch(config)#router ldp

Switch(config-router)#global-merge-capability non-merge-capable

2.3.19 hello-interval

Command: hello-interval <*hello-interval*>

no hello-interval

Function: Set the global time interval between hello messages; the no operation will restore the default value.

Parameters: <*hello-interval*> is the time interval between hello messages, ranging from 1 to 65535 seconds.

Default: 5s.

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: LDP discovers its neighbors and keeps the communication with them through multicast Hello. Implementing this command will set the time interval of sending hello messages. Please pay attention to the relationship between it and the hold-time. It is better to set a value no greater than 1/3 of the latter. When the interface is configured with Hello-interval, the global configuration will have no effect on it.

Example: Configure the hello-interval as 10:

Switch(config)#router ldp

Switch(config-router)#hello-interval 10

Related Commands: hold-time，ldp hello-interval，ldp hold-time

2.3.20 hold-time

Command: hold-time <*hold-time*>

no hold-time

Function: Configure the hold-time of LDP multicast peers, whose default value is 15 seconds; the no operation will restore the default value.

Parameters: <hold-time> is the hold-time of multicast peer, ranging from 1 to 65535 seconds

Default: 15s.

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: LDP discovers its neighbors and keeps in communication with them through multicast Hello. Implementing this command will set the time interval of sending hello messages. Please pay attention to the relationship between it and the hello-interval. It is better to set a value at least three times as long as the latter. When the interface is configured with Hold-interval, the global configuration will have no effect on it.

Example: Configure the hold-time as 50:

Switch(config)#router ldp

Switch(config-router)#hold-time 50

Related Commands: hello-interval，ldp hold-time，ldp hello-interval

2.3.21 import-bgp-routes

Command: import-bgp-routes

no import-bgp-routes

Function: Configure to import BGP routes; the “no” operation will restore the default configuration.

Parameters: None.

Default: LDP doesn’t import BGP routes by default.

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: In common cased, LDP finds routes the route table of the system. But there are exceptions where it doesn’t import default routes or BGP routes. Importing the default routes may cause disorder, so it is forbidden in any case. If the users can make sure the security, then they can import BGP routes through this command and allocate labels for them.

Example: Import BGP routes and set the import route labels.

Switch(config)#router ldp

Switch(config-router)#import-bgp-routes

2.3.22 keepalive-interval

Command: keepalive-interval <*interval*>

no keepalive-interval

Function: Configure the interval between LDP keep-alive messages, whose default value is 10 seconds; the no operation will restore the default value.

Parameters: <interval>is the interval between keep-alive messages, ranging from 1 to 65535 seconds.

Default: 10s.

Command Mode: LDP Protocol Configuration Mode

Usage Guide: LDP will send keepalive messages to each other for keeping the communication, if there is no data after the creation of a TCP session. Implementing this command will set the interval of sending keepalive messages. Please make sure the value is big enough to prevent too many keepalive messages. When this value is configured on the interface, the global configuration command will lose effect.

Example: Configure the global keepalive-interval as 50s.

Switch(config)#router ldp

Switch(config-router)#keepalive-interval 50

Related Commands: keepalive-timeout，ldp keepalive-interval

2.3.23 keepalive-timeout

Command: keepalive-timeout <*time-val*>

no keepalive-timeout

Function: Configure the timeout value of LDP sessions, whose default value is 30 seconds; the no operation will restore the default value.

Parameters: <time-val>is the timeout value of LDP sessions, ranging from 1 to 65535 seconds.

Default: 30s.

Command Mode: LDP Protocol Configuration Mode

Usage Guide: LDP will send keepalive messages to each other for keeping the communication, if there is no data after the creation of a TCP session. Without receiving a keepalive message within the timeout period set by this command, the connection will be treated as disconnected. Usually this value should be at least three times as long as the keepalive interval. When this value is configured on the interface, the global configuration command will lose effect.

Example: Configure the global timeout value.

Switch(config)#router ldp

Switch(config-router)#keepalive-timeout 50

Related Commands: keepalive-interval, ldp keepalive-timeout

2.3.24 label-retention-mode

Command: label-retention-mode {conservative|liberal}

no label-retention-mode {conservative|liberal}

Function: Set the label retention mode; the no operation will cancel the configuration.

Parameters: None.

Default: Liberal

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: The LDP label retention mode determines how the LDP protocol handles the label information. The protocol provides two modes: the first one is conservative, which means only allows the retention of label information useful for the switch and drops other information. The other one is liberal, which means to allow the retention of all label information. This mode works together with the label advertisement mode, with liberal working with the “downstream unsolicited” advertisement mode, and conservative with the “downstream-on-demand” mode. Please notice that the manually configured liberal mode and the default one are different. When the liberal mode is set manually, the conservative mode of the interface will be the same as the global one if there is no configuration; while in the default liberal mode, it will be adjusted according to the label advertisement mode of the interface. In common cases, it is not recommended to configure this attributes, for it is in accordance with the label advertisement mode, and will be changed automatically when the label advertisement mode changes. Configuring this attribute separately may cause unmatched attributes. If the label retention mode changes when the label retention modes of all sessions on the interface are already configured, the session will be reconnected.

Example: Set the global label retention mode as liberal.

Switch(config)#router ldp

Switch(config-router)#label-retention-mode liberal

Related Commands: advertisement-mode，ldp advertisement-mode

2.3.25 label-switching

Command: label-switching

no label-switching

Function: Enable the label-switching function; the no operation will disable the function.

Parameters: None.

Command Mode: Interface Configuration Mode

Default: The label-switching function is disabled.

Usage Guide: Implementing this command to enable the label-switching function. This is a necessity to ensure the normal operation of the LDP protocol.

Example: Enable the label-switching function of the interface vlan1:

Switch#config terminal

Switch(config)#interface vlan 1

Switch(Config-if-Vlan1)#label-switching

Related Commands: enable-ldp

2.3.26 ldp advertisement-mode

Command: ldp advertisement-mode {downstream-on-demand | downstream-unsolicited}

no ldp advertisement-mode {downstream-on-demand | downstream-unsolicited}

Function: Set the interface label advertisement mode; the no operation will cancel the configuration.

Command Mode: Interface Configuration Mode.

Usage Guide: Implementing this command will set the label advertisement mode as downstream-unsolicited or downstream-on-demand. Parameters different with the global configuration can be used when configuring the interface. By default, the value is the global default or the global configuration, unless the interface has its own settings. This mode works together with two other modes, and any change of it will affect the other two at the same time. If the parameter is downstream-unsolicited, the label retention mode will be Liberal and the LSP control mode will be Independent, if it is downstream-on-demand, the label retention mode will be Conservative and the LSP control mode will be Ordered. Parameters different with the global configuration can be used when configuring the interface with this command.

Example: Configure the label advertisement mode as downstream-unsolicited in the interface mode.

Switch(config)#int vlan 9

Switch(Config-if-Vlan9)#ldp advertisement-mode downstream-unsolicited

Related Commands: label-retention-mode, ldp label-retention-mode, advertisement-mode

2.3.27 ldp hello-interval

Commands: ldp hello-interval <*hello-interval*>

no ldp hello-interval

Function: Set the hello-interval of the interface; the no operation will cancel the configuration.

Parameters: <hello-interval> is the interval between multicast Hello messages, ranging from 1 to 65535 seconds.

Default: Using the global configuration.

Command Mode: Interface Configuration Mode

Usage Guide: Implementing this command will set the interval between multicast Hello messages. Parameters different with the global configuration can be used when configuring the interface with this command.

Example: Set the hello interval of the interface as 25s.

Switch(config)#int vlan 9

Switch(Config-if-Vlan9)#ldp hello-interval 25

Related Commands: ldp hold-time，hold-time

2.3.28 ldp hold-time

Command: ldp hold-time <*hold-time*>

no ldp hold-time

Function: Set the neighbor hold-time of the interface; the no operation will restore the default value.

Parameters: <hold-time>is the neighbor hold time, ranging from 1 to 65535 seconds.

Default: Use the global configuration.

Command Mode: Interface Configuration Mode.

Usage Guide: LDP discovers its neighbors and keeps the communication with them through multicast Hello. Implementing this command will set neighbor hold-time when configuring the multicast. Please pay attention to the relationship between it and the hello-time, that is, it is better to set a value at least three times as long as the hello-time. When the interface is configured with Hold-interval, the global configuration will have no effect on it.

Example: Set the neighbor hold-time as 220s:

Switch(config)#int vlan 9

Switch(Config-if-Vlan9)#ldp hold-time 220

Related Commands: ldp hello-interval，hello-interval

2.3.29 ldp keepalive-interval

Command: ldp keepalive-interval *<interval-time>*

no ldp keepalive-interval

Function: Configure the interval between keep-alive messages; the no operation will restore the default value.

Parameters: <interval-time>is the interval between keep-alive messages, ranging from 1 to 65535 seconds.

Default: Use the global configuration.

Command Mode: Interface Configuration Mode

Usage Guide: LDP will send keepalive messages to each other for keeping the communication, if there is no data after the creation of a TCP session. Implementing this command will set the interval of sending keepalive messages. Please make sure the value is big enough to prevent too many keepalive messages. Parameters different with the global configuration can be used when configuring the interface.

Example: Configure the keepalive-interval of the interface as 33s.

Switch(config)#int vlan 9

Switch(Config-if-Vlan9)#ldp keepalive-interval 33

Related Commands: ldp keepalive-timeout，keepalive-timeout

2.3.30 ldp keepalive-timeout

Command: ldp keepalive-timeout *<time-val>*

no ldp keepalive-timeout

Function: Configure the session timeout value of the interface; the no operation will restore the default value.

Parameters: <time-val>is the timeout value of sessions, ranging from 1 to 65535 seconds.

Default: 30s.

Command Mode: LDP Protocol Configuration Mode

Usage Guide: LDP will send keepalive messages to each other for keeping the

communication, if there is no data after the creation of a TCP session. Without receiving a keepalive message within the timeout period set by this command, the connection will be treated as disconnected. Usually this value should be at least three times as long as the keepalive interval. Parameters different with the label configuration can be used when configuring the interface.

Example: Configure the keepalive-interval of the interface as 200s.

Switch(config)#int vlan 9

Switch(Config-if-Vlan9)#ldp keepalive-timeout 200

Related Commands: ldp keepalive-interval，keepalive-interval

2.3.31 ldp label-retention-mode

Command: ldp label-retention-mode {conservative | liberal}

no ldp label-retention-mode {conservative | liberal}

Function: Set the label retention mode; the no operation will restore the default value.

Parameters: None.

Default: Liberal

Command Mode: Interface Configuration Mode.

Usage Guide: Set the label retention mode as conservative or liberal. When the label retention mode is changed, all the sessions on the interface will be created. If the configuration of the interface is different with the global one, the latter will be ignored. Parameters different with the global configuration can be used when configuring the interface with this command.

Example: Set the label retention mode of the interface as conservative.

Switch(config)#int vlan 9

Switch(Config-if-Vlan9)#ldp label-retention-mode conservative

Related Commands: advertisement-mode，ldp advertisement-mode

2.3.32 ldp multicast-hellos

Command: ldp multicast-hellos

no ldp multicast-hellos

Function: Configure the interface to discover LDP neighbors with multicast Hello messages; the no operation will cancel the configuration.

Parameters: None.

Default: Use the global configuration.

Command Mode: Interface Configuration Mode

Usage Guide: LDP can discover its neighbors through multicast Hello messages or specify one via the “targeted-peer” command. Implementing this command will enable the multicast hello based neighbor discovery. Implementing the no operation will stop receiving and sending multicast Hello messages, so that the only way to discover neighbors is “targeted-peer”. Parameters different with the global configuration can be used when configuring the interface with this command.

Example:

Switch(config)#int vlan 9

Switch(Config-if-Vlan9)#ldp multicast-hellos

Related Commands: multicast-hellos

2.3.33 ldp targeted-peer-hello-interval

Command: ldp targeted-peer-hello-interval <*hello-interval*>

no ldp targeted-peer-hello-interval

Function: Set the interval of Hello to the specified target, the no operation will cancel the configuration and restore to the global one.

Parameters: <hello-interval> is the interval of Hello to the specified target, ranging from 1 to 65535 seconds.

Default: Use the global configuration

Command Mode: Interface Configuration Mode.

Usage Guide: LDP discovers its neighbors and keeps the communication with them by sending Hello to specified targets. Implementing this command will configure the interval of Hello to the specified target. Please pay attention to the relationship between it and the targeted-peer-hold-time. It is recommended to set a value no greater than 1/3 of the targeted-peer-hold-time. Parameters different with the global configuration can be used when configuring the interface with this command.

Example: Set the interval of Hello to the specified target as 225s.

Switch(config)#int vlan 9

Switch(Config-if-Vlan9)#ldp targeted-peer-hello-interval 255

Related Commands: ldp targeted-peer-hold-time，targeted-peer-hold-time

2.3.34 ldp targeted-peer-hold-time

Command: ldp targeted-peer-hold-time <*hold-time*>

no ldp targeted-peer-hold-time

Function: Set the peer-hold-time of specified destination for the interface; the no operation will cancel the configuration can restore to the global one.

Parameters: <*hold-time*> is the peer-hold-time of the specified target, ranging from 1 to 65535 seconds.

Default: Use the global configuration.

Command Mode: Interface Configuration Mode.

Usage Guide: LDP keeps the communication with neighbors by sending Hello to specified targets. Implementing this command will configure the peer-hold-time of specified destination. Please pay attention to the relationship between it and the targeted-peer-hello-time. It is recommended to set a value at least 3 times as long as the targeted-peer-hello-time. Parameters different with the global configuration can be used when configuring the interface with this command.

Example:

Switch(config)#int vlan 9

Switch(Config-if-Vlan9)#ldp targeted-peer-hold-time 50

Related Commands: ldp targeted-peer-hello-interval，targeted-peer-hello-interval

2.3.35 loop-detection

Command: loop-detection

no loop-detection

Function: Enable the LDP loop detection; the no operation will cancel the configuration.

Parameters: None.

Default: The loop detection is disabled by default.

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: LDP can be configured to enable the loop detection or not. If it is enabled, LDP provides two methods: the first is to check whether the HOP-COUNT exceeds the upper limit; the other is to check whether there is any repeated LSR-ID on the path vector.

Example:

Switch(config)#router ldp

Switch(config-router)#loop-detection

2.3.36 loop-detection-count

Command: loop-detection-count <*count*>

Function: Set the max number of hops allowed in the LDP loop detection; the no operation will restore to the default value.

Parameters: <count> is the allowed hop number, ranging from 1 to 255.

Default: 255.

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: LDP can be configured to enable the loop detection or not. If it is enabled, implementing this command will set the allowed hop number. The configuration will only take effect with loop-detection enabled. The no operation will restore to the default value.

Example: Set the allowed hop number in the LDP loop detection as 200:

Switch(config)#router ldp

Switch(config-router)#loop-detection-count 200

Related Commands: loop-detection

2.3.37 multicast-hellos

Command: multicast-hellos

no multicast-hellos

Function: Configure the interface to discover LDP neighbors with multicast Hello messages or not; the no operation will stop receiving and sending multicast hellos.

Parameters: None.

Default: Enable the receiving and sending of multicast Hellos on the LDP interface.

Command Mode: LDP Protocol Configuration Mode

Usage Guide: LDP can discover its neighbors through multicast Hello messages or specify one via the “targeted-peer” command. Implementing this command will enable the multicast hello based neighbor discovery. Implementing the no operation will stop sending multicast Hello messages, so that the only way to discover neighbors is “targeted-peer”. Configure to sending and receiving multicast hello messages globally, and enumerate all interfaces. If this attribute is already configured on the interface, the global configuration will be ignored, otherwise, the global one will take effect.

Example:

Switch(config)#router ldp

Switch(config-router)#multicast-hellos

2.3.38 propagate-release

Command: propagate-release

no propagate-release

Function: Configure to propagate the label release to neighbors; the no operation will do the opposite.

Parameters: None.

Default: Disabled.

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: If the label is expired, the switch won't send it to the upstream, unless this command is enabled.

Example:

Switch(config)#router ldp

Switch(config-router)#propagate-release

2.3.39 request-retry

Command: request-retry

no request-retry

Function: Set LDP to retry 5 times after the request for a label is rejected; the no operation will cancel the configuration.

Parameters: None.

Default Settings: Don't retry.

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: When LDP send a label request to the downstream, if the latter rejects it for some reasons, LDP will retry for 5 times with this attribute is configured, at an interval of request-retry-timeout.

Example:

Switch(config)#router ldp

Switch(config-router)#request-retry

Related Commands: request-retry-timeout

2.3.40 request-retry-timeout

Command: request-retry-timeout <*time-val*>

no request-retry-timeout

Function: Set the retry timeout interval after LDP's request for a label is rejected; the no operation will restore the default value.

Parameters: <time-val> is the timeout interval, ranging from 1 to 65535 seconds.

Default: 5s.

Command Mode: LDP Protocol Configuration Mode

Usage Guide: When LDP send a label request to the downstream, if the latter rejects it for some reasons, LDP will retry for 5 times with this attribute is configured, at an interval of request-retry-timeout.

Example: Set the retry timeout interval as 10 seconds.

Switch(config)#router ldp

Switch(config-router)#request-retry-timeout 10

Related Commands: request-retry

2.3.41 router ldp

Command: router ldp

no router ldp

Function: Enable the LDP protocol; the no operation will disable it.

Parameters: None.

Default: LDP is disabled.

Command Mode: Global Mode.

Usage Guide: The LDP protocol is a label advertising protocol used when switching labels in the public network, which usually works in a BGP VPN environment. Implementing this command will globally enable the LDP protocol, however, in interfaces where the protocol is actually working, implementing “enable-ldp” in the interface configuration mode is required, so does enabling Label-switching, which, in combination with this command, work as a whole to ensure the normal operation of the protocol.

Example:

Switch(config)#router ldp

Switch(config-router)#

2.3.42 router-id

Command: router-id *<ip-addr>*

no router-id

Function: Set the router ID used by LDP; the no operation will cancel the configuration.

Parameters: <ip-addr> is the router ID, in dotted decimal format.

Default: The ID will be automatically obtained.

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: The router ID exclusively identifies a LDP device in the network. Router-id is the value of router-id in Hello messages.

Example:

Switch(config)#router ldp

Switch(config-router)#router-id 10.10.10.10

2.3.43 show ldp

Command: show ldp

Function: Display some basic LDP attributes of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Implementing this command will display the current configuration information of LDP.

Example:

Switch#show ldp

Router ID : 10.10.0.11

LDP Version : 1

Global Merge Capability : N/A

Label Advertisement Mode : Downstream Unsolicited

Label Retention Mode : Liberal

Label Control Mode : Independent

Loop Detection : Off

Loop Detection Count : 0

Request Retry : Off

Propagate Release : Disabled

Hello Interval : 5

Targeted Hello Interval : 15

Hold time : 15

Targeted Hold time : 45

Keepalive Interval : 10

Keepalive Timeout : 30

Request retry Timeout : 5

Multicast Hello : Enabled

Targeted Hello Accept : Disabled

Transport Interface : N/A

Import BGP routes : No

Display	Explanation
Router ID : 10.10.0.11	Router id is 10.10.0.11
LDP Version : 1	The LDP version is 1
Global Merge Capability : N/A	The global label merging capability is disabled
Label Advertisement Mode : Downstream Unsolicited	The label advertisement mode is downstream unsolicited
Label Retention Mode : Liberal	The label retention mode is Liberal
Label Control Mode : Independent	The label control mode is Independent
Loop Detection : Off	The loop detection is disabled
Loop Detection Count : 0	The loop detection count is 0
Request Retry : Off	The switch won't retry after a rejected label request.
Propagate Release : Disabled	The switch won't propagate the label release messages
Hello Interval : 5	The interval between Hello messages is 5s
Targeted Hello Interval : 15	The interval between Hello messages to a specified target is 15s
Hold time : 15	The hold time of adjacency is 15s
Targeted Hold time : 45	The hold time of adjacency with specified targets is 45s
Keepalive Interval : 10	The intervals between keepalive messages sent by the interface is 10s
Keepalive Timeout : 30	The keepalive timeout period is 30s
Request retry Timeout : 5	The retry timeout after the label request being rejected is 5s.
Multicast Hello : Enabled	Discover neighbors via multicast Hello messages
Targeted Hello Accept : Disabled	The switch won't accept Hello from specified targets.
Transport Interface : N/A	No transport interface
Import BGP routes : No	The switch won't import BGP routes

2.3.44 show ldp adjacency

Command: show ldp adjacency

Function: Display all adjacency information of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Implementing this command will display LDP adjacency information, for diagnosing and troubleshooting.

Example:

Switch#show ldp adjacency

IP Address Interface Name Holdtime LDP ID

192.168.3.5 vlan1 15 10.10.0.18:0

192.168.4.5 vlan2 15 10.10.0.18:0

Display	Explanation
IP Address	The IP address of the neighbor
Interface Name	The interface name of the connection with the neighbor
Holdtime	The holdtime of the adjacency
LDP ID	（LSR-ID : Label Space）The LDP ID

2.3.45 show ldp downstream

Command: show ldp downstream

Function: Display all downstream information of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode

Usage Guide: Implementing this command will display the information of downstreams maintained by the current protocol.

Example:

Switch#show ldp downstream

Session peer 192.168.11.50:

Downstream state: Established Label: impl-null RequestID: 0 Peer: 192.168.11.50 Attr:

Downstream state: Established Label: impl-null RequestID: 0 Peer: 192.168.11.50 Attr:

Downstream state: Established Label: impl-null RequestID: 0 Peer: 192.168.11.50 Attr:

Downstream state: Established Label: 20 RequestID: 0 Peer: 192.168.11.50 Attr:

2.3.46 show ldp fec

Command: show ldp fec

Function: Display information about all FECs (Forwarding Equivalence Class) of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display information about all FECs (Forwarding Equivalence Class) of this LSR.

Example:

Switch#show ldp fec

LSR codes : E/N - LSR is egress/non-egress for this FEC,
L - LSR received a label for this FEC,
> - LSR will use this route for the FEC

Code	FEC	Session	Out Label	Nexthop Addr
E >	3.3.3.1/32	Non-Existent	None	Connected
E >	4.4.4.1/32	Non-Existent	None	80.80.90.2
E >	80.80.90.0/24	Non-Existent	None	Connected
E >	80.90.70.0/24	Non-Existent	None	80.80.90.2
E >	80.90.70.10/32	Non-Existent	None	Connected
E >	80.90.70.78/32	Non-Existent	None	Connected

2.3.47 show ldp interface

Command: show ldp interface [vlan <*1-4094*> | IFNAME]

Function: Display LDP information about all or specified interfaces of this LSR.

Parameters: <1-4094> VLAN ID;
IFNAME: the interface name.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display the LDP information of the interface; user-provided parameters can specify some particular interfaces; no parameter means to display information of all interfaces.

Examples:

Switch#show ldp interface

Interface LDP Identifier Label-switching Merge Capability

vlan0	10.10.0.11:0	Disabled	N/A
vlan1	10.10.0.11:0	Enabled	Merge capable
vlan2	10.10.0.11:0	Enabled	Merge capable

2.3.48 show ldp lsp

Command: show ldp lsp

Function: Display the label switching path of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display the label switching path of the switch.

Example:

Switch#show ldp lsp

FEC IPV4:10.1.1.0/24 -> 0.0.0.0

Downstream state: Established Label: none RequestID: 0 Peer: EGRESS Attr: None

Upstream state: Established Label: impl-null RequestID: 0 Peer: 15.1.1.70 Attr: None

Upstream state: Established Label: impl-null RequestID: 0 Peer: 20.1.1.1 Attr: None

Downstream state: Established Label: impl-null RequestID: 0 Peer: 15.1.1.70 Attr: None

FEC IPV4:11.1.1.0/24 -> 0.0.0.0

Downstream state: Established Label: impl-null RequestID: 0 Peer: 15.1.1.70 Attr: None

Downstream state: Established Label: none RequestID: 0 Peer: EGRESS Attr: None

Upstream state: Established Label: impl-null RequestID: 0 Peer: 15.1.1.70 Attr: None

Downstream state: Established Label: impl-null RequestID: 0 Peer: 20.1.1.1 Attr: Hop Count: 1

2.3.49 show ldp session

Command: show ldp session [<*ip-addr*>]

Function: Display information about specified or all LDP sessions of this LSR.

Parameters: <ip-addr>: the IP address of the neighbor to display, in dotted decimal format.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display information about current LDP sessions of this switch.

Example:

Switch#show ldp session

Peer IP Address	IF Name	My Role	State	KeepAlive
192.168.11.50	vlan1	Passive	OPERATIONAL	30
192.168.13.60	vlan2	Passive	OPERATIONAL	30

2.3.50 show ldp statistics

Command: show ldp statistics

Function: Display the LDP statistics of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display the current LDP statistics of this switch.

Example:

Switch#show ldp statistics

PacketType	Sent	Received
Notification	18	22
Hello	102589	103935
Initialization	37	37
Keepalive	45216	45224
Address	44	40
Address Withdraw	3	1
Label Mapping	97	152
Label Request	0	0
Label Withdraw	3	38
Label Release	42	3
Request About	0	0

Display		Explanation
PacketType		The packet types will be listed as below:
Total	Sent	The total number of this type of packets that have been sent.

	Received	The total number of this type of packets that have been received.

2.3.51 show ldp targeted-peers

Command: show ldp targeted-peers

Function: Display the information of LDP targeted peers in the configuration of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display the currently configured LDP neighbor information.

Example:

Switch#show ldp targeted-peers

IP Address Interface

10.1.1.66 Vlan2

2.3.52 show ldp upstream

Command: show ldp upstream

Function: Display information of all upstreams of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display information of all LDP upstreams maintained by the switch.

Example:

Switch#show ldp upstream

Session peer 192.168.11.50:

Upstream state: Established Label: impl-null RequestID: 0 Peer: 192.168.11.50 Attr:

Upstream state: Established Label: impl-null RequestID: 0 Peer: 192.168.11.50 Attr:

2.3.53 show mpls ldp discovery

Command: show mpls ldp discovery interface [vlan *<1-4094>* | IFNAME]

Function: Display all interfaces and label-switching information of this LSR.

Parameters: <*1-4094*>：VLAN ID.

IFNAME：The interface name

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display all or specified interfaces and label-switching information.

Example:

Switch#show mpls ldp discovery

Interface	LDP Identifier	Label-switching	Merge Capability
Vlan1	10.10.0.11:0	Enabled	Merge capable
Vlan2	10.10.0.11:0	Enabled	Merge capable
Loopback1	0.0.0.0:0	Disabled	N/A

2.3.54 show mpls ldp fec

Command: show mpls ldp fec

Function: Display information about all FECs of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display information about currently maintained FECs.

Example:

Switch#show mpls ldp fec

LSR codes : E/N - LSR is egress/non-egress for this FEC,
L - LSR received a label for this FEC,
> - LSR will use this route for the FEC

Code	FEC	Session	Out Label	Nexthop Addr
E >	10.1.1.0/24	non-existent	none	15.1.1.68
NL	10.1.1.0/24	10.1.1.66	impl-null	15.1.1.68
E >	11.1.1.0/24	non-existent	none	15.1.1.68
E >	15.1.1.0/24	non-existent	none	connected
NL>	15.1.1.0/24	10.1.1.66	impl-null	connected
E >	20.1.1.0/24	non-existent	none	15.1.1.68
NL	30.1.1.0/24	10.1.1.66	impl-null	invalid
E >	100.1.1.0/24	non-existent	none	connected
NL	100.1.1.0/24	10.1.1.66	impl-null	connected

2.3.55 show mpls ldp neighbor

Command: show mpls ldp neighbor

Function: Display information about all neighbors of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display information of LDP neighbors, which is useful for troubleshooting.

Example:

Switch#show mpls ldp neighbor

IP Address	Interface Name	Holdtime	LDP ID
192.168.3.5	vlan1	15	10.10.0.18:0
192.168.4.5	vlan2	15	10.10.0.18:0

2.3.56 show mpls ldp parameter

Command: show mpls ldp parameter

Function: Display basic LDP attributes of this LSR.

Parameters: None.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display information of current LDP configurations.

Example:

Switch#show mpls ldp parameter

Router ID : 10.10.0.11

LDP Version : 1

Global Merge Capability : N/A

Label Advertisement Mode : Downstream Unsolicited

Label Retention Mode : Liberal

Label Control Mode : Independent

Loop Detection : Off

Loop Detection Count : 0

Request Retry : Off

Propagate Release : Disabled

Hello Interval : 5

Targeted Hello Interval : 15

Hold time : 15

Targeted Hold time : 45

Keepalive Interval : 10

Keepalive Timeout : 30

Request retry Timeout : 5

Targeted Hello Receipt : Disabled

Transport Address : N/A

Transport Interface : N/A

Import BGP routes : No

Display	Explanation
Router ID : 10.10.0.11	Router id 为 10.10.0.11 Router ID is 10.10.0.11
LDP Version : 1	The LDP version is 1
Global Merge Capability : N/A	The global label merging capability is disabled
Label Advertisement Mode : Downstream Unsolicited	The label advertisement mode is Downstream Unsolicited
Label Retention Mode : Liberal	The label retention mode is Liberal
Label Control Mode : Independent	The label control mode is Independent
Loop Detection : Off	The loop detection is disabled
Loop Detection Count : 0	The loop detection count is 0.
Request Retry : Off	Don’t retry when the request is rejected
Propagate Release : Disabled	Don’t propagate the label release message
Hello Interval : 5	The interval between Hello messages is 5s
Targeted Hello Interval : 15	The interval between Hello messages to the specified target is 15s
Hold time : 15	The adjacency hold time is 15s
Targeted Hold time : 45	The hold time of adjacency with the specified target is 45s
Keepalive Interval : 10	The interval between keepalive messages is 10s
Keepalive Timeout : 30	The keepalive timeout of is 30s
Request retry Timeout : 5	The retry timeout after the request is rejected is 5s.
Targeted Hello Receipt : Disabled	Forbidden the receipt of Hello messages from the specified target.
Transport Address : N/A	No configuration of the Transport address
Transport Interface : N/A	No configuration of the Transport Interface

Import BGP routes : No	Don’t import BGP routes.

2.3.57 show mpls ldp session

Command: show mpls ldp session [<*ip-addr*>]

Function: Display all or specified LDP sessions of this LSR.

Parameters: <ip-addr> is the IP address of the neighbors to be displayed, in dotted decimal format.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display information about current LDP sessions of this switch.

Example:

Switch#show mpls ldp session

Peer IP Address	IF Name	My Role	State	KeepAlive
192.168.11.50	vlan1	Passive	OPERATIONAL	30
192.168.13.60	vlan2	Passive	OPERATIONAL	30

2.3.58 targeted-hello-accept

Command: targeted-hello-accept [filter <*1-99*>]

no targeted-hello-accept

Function: Configure the LDP to receive Hello messages from the specified target, applied in the extended mode.

Parameters: <1-99>: the access list ID that will be used.

Default: Don’t accept target-Hello messages.

Command Mode: LDP Protocol Configuration Mode

Usage Guide: By implementing this command, users can specify targets, from which the LDP will accept Hello messages, via access list commands.

Example:

Switch(config)#router ldp

Switch(config-router)#targeted-hello-accept filter 1

2.3.59 targeted-peer

Command: targeted-peer <*ip-addr*>

no targeted-peer <*ip-addr*>

Function: Configure the LDP neighbor of the specified target; the no operation will delete the configuration.

Parameters: <ip-adddr> is the IP address of the neighbor, in dotted decimal format.

Default: No targeted-peer.

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: LDP can discover a neighbor via multicast Hello messages or manual configurations. This command enables the latter method by adding a targeted-peer and establishing the adjacency with it. The no operation will delete the configuration. Configuring a targeted-peer neighbor means to establish an extended session.

Example: Configure the LDP neighbor of the specified target is 10.10.10.10

Switch(config)#router ldp

Switch(config-router)#targeted-peer 10.10.10.10

2.3.60 targeted-peer-hello-interval

Command: targeted-peer-hello-interval <*hello-interva*>

no targeted-peer-hello-interval

Function: Configure the global interval between Hello messages to the specified target; the no operation will restore the default value.

Parameters: <*hello-interval*> is the interval between Hello messages to the specified target, ranging from 1 to 65535 seconds.

Default: 15s.

Command Mode: LDP Protocol Configuration Mode

Usage Guide: LDP discovers a neighbor and stays in communication with it via sending Hello messages to the specified target. Implementing this command will configure the interval between those Hello messages. Please pay attention to the relationship between it and the targeted-peer-hold-time. It is recommended to configure a value no greater than 1/3 of the latter. When a specified interface has its own configuration, this command will lose effect on it.

Example: Configure the Hello interval as 50s.

Switch(config)#router ldp

Switch(config-router)#targeted-peer-hello-interval 50

Related Commands: targeted-peer-hold-time， ldp targeted-peer-hold-time， ldp targeted-peer-hello-Interval

2.3.61 targeted-peer-hold-time

Command: targeted-peer-hold-time <*hold-time*>

no targeted-peer-hold-time

Function: Configure the global hold-time of the specified target; the no operation will restore the default value.

Parameters: <*hold-time*> is the hold-time of the specified target, ranging from 1 to 65535 seconds.

Default: 45s.

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: LDP discovers a neighbor and stays in communication with it via sending Hello messages to the specified target. Implementing this command will configure the hold-time of neighbors discovered by the specified target. Please pay attention to the relationship between it and the targeted-peer-hello-interval. It is recommended to configure a value at least three times as long as the latter. When a specified interface has its own configuration, this command will lose effect on it.

Example: Configure the neighbor hold-time as 50s.

Switch(config)#router ldp

Switch(config-router)#targeted-peer-hold-time 50

Related Commands: targeted-peer-hello-interval ，ldp targeted-peer-hold-time，ldp targeted-peer-hello-interval

2.3.62 transport-address

Command: transport-address <*ip-addr*>

no transport-address

Function: Configure the IP address used by LDP to establish TCP connections; the no operation will cancel the configuration.

Parameters: <*ip-addr*> is the IP address, in dotted decimal format.

Default: The address is automatically obtained.

Command Mode: LDP Protocol Configuration Mode.

Usage Guide: After the discovery of a neighbor via multicast or targeted Hello messages, LDP doesn't use the interface address sending the messages as the source address when establishing TCP connections, instead it uses the transport-address in the Hello messages to guarantee the uniqueness of the connection. Usually, LDP chooses an interface address as transport-address. Implementing this command will configure this address. Please notice that, this address should be one of a loopback interface to ensure a successful configuration. The no operation will cancel the configuration, and regain an

interface address as transport-address automatically.

Example: Configure 10.10.10.10 as the source address of TCP connections.

Switch(config)#router ldp

Switch(config-router)#transport-address 10.10.10.10

2.4 LDP Typical Instances

Some designations of LDP are for adapting different network environments. Its configuration is very simple in the typical Ethernet environment. Due to the development of hardware system, especially the popularity of L3 switches, the pure MPLS network has already lost its importance to MPLS VPN.

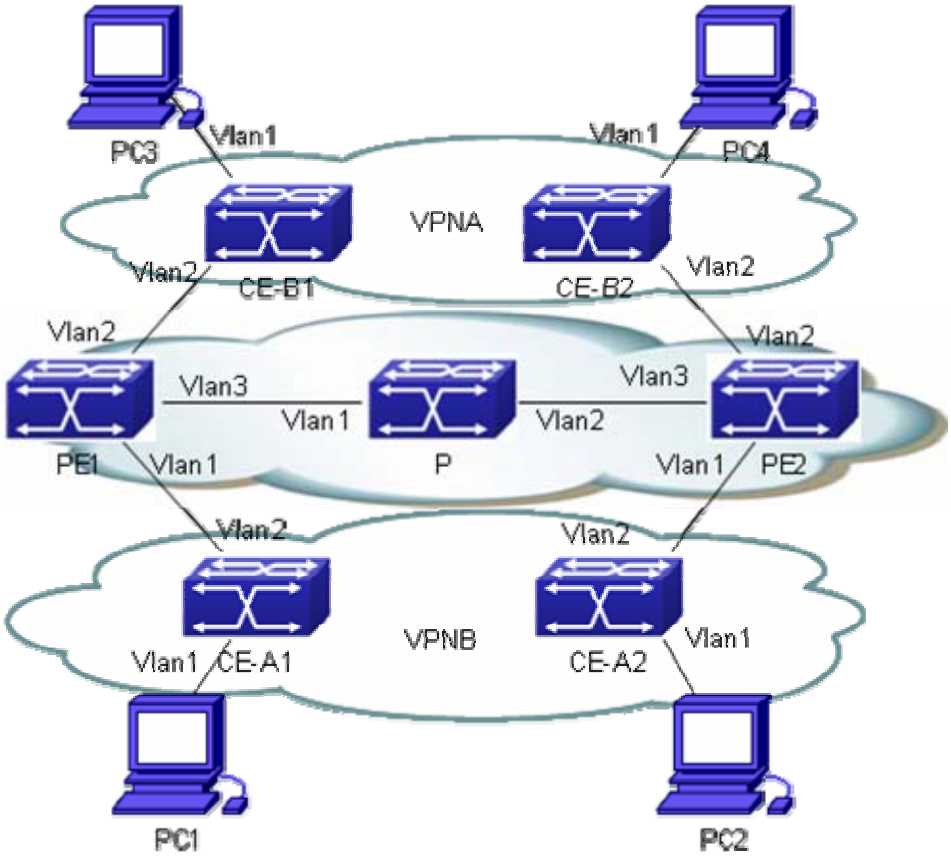

Fig 2-4 MPLS VPN Typical Instance

The above figure demonstrates a typical MPLS VPN instance, in which, PE1, P and PE2 form the public network area – the area switching via MPLS. CE-A1 and CE-A2 form VPN-A, CE-B1 and CE-B2 form VPN-B. Both VPNs communicate via the public network label switching, and need to configure LDP for distributing and advertising labels in the public network area. To guarantee the reachability of routes, we advertise routes via OSPF.

The LDP configuration of PE1 is as follows:

```
PE1#config
PE1(config)#mpls enable
PE1(config)# router ldp
PE1(config-router)#exit
PE1(config)#interface vlan 3
PE1(config-if-Vlan3)#ip address 202.200.1.2 255.255.255.0
PE1(config-if-Vlan3)#ldp enable
PE1(config-if-Vlan3)#label-switching
PE1(config-if-Vlan3)#exit
PE1(config)#router ospf
PE1(config-router)#network 200.200.1.1/32 area 0
PE1(config-router)#network 202.200.1.0/24 area 0
PE1(config-router)#exit
```

The LDP configuration of P is as follows:

```
P#config
P(config)#mpls enable
P(config)# router ldp
P(config-router)#exit
P(config)#interface vlan 1
P(config-if-Vlan1)#ip address 202.200.1.1 255.255.255.0
P(config-if-Vlan1)#ldp enable
P(config-if-Vlan1)#label-switching
P(config-if-Vlan1)#exit
P(config)#interface vlan 2
P(config-if-Vlan2)#ip address 202.200.2.1 255.255.255.0
P(config-if-Vlan2)#ldp enable
P(config-if-Vlan2)#label-switching
P(config-if-Vlan2)#exit
P(config)#router ospf
P(config-router)#network 202.200.1.0/24 area 0
P(config-router)#network 202.200.2.0/24 area 0
P(config-router)#exit
```

The LDP configuration of PE2 is as follows:

```
PE2#config
PE2(config)#mpls enable
PE2(config)# router ldp
PE2(config-router)#exit
```

PE2(config)#interface vlan 3

PE1(config-if-Vlan3)#ip address 202.200.2.2 255.255.255.0

PE2(config-if-Vlan3)#ldp enable

PE2(config-if-Vlan3)#label-switching

PE2(config-if-Vlan3)#exit

PE2(config)#router ospf

PE2(config-router)#network 200.200.1.2/32 area 0

PE2(config-router)#network 202.200.2.0/24 area 0

PE2(config-router)#exit

Please refer to BGP VPN typical instances for the configuration of BGP.

2.5 LDP Troubleshooting

When configuring and using LDP, some problems like incorrect physical connections, configuration errors may cause it to fail, so plesase pay attention to the following notices to avoid them:

- ☞ First, make sure the system enables LDP globally and on the active interface. Notice that the LDP can only be enabled on interfaces after it is enabled globally.
- ☞ Second, use the “show ldp interface” command to check whether the LDP has been enabled correctly on the interface after the connection succeeds. If the LDP has been correctly enabled but cannot be displayed, it is possible that the interface is not in the UP mode or not configured with interface label-switching.
- ☞ Then, make sure the adjacent interfaces are in the same segment, and check whether the LDP can discover peers and establish adjacencies with them normally via the “show ldp adjacency” command. If no peer is discovered or no adjacency is established, it is possible that the interfaces may belong to different segments, or one of the local host and its remote neighbor disables multicast HELLO. Besides, when establishing TCP connection, LSR ID is the default address, as, please make sure advertise the LSR ID route to the remote end.
- ☞ Check whether the state of LDP session with “show ldp session” is operational, since only in this state, LDP sessions can switch messages. If the LDP session can’t be established, use “show ldp” to check the TCP addresses of the two parties, and lookup the route table to make sure the route of the remote end is reachable.
- ☞ At last, given all above steps succeed, use “show ldp fec” to check the routes imported by LDP and their information, or check the created entries with “show mpls ftn” and “show mpls ilm”.
- ☞ Besides, if there are configurations of LDP targeted peers, make sure that the

remote end also configures a LDP peer whose destination address is the host, or allows the receipt of HELLOs from specified targets. The addresses specified by the two ends should be route-reachable.

Chapter 3 MPLS VPN

3.1 BGP/MPLS VPN Introduction

3.1.1 BGP/MPLS VPN Network Structure

BGP/MPLS VPN is a PE-based L3VPN technology in the VPN solutions provide by providers, using BGP to advertise VPN routes and MPLS to forward VPN messages in the provider backbone network.

The BGP/MPLS VPN networking is flexible, extendible, and can support MPLS QoS and MPLS TE conveniently, resulting in its increasingly popular application.

BGP/MPLS VPN model consists of three parts: CE, PE and P.

- ☞ P router: Provide Router. It locates in the MPLS domain, and is able to switch fast-forwarding MPLS data flow based on labels. P router receives MPLS messages, switch labels and then output them.
- ☞ PE router: Provide Edge Router. It locates at the edge of the MPLS domain, for converting IP messages and MPLS messages. PE router receives IP messages, pushes MPLSU labels, and output MPLS messages; or receives MPLS messages, pop labels, and output IP messages. On PE routers, the ports connected with other P routers or PE routers are “public network port”, configured with public network IP address; those connected with CE routers are “private network port”, configured with private network address.
- ☞ CE router: Customer Edge Router. It locates at the edge of the customer IP domain, connected directly to PE route, for aggregating customer data and forwarding route information of the customer IP domain to PE router.

The next figure demonstrates a BGP/MPLS VPN networking:

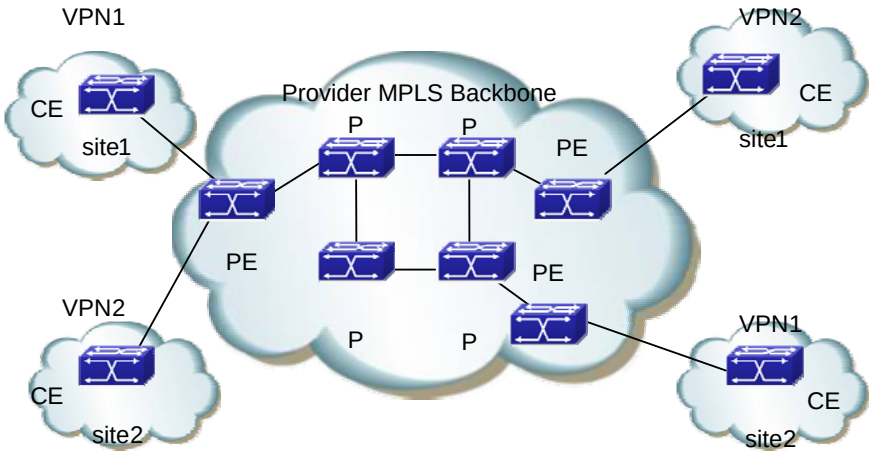

Fig 3-1 BGP/MPLS VPN Networking

The division of CE and PE is based on the management areas of SP and customers, since CE and PE are the edge between the two areas.

CE is usually a router. When the adjacency between it and the PE directly connected to it, CE will advertise the local VPN route to PE, and learn the remote VPN route from PE. CE and PE use BGP/IGP to exchange route information or static routes.

PE will exchange VPN route information with other PEs via BGP after learning the local VPN route form CE. It only maintains the VPN route directly connected with it rather than all VPN routes in the service provider network.

P router only maintains routes to PE, without learning any VPN route information.

Then transmitting VPN traffic in the MPLS backbone network, the ingress PE serves as the Ingress LSR (Label Switch Router), the egress PE the Egress LSR, and P router the Transit LSR.

3.1.2 Basic Concept of BGP/MPLS VPN

Site

"Site" is a concept usually mentioned when introducing VPN, which can be understood from the following aspects:

- ☞ Site is a set of IP systems with IP connectivity between each other. This connectivity is independent of SP network.
- ☞ The division of site is based on the topology of devices instead of devices' location, although in most cases, the devices in a site locate next to each other.
- ☞ The devices in a site can belong to multiple VPN. In other words, a site can belong to multiple VPN;
- ☞ Site connects to SP network via CE. One site can include multiple CE while a CE

can only belong to one site.

Multiple sites connected to the same SP network can be divided into different sets according to special policies, which only allow intercommunication via the SP network to happen between the sites within the same set. Such sets are VPN.

VRF

VRF (VPN Routing & Forwarding Instance), consisting of VPN IP route table and VPN IP forwarding table (the forwarding table contains the MPLS encapsulation information), is the core entry of MPLS VPN packet forwarding. Each VPN has its own independent VRF. The VRF address spaces of different VPN can overlap with each other. A PE/P router in the MPLS VPN network usually contains multiple independent VRF.

Overlapping Address Space

VPN is a private network, which means each VPN manages its own address range independently. This range is called Address Space.

The address spaces of different VPN may partially overlap with each other. For example, if VPN1 and VPN2 both use the segment of 10.110.10.0/24, there would be Overlapping Address Space.

VPN instance

In the MPLS VPN, the route isolation between different VPN is implemented via VPN instance.

PE creates and maintains a special VPN instance for every site directly connected to it. VPN site contains the VPN membership and route rules of the corresponding site. If the customers of a site belong to more than one VPN, then its VPN instance will contain the information of all those VPN.

To guarantee the data independency and security of VPN, each VPN instance on PE has its own independent route table and IFIL (Label Forwarding Information Base).

To be specific, the information in VPN instances include: LFIB, IP route table, interfaces bound with VPN instance, and its management information (including RD, route filter policy, member interface list and etc).

VPN-IPv4 Address

The traditional BGP can’t correctly handle the VPN routes with overlapping address spaces. Assume that VPN1 and VPN2 both use the segment of 10.110.10.0/24, and advertise separately a route reaching this segment, BGP will only choose one of the two routes, losing the one reaching the other VPN.

PE routers use MP-BPG to advertise VPN routes between each other and solve the above problem via VPN-IPv4 address family.

A VPN-IPv4 address consists of 12 bytes, including 8 bytes of RD (Route Distinguisher) and 4 bytes of IPv4 address prefix.

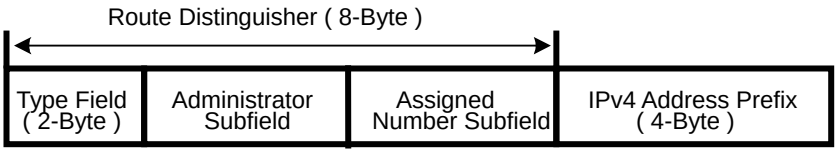

Fig 3-2 VPN-IPv4 Address Structure

After receiving the regular IPv4 routes from CE, PE should advertise these private network VPN routes to the remote PE. The independency of the private network routes is based on the additional RD patched to them.

SP can independently distribute globally unique RD, thus, even the VPN from different SP networks use the same IPv4 address space, the PE routers can advertise different routes to them.

It is recommended to allocate a special RD for each VPN instance on the PE to ensure all routes reaching the same CE uses the same RD. the VPN-IPv4 address whose RD is 0 is a globally unique IPv4 address.

Adding RD is to a specific IPv4 prefix will make the latter globally unique, which is the meaning of RD.

RD may relate with ASN, in which case, it is a combination of an ASN and a random number; it may also relate with IP address, in which case, it is a combination of an IP address and a random number.

There are two RD formats, differing with each other via 2 bytes of Type filed:

- ☞ If Type is 0, the Administrator sub-field takes up 2 bytes, Assigned Number sub-field takes up 4 bytes. The format would be: 16 bits of ASN: 32 bits of user-defined number. For example: 100:1
- ☞ If Type is 0, the Administrator sub-field takes up 2 bytes, Assigned Number sub-field takes up 4 bytes. The format would be: 32 bits of IPv4 address: 16 bits of user-defined number. For example: 172.1.1.1:1

To guarantee the global uniqueness of RD, please don't set the value of Administrator sub-filed as private ASN or private IP address.

VPN Target Attribute

BGP/MPLS VPN uses a 32 bit BGP extended community attribute – VPN Target (also called Route Target) to control the advertisement of VPN route information.

There are two types of VPN Target attribute used by VPN instances on PE routers:

- ☞ Export Target attribute: the local PE sets the Export Target attribute for the VPN-IPv4 routes it learns from the sites directly connected to it, before advertising the routes to other PE.
- ☞ Import Target Attribute: when receiving the VPN-IPv4 route advertised by other PE routers, PE will check their Export Target Attribute, and add the routes into

corresponding VPN route table only when their Export Target attributes match the Import Target attributes of the VPN instances on it.

In other words, VPN Target attribute defines which sites can accept a VPN-IPv4 route, and a PE router can receive routes from witch sites.

Like RD, there are two VPN Target formats:

- ☞ 16 bits ASN : 32bits user-defined number, for example: 100:1
- ☞ 32bits IPv4 address: 16 bits user-defined number, for example: 172.1.1.1:1

MP-BGP

MP-BGP (Multiprotocol extensions for BGP-4) transmits VPN information and routes between PE routers. MP-BGP is backward-compatible, simultaneously supporting traditional IPv4 address family and other address family (such as VPN-IPv4 address family). It can ensure the advertisement of private network VPN routes only happens within the VPN, and can realize the communication between MPLS VPN members.

Routing Policy

On the basis of controlling VPN route advertisement via ingress and egress extended community, the import or export route policy can be used for a more precise control of importing and advertising VPN routes.

The import route policy can filter the routes importable for VPN instances according to the VPN target attribute of routes. It can deny the receipt of routes specified by the community in the import list. The export route policy can deny advertising the routes specified by the community in the export list.

After creating VNP instances, users can choose whether to configure import or export route policy.

Tunneling Policy

Tunneling Policy is used to choose tunnels for specified VPN instances messages.

Tunneling Policy is optional. After creating VNP instances, users can configure it. By default, it will choose LSP as the tunnel without load sharing (the load sharing number is 1). Besides, this policy only takes effect in one AS domain.

3.1.3 Forwarding BGP/MPLS VPN Messages

In basic L3VPN applications (not include Multi-AS VPN), the forwarding of VPN packets adopts the 2-layer label mode:

- ☞ The first layer (outer layer) labels will be switched within the backbone network, indicating a LSP from the PE to the remote PE. With this layer of label, VPN messages can reach the remote PE along the LSP.
- ☞ The second layer label (inner layer) will be used when the packet reaches CE from the remote PE, indicating which site to send the packet, or, more specifically,

which CE it will reach. Thus the remote PE will find the correct interface to forward the packet according to this layer of label.

In some special conditions, two sites belonging to the same VPN may connect to a same PE, in which case, the only information matters is how to reach the remote CE.

The next figure demonstrates an example of forwarding VPN packets:

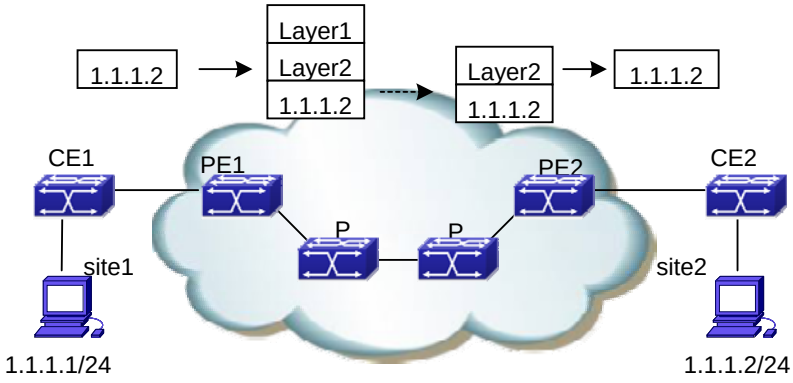

Fig 3-3 Forwarding VPN Packets

(1) Site1 sends an IP packet with a destination address of 1.1.1.2, which is sent by CE1 to PE1.

(2) PE1 looks up VPN-instance entries according to the interface receiving the packet and the destination address, then forwards the packet after adding two layers of label (inner and outer) to it, if there is a match.

(3) The MPLS network will send the packet to PE2 according to the outer layer label (removed when the packet reaching the last-hop of PE2, leaving only the inner layer) of it.

(4) PE1 looks up VPN-instance entries according to the inner layer of label and the destination address, then forwards the packet to CE2 after determining its egress interface.

(5) CE2 forwards the packet to its destination according to the regular IP forwarding process.

3.1.4 BGP/MPLS VPN Networking Resolution

In BGP/MPLS VPN networks, the advertisement and receipt of VPN routes between different sites are controlled by VPN Target Attribute. The configurations of VPN Export Target and Import Target are independent, both allowing multiple values, and hence can realize flexible VPN access control and various VPN networking resolutions.

Basic VPN

In the most basic instance, all users of a VPN form a closed user group, allowing the forwarding of traffic between them. But no user within the VPN can communicate with outside users.

In such networking, each VPN will obtain an exclusive VPN Target as its Export Target and Import Target, which should not be used by other VPN.

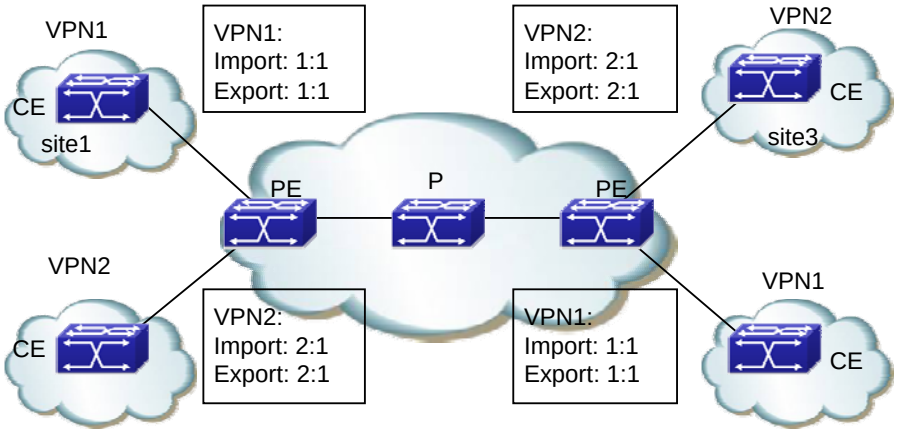

Fig 3-4 Basic VPN Networking Resolution

In the above figure, the VPN Target distributed by PE for VPN1 is 100:1; and that for VPN2 is 200:1. The sites of VPN1 can intercommunicate with each other, so do the two of VPN2. But the intercommunication between sites in VPN1 and those in VPN2 arise forbidden.

Hub&Spoke VPN

To use a central access control device in VPN to control the intercommunication of other users, Hub&Spoke networking resolution is a good choice, so that the central device can monitor and filter the intercommunication between the devices at two ends.

Two VPN target is needed in this networking, one for “Hub”, the other for “Spoke”.

All sites should follow the following rules to configure VPN Target for VPN instances on PE:

- Spoke-PE: Export Target is “Spoke”, Import Target is “Hub”
- Hub-PE: two interfaces or sub-interfaces are needed, one for receiving routes from Spoke-PE, the Import Target of whose VPN instance is “Spoke”; the other for advertising routes to Spoke-PE, the Export Target of whose VPN instance is “Hub”.

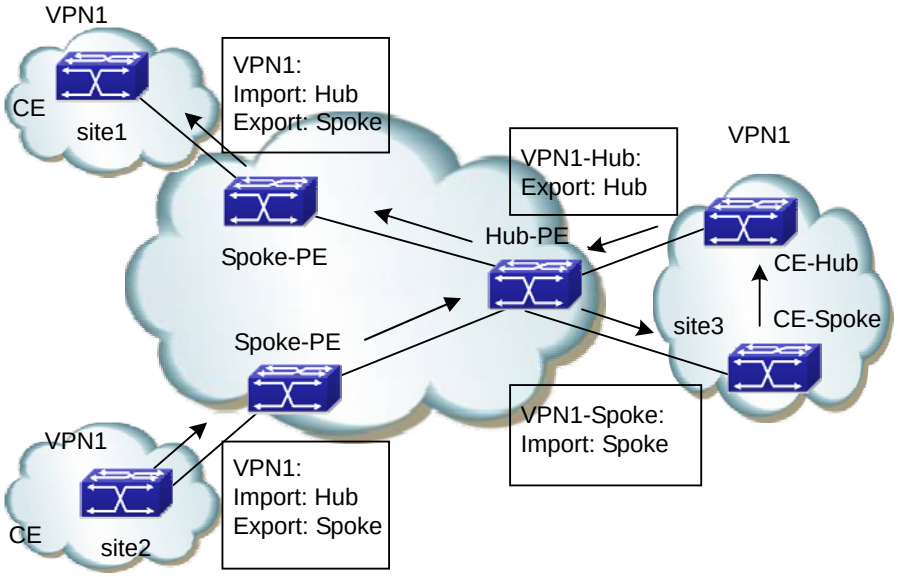

Fig 3-5 Hub&Spoke Networking Resolution

In the above figure, Spoke sites communicate with each other via Hub sites (the arrow in the figure is the route advertisement process from site2 to site1):

- Hub-PE can receive VPN-IPv4 routes advertised by all Spoke-PE
- The VPN-IPv4 routes advertised by Hub-PE can be received by all Spoke-PE;
- Since Hub-PE can advertise routes it learns from Spoke-PE to other Spoke-PE, the spoke sites can intercommunicate with each other via the Hub site.
- The Import Target attribute of any Spoke-PE is different from the Export Target attribute of other Spoke-PE. So, any pair of Spoke-PE cannot advertise VPN-IPv4 routes to each other or intercommunicate directly.

Extranet VPN

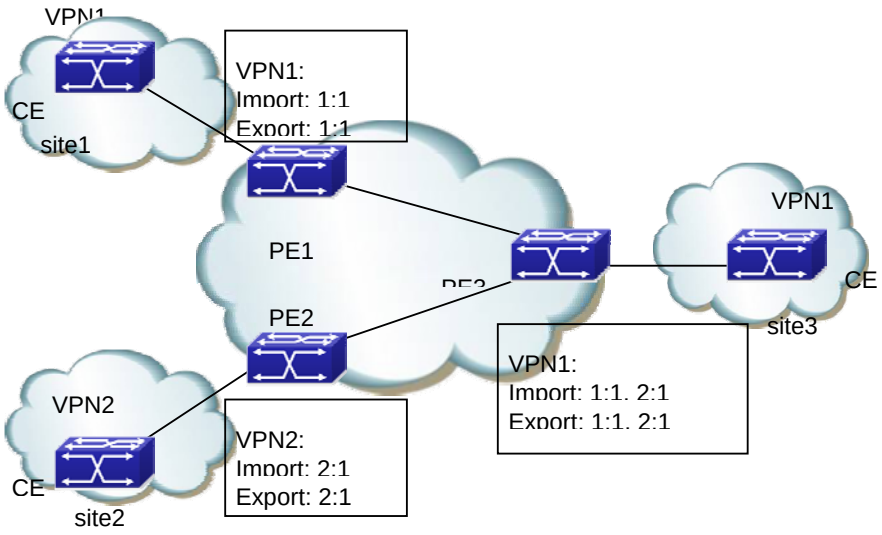

Fig 3-6 Extranet Networking Resolution

If a VPN user wants to provide some site resource of this VPN to outside users, the Extranet Networking resolution can solve the problem.

In this networking if a VPN needs to access the sharing site, its Export Target should be included in the Import Target of the sharing site VPN instances, and its Import Target should be included in the Export Target of the sharing site VPN instances.

In the above figure, site3 of VPN1 can be accessed by VPN1 and VPN2:

- PE3 can receive the VPN-IPv4 routes advertised by PE1 and PE2
- PE1 and PE2 can receive the VPN-IPv4 routes advertised by PE3
- Based on the above two conditions, site1 and site3 of VPN1 can intercommunicate, so do the site2 of VPN2 and site3 of VPN1.

PE3 won't advertise VPN-IPv4 routes from PE1 to PE2, or advertise the VPN-IPv4 route from PE2 to PE1 (the routes learnt from an IGBP neighbor won't be sent to other IBGP neighbors), so site1 of VPN1 and site2 of VPN2 can't intercommunicate.

3.1.5 BGP/MPLS VPN Route Advertisement

In basic BGP/MPLS VPN networks, VPN route advertisement concerns CE and PE, since P routers only maintains routes of the backbone network, and doesn't need any VPN route information. PE routers only maintain the VPN route information directly connected to it, not all VPN routes. SO the BGP/MPLS VPN network is easy to extend.

The VPN route advertisement process includes three parts to create a reachable route from the local CE to the remote CE, enabling the advertisement of VPN private network route information in the backbone network: from local CE to ingress PE, from the ingress PE to the egress PE, from egress PE to the remote CE.

The followings are introduction to the three parts:

The route information switch from the local CE to the ingress PE

CE will send the local VPN route to the PE directly connected to it after establishing an adjacency to the latter.

CE can use static routes, RIP, OSPF, IS-IS or EBGP to send routes to PE, all in the form of standard IPv4 routes.

The route information switch from the ingress PE to the egress PE

PE will add RD and VPN target attributes to the VPN routes it learns from CE, then store these VPN-IPv4 routes into the VPN instances created for CE.

The ingress PE will advertise the VPN-IPv4 routes to the egress PE via MP-BGP. The egress PE will determine whether to add this route into the route table of VPN instance according to the routes' Export Target attribute and the import Target of the VPN instances it maintains.

Different PE ensure the intercommunication between them via IGP.

The route information switch between the egress PE to the remote CE

Like the route information switch from the local CE to the ingress PE, there are many available methods for the remote CE to learn VPN routes the egress PE, including static route, RIP, OSPF, IS-IS and EBGP.

3.1.6 Multi-AS VPN Introduction

In real networking applications, multiple sites of a user VPN may connect to SP with different ASN, or to different AS of the same SP. Such applications of one VPN crossing multiple autonomy systems are called Multi-AS VPN. RFC 2547 provides three Multi-AS VPN resolutions:

- VRF-to-VRF：ASBR use VRF interface to create EBGP neighbors and manage VPN routes, which is also called Inter-Provider Option A;
- EBGP Redistribution of labeled VPN-IPv4 routes： ASBR use MP-EBGP to advertise label VPN-IPv4 routes, which is also called Inter-Provider Option B;
- Multihop EBGP redistribution of labeled VPN-IPv4 routes：PE use Multi-hop MP-EBGP to advertise label VPN-IPv4 routes, which is also called Inter-Provider Option C.

At present we support the first resolution: VRF-to-VRF Multi-VPN resolution.

Multi-VPN resolution

As demonstrated in the nest figure, in this mode, PE routers from two AS directly connects with each other, and serve as ASBR of the AS they belong to. These PE routers (ASBR) connect with each other via VRF interfaces, import all RT this system need the other end to learn, export all RT this system want to obtain from the other, and establish

EBGP connections through the VRF interfaces. As a result, the CE they serve will be able to intercommunicate with and isolate from each other like locating in the same AS, with two PE routers treating each other as their own CE. Packets will be forwarded within the AS as VPN packets in the 2-layer label mode, and forwarded as regular IP packets between ASBR.

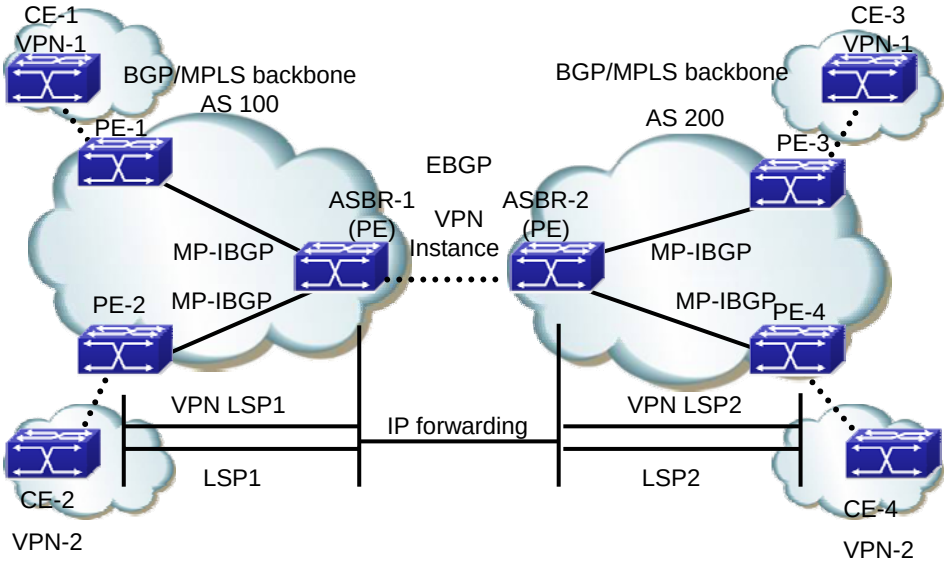

Fig 3-7 Multi-AS VPN Networking

- The advantage of this Multi-AS VPN mode is easy to realize: no special configuration is needed between the two PE serving as ASBR.
- The disadvantage is poor extendibility: the PE serving as ASBR need to manage all VPN routes, and create VPN instances for each VPN. This will cause too many VPN-IPv4 routes on PE.

3.2 BGP MPLS VPN Configuration

BGP MPLS VPN configuration task sequence:

1. Enable globally MPLS (necessary)
2. ） Configure VPN instances (necessary)
   (1) Create VPN instances, and enter the VPN instance view.
   (2) RD Configure the VPN instance RD
   (3) Configure the VPN instance RT
   (4) Configure the VPN instance to relate with the interface
3. Configure basic MPLS VPN (necessary)
   (1) Configure to use EBGP between PE-CE

1) Configure the remote PE as the public network VPNv4 neighbor
2) Enter the BGP-VPN instance view
3) Configure CE as the VPN private network neighbor
4) Advertise local private network routes

(2) Configure to use EBGP between PE-CE
1) Configure the remote PE as the public network VPNv4 neighbor
2) Create the OSPF instance between PE-CE, and enter the Router OSPF view.
3) Enable OSPF in the segment between PE-CE
4) Configure to re-advertise BGP routes
5) Enter the BGP-VPN instance view
6) Configure to re-advertise OSPF routes
7) Advertise local private network routes

(3) RIP Configure to use EBGP between PE-CE
1) Configure the remote PE as the public network VPNv4 neighbor
2) Enter the RIP VPN instance view
3) Enable RIP in the segment between PE-CE
4) Configure to re-advertise BGP routes
5) Enter the BGP-VPN instance view
6) Configure to re-advertise RIP routes
7) Advertise local private network routes

(4) Configure to use static routes between PE-CE
1) Configure the remote PE as the public network VPNv4 neighbor
2) Configure static VPN routes
3) Enter the BGP-VPN instance view
4) Configure to re-advertise static routes
5) Advertise local private network routes

1. Enable MPLS (necessary)

Command	Explanation
Global Configuration Mode	
mpls enable **no mpls enable**	Necessary Enable MPLS; the no operation will disable MPLS

2. Configure VPN instances (necessary)

(1) Create VPN instances and enter VPN instance view

(2) Configure VPN instance RD

(3) Configure VPN instance RT

(4) Configure VPN instance to relate with the interface

Command	Explanation
Global Configuration Mode	
[no] ip vrf <*vrf-name*>	Necessary Create VPN instances; no VPN instance is created by default
VRF Configuration Mode	
[no] rd <*ASN:nn*_or_*IP-address:nn*>	Necessary Configure VPN instance RD; no RD is created by default
[no] route-target {import | export | both} <*rt-value*>	Necessary Configure VPN instance RT
Interface Configuration Mode	
[no] ip vrf forwarding < ***vrf-name*** >	Necessary Configure VPN instance to relate with the interface
[no] ip address <*ip-address*> <*mask*>	Necessary Configure the private network IP address of the interface directly connecting PE and CE

3 Configure basic MPLS VPN (necessary)

(1) Configure to use EBGP between PE-CE

1) Configure the remote PE as the public network VPNv4 neighbor
2) Enter the BGP-VPN instance view
3) Configure CE as the VPN private network neighbor
4) Advertise local private network routes

Command	Explanation
BGP Protocol Configuration Mode	
neighbor <*ip-address*> remote-as <*as-num*>	necessary Configure the remote PE as the public network VPNv4 neighbor. It's suggest to select loopback interface to set up the BGP neighbor among public network PE.
neighbor <*ip-address*> update-source <*as-num*>	Point the local loopback interface for set up neighbor.
Enter the BGP-VPNv4 view	

address-family vpnv4 [unicast]	necessary Create BGP VPNv4. No VPNv4 is created by default.
[no] neighbor <*ip-address*> active	optional Activate all neighbors in VPNv4. All neighbors in VPNv4 view are inactive by default
BGP Protocol Configuration Mode	
[no] address-family ipv4 {unicast| multicast|vrf <*vrf-nam*>}	optional; Create BGP protocol IPv4 and enter the BGP-VPN instance view. No IPv4 is created by default
BGP-VPN instance view	
[no] neighbor <*ip-address*> remote-as <*as-num*>	optional Configure CE as the VPN private network neighbor. No private network neighbor is configured by default
[no] neighbor <*ip-address*> active	optional Activate all neighbors in VPNv4. All neighbors in VPNv4 view are active by default
[no] redistribute {connected|ospf|rip| static}	optional Configure to re-advertise the directly connected routes and other protocol routes. No re-advertisement of any route by default.

(2) Configure to use EBGP between PE-CE

1) Configure the remote PE as the public network VPNv4 neighbor
2) Create the OSPF instance between PE-CE, and enter the Router OSPF view
3) Enable OSPF in the segment between PE-CE
4) Configure to re-advertise BGP routes
5) Enter the BGP-VPN instance view
6) Configure to re-advertise OSPF routes
7) Advertise local private network routes

Command	Explanation
BGP Protocol Configuration Mode	

neighbor <*ip-address*> remote-as <*as-num*>	necessary Configure the remote PE as the public network VPNv4 neighbor. It's suggest to select loopback interface to set up the BGP neighbor among public network PE.
neighbor <*ip-address*> update-source <*as-num*>	Point the local loopback interface for set up neighbor.
Enter the BGP-VPNv4 view	
address-family vpnv4 [unicast]	necessary Create BGP VPNv4. No VPNv4 is created by default.
[no] neighbor <*ip-address*> active	optional Activate all neighbors in VPNv4. All neighbors in VPNv4 view are active by default
Global Configuration Mode	
[no] router ospf [<*process_id*> [<*vrf-nam*>]]	optional Create the OSPF instance between PE-CE, and enter the Router OSPF view
OSPF VPN instance view	
[no] network {<network> <mask> | <network>/<prefix>} area <area_id>	optioanal Enable OSPF in the segment between PE-CE. Enabled in no segment by default.
[no] redistribute { bgp | connected | static| rip | kernel} [metric-type { 1 | 2 }] [tag <tag>] [metric <cost_value>] [router-map <WORD>]	optional Configure to re-advertise the BGP routes. No re-advertisement of any route by default.
BGP Protocol Configuration Mode	
[no] address-family ipv4 {unicast| multicast|vrf <*vrf-nam*>}	optional create BGP VPNv4 and enter the BGP-VPN instance view. No VPNv4 is created by default.
BGP-VPN instance view	
[no] redistribute {connected | ospf | rip | static}	optional Configure to re-advertise the directly connected routes and other protocol routes. No re-advertisement of any route by default.

(3) Configure to use EBGP between PE-CE

1) Configure the remote PE as the public network VPNv4 neighbor
2) Enter the RIP VPN instance view
3) Enable RIP in the segment between PE-CE
4) Configure to re-advertise BGP routes
5) Enter the BGP-VPN instance view
6) Configure to re-advertise RIP routes
7) Advertise local private network routes

Command	Explanation
BGP Protocol Configuration Mode	
neighbor <*ip-address*> remote-as <*as-num*>	necessary Configure the remote PE as the public network VPNv4 neighbor. It's suggest to select loopback interface to set up the BGP neighbor among public network PE.
neighbor <*ip-address*> update-source <*as-num*>	Point the local loopback interface for set up neighbor.
Enter the BGP-VPNv4 view	
address-family vpnv4 [unicast]	necessary Create BGP VPNv4. No VPNv4 is created by default.
[no] neighbor <*ip-address*> active	optional Activate all neighbors in VPNv4. All neighbors in VPNv4 view are active by default
RIP Protocol Configuration Mode	
[no] address-family ipv4 vrf <*vrf-name*>	optional Create RIP IPv4 protocol family and enter RIP VPN instance view
RIP VPN instance view	
[no] network {*A.B.C.D/M*|*ifname*|*vlan <id>*|loopback <*1-1024*> }	Optional Enable the RIP between PE-CE
[no] redistribute { kernel | connected | static | ospf | isis | bgp} [metric <value>] [route-map<word>]	optional Configure to re-advertise the BGP routes. No re-advertisement of any route by default.
BGP Protocol Configuration Mode	

[no] address-family ipv4 {unicast| multicast|vrf <*vrf-nam*>}	optional Create BGP VPNv4 and enter the BGP-VPN instance view. No VPNv4 is created by default.
BGP-VPN instance view	
[no] redistribute {connected | ospf | rip | static}	optional Configure to re-advertise the directly connected routes and other protocol routes. No re-advertisement of any route by default.

(4) Configure to use static routes between PE-CE

1) Configure the remote PE as the public network VPNv4 neighbor
2) Configure static VPN routes
3) Enter the BGP-VPN instance view
4) Configure to re-advertise static routes
5) Advertise local private network routes

Command	Explanation
BGP Protocol Configuration Mode	
neighbor <*ip-address*> remote-as <*as-num*>	necessary Configure the remote PE as the public network VPNv4 neighbor. It's suggest to select loopback interface to set up the BGP neighbor among public network PE.
neighbor <*ip-address*> update-source <*as-num*>	Point the local loopback interface for set up neighbor.
Enter the BGP-VPNv4 view	
address-family vpnv4 [unicast]	necessary Create BGP VPNv4. No VPNv4 is created by default.
[no] neighbor <*ip-address*> active	optional Activate all neighbors in VPNv4. All neighbors in VPNv4 view are active by default
Global Configuration Mode	
[no] ip route vrf <vrf-name> {<ip-prefix> <mask>|<ip-prefix/<prefix-length>} {<gateway-address>|null0}	optional Manually configure the static VPN routes between PE-CE
BGP Protocol Configuration Mode	

[no] address-family ipv4 {unicast| multicast|vrf <*vrf-nam*>}	optional Create BGP VPNv4 and enter the BGP-VPN instance view. No VPNv4 is created by default.
BGP-VPN instance view	
[no] redistribute {connected|ospf|rip| static}	optional Configure to re-advertise the static routes, directly connected routes and other protocol routes. No re-advertisement of any route by default.

3.3 MPLS VPN

3.3.1 address-family ipv4

Command: address-family ipv4 [unicast | vrf <*vrf-name*>| multicast]

no address-family ipv4 vrf <*vrf-name*>

Function: Configure the BGP VPN address family; the no operation will cancel the configuration. Before entering the BGP-VPN view, this VRF should be created and configured with rd.

Parameters: unicast: unicast address family factor

<vrf-name> : the VPN route/forwarding instance name

Default: No BGP VPN address family.

Command Mode: BGP Route Configuration Mode.

Example:

Switch(config)#router bgp 100

Switch(config-router)#address-family ipv4 vrf VRF-A

Switch(config-router-af)#

3.3.2 address-family vpnv4

Command: address-family vpnv4 [unicast]

Function: Configure the BGP VPNv4 address family in non-default mode.

Parameters: unicast: the unicast address family factor.

Default: No BGP VPNv4 address family.

Command Mode: BGP Route Configuration Mode.

Example:

Switch(config)#router bgp 100

Switch(config-router)#address-family vpnv4 unicast

Switch(config-router-af)#

3.3.3 aggregate-address

Command: aggregate-address <*ip-address/M*> [summary-only] [as-set]

no aggregate-address <*ip-address/M*> [summary-only] [as-set]

Function: By aggregating addresses, users can decrease the route message propagation; the no operation will cancel the configuration.

Parameters: <*ip-address/M*>：IP address, MASK length

[summary-only]: Only send the summary and ignore the route.

[as-set]：Display each AS of the path once in the list form.

Default: No aggregate configuration.

Command Mode: BGP Route Configuration Mode, VRF Address Family Configuration Mode.

Usage Guide: By aggregating addresses, users can decrease the route message propagation. The summary-only option means only to send the summary and ignore the route, and the as-set option will display the AS of every route covered by the aggregate for once without repetition.

Example:

Switch(config-router)#aggregate-address 100.1.0.0/16 summary-only

Switch(config-router)#aggregate-address 100.2.0.0/16 summary-only as-set

Switch(config-router)#aggregate-address 100.3.0.0/16 as-set

Related Commands: bgp aggregate-nexthop-check, no bgp aggregate-nexthop-check

3.3.4 clear ip bgp

Command: clear ip bgp * [vrf <*vrf-name*>] [in | out | soft [in | out]]

Function: Reboot the corresponding bgp process of vrf-name, and the connections between all peers of the process.

Parameters: <*vrf-name*>: the configured VPN instance name, whose length ranges from 1 to 64 characters.

in: soft reboot and configure the inbound update;

out: soft reboot and configure the outbound update;

soft: soft reboot

Default: No configuration.

Command Mode: Admin Mode

Usage Guide: Implementing the “clear ip bgp *” command will restart the BGP process; configuring the “in” parameter will send route request message to neighbors; configuring the “out” parameter will send its route to neighbors; configuring the “soft” parameter won’t restart the BGP process.

Switch#clear ip bgp * vrf VRF-A

Switch#

3.3.5 debug bgp mpls

Command: debug bgp mpls

no debug bgp mpls

Function: Display the information about processing VRF FTN, the global FTN, and global ILM entries while the bgp vpn is running; the no operation will disable the display.

Parameters: None.

Default: No display of debug information.

Command Mode: Admin Mode.

Usage Guide: Enable the debug information to check the information about processing VRF FTN, the global FTN, and global ILM entries while the bgp vpn is running.

Example:

Switch#debug bgp mpls

Switch#

3.3.6 debug bgp update

Command: debug bgp update

no debug bgp update

Function: Display the route update information received by bgp vpn while it is running; the no command will disable the information.

Parameters: None.

Default: No display of debug information.

Command Mode: Admin Mode.

Example:

Switch#debug bgp update
Switch#

3.3.7 description

Command: description <*text*>

no description

Function: Configure the description of VRF to record information like the relationship between the VNP instance and a VPN; the no operation will disable the description.

Parameters: <text>: the descriptive text, whose length ranges from 1 to 256 characters.

Default: No configuration.

Command Mode: VRF Configuration Mode.

Usage Guide: Following “description” is user’s description of VRF, which will be displayed below the corresponding VRF to provide instructions.

Example: Configure the VRF description as “associate with VRF-B VRF-C**”.**

Switch(config)#ip vrf VRF-A
Switch(config-vrf)#description associate with VRF-B VRF-C

3.3.8 import map

Command: import map <*route-map-name*>

no import map

Function: Apply import-route-map policy to the specified VPN instance.

Parameters: <*route-map-name*>: the *route-map* policy name.

Default: No configuration.

Command Mode: VRF Configuration Mode.

Usage Guide: When a more accurate method of importing VPN instance routes than the extended-community attribute is required, the import-route policy is an option. By default, the imported routes will be filtered according to their VPN-target extended-community attribute. The import-route policy may decline the routes chosen from the communities in the import list.

Example: Apply the map-a route-map to the VRF instance VRF-A.

Switch(config)#ip vrf VRF-A
Switch(config-vrf)#import map map-a
Switch(config-vrf)#

3.3.9 ip route

Command: ip route <*Destination_prefix*> <*Destination_prefix_mask*> {vlan <*Vlan_ID*>| IFNAME} <*nexthop_address*> <*1~255*>

no ip route <*Destination_prefix*> <*Destination_prefix_mask*> {vlan <*Vlan_ID*>|IFNAME} <*nexthop_address*> <*1~255*>

Function: Configure a static route directing to the VPN site in the global route table, whose output interface is the one bound to VRF; the no operation will delete the configured static route.

Parameters: <*Destination_prefix*> is the destination prefix of the route；

<*Destination_prefix_mask*> is the destination prefix mask of the route；

<*Vlan_ID*> is the VLAN ID of the output interface; IFNAME is the interface name；

<*nexthop_addresss*> is the next-hop address of the route；

<*1~255*> is the administrative distance of the route.

Default: No static route.

Command Mode: Global Mode.

Usage Guide: This command is usually used to configure the route for the Internet to access the VPN on PE, where the VPN can access the Internet.

Example: Configure a static route, in which the destination IP is 20.20.20.0, the mask length is 24, the port is vlan 9 and the next-hop address is 20.20.20.23.

Switch(config)#ip route 20.20.20.0 255.255.255.0 vlan 9 20.20.20.23

Switch(config)#

3.3.10 ip route vrf

Command: ip route vrf <*vrf-name*>{<*ip-prefix*> <*mask*>|<*ip-prefix/prefix-length*>} {<*gateway-address*>|null0} [<*1-255*>]

no ip route vrf <*vrf-name*>{<*ip-prefix*> <*mask*>|<*ip-prefix/prefix-length*>} {<*gateway-address*>|null0} [<*1-255*>]

Function: Specify static routes for the specified VRF. Before doing this, a successful VPN forwarding instance is required. The no operation will delete the configured static routes.

Parameters: <*vrf-name*>： The specified VRF name

<*ip-prefix*>： the destination IP address

<*mask*>: mask, in dotted decimal format

<*prefix-length*>： the length of the prefix

<*gateway-address*>： the next-hop address

null0：the black hole route;

<***1-255***>：Administrative distance.

Example:

Switch(config)#ip route vrf VRF-A 10.1.1.10 255.255.255.0 10.1.1.1

Switch(config)#

3.3.11 ip vrf

Command: ip vrf <*vrf-name*>

Function: Configure a VPN instance with the specified name; the no operation will cancel the instance.

Parameters: <vrf-name> the configured VPN instance name, whose length is 1 to 64.

Default: No configuration.

Command Mode: Global Mode.

Usage Guide: Configure a VPN instance with the specified name. There is no default VPN instance on PE, which allows multiple VPN instances. The VPN instance name is case sensitive. Please notice that only after configuring RD will the VPN instance take effect.

Example:

Switch(config)#ip vrf VRF-A

Switch(config-vrf)#

3.3.12 ip vrf forwarding vrfName

Command: ip vrf forwarding <*vrfName*> [fallback global]

no ip vrf forwarding <*vrfName*> [fallback global]

Function: Bind interfaces to the specified VRF. With configuring the fallback global option of the interface, the interface, being the IP message input interface, will try a second lookup in the global route table if the lookup fails in the route table of the bound VRF.

Parameters: <vrfName> is the VRF name, a string shorter than 32 characters.

Fallback global: Look up the global route table. With configuring the fallback global option of the interface, the interface, will try a second lookup in the global route table if the lookup fails in the route table of the bound VRF.

Command Mode: Interface Configuration Mode.

Usage Guide: Implementing the command if the interface needs to access the Internet. Each interface can only be bound to one VRF, while the latter can be bounded with

multiple interfaces. The IGP supporting VPN will record the binding relationship between interfaces and VRF by adding a route received from the bound interface to the route table of the bound VRF. By default, the interface is bound to no VRF, and is a public network interface.

Example:

Switch(config)#int vlan 9

Switch(Config-if-Vlan9)#ip vrf forwarding vpn1 fallback global

3.3.13 neighbor remote-as

Command: neighbor <*ip-address*> remote-as <*as-num*>

no neighbor <*ip-address*> remote-as <*as-num*>

Function: Add a new BGP neighbor; the no operation will delete it.

Parameters: <ip-address>: specify the BGP neighbor address. BGP neighbor address should be Loopback port IP for neighbor switch.

<as-num>: specify the AS number of the BGP neighbor.

Default: No BGP neighbor.

Command Mode: VRF Address Family Configuration Mode.

Usage Guide: Implementing this command will add a new neighbor for the switch.

Example:

Switch(config)#router bgp 100

Switch(config-router)#address-family ipv4 vrf VRF-A

Switch(config-router-af)#neighbor 3.0.0.1 remote-as 65001

Switch(config-router-af)#

3.3.14 neighbor as-override

Command: neighbor {<*ip-address*> | <*TAG*>} as-override

no neighbor {<*ip-address*> | <*TAG*>} as-override

Function: Override the AS path (the previous AS number). Before implementing this command, users should create a neighbor first. The no operation will delete the configuration.

Parameters: <ip-address>: specify the BGP neighbor address;

<TAG>: Specify the BGP neighbor group number.

Default: Not configured.

Command Mode: VRF Address Family Configuration Mode.

Usage Guide: After this command being implemented, the route from the neighbor will override the existing AS number.

Example:

Switch(config)#router bgp 100

Switch(config-router)#address-family ipv4 vrf VRF-A

Switch(config-router-af)#neighbor 3.0.0.1 remote-as 65001

Switch(config-router-af)#neighbor 3.0.0.1 as-override

Switch(config-router-af)#

3.3.15 neighbor soo

Command: neighbor <*ip-addr*> soo <*soo-val*>

no neighbor <*ip-addr*> soo <*soo-val*>

Function: Configure the site-of-origin from the neighbor route; the no operation will delete the configuration.

Parameters: <ip-addr> the neighbor's ip address, in dotted-decimal format.

<soo-val> is the site-of-origin, in the same form as RD.

Default: Not configured.

Command Mode: VRF Address Family Configuration Mode.

Usage Guide: If the customer AS is connected with multiple ISP devices, configuring this attribute can prevent the customer route from returning to the customer after passing the P area. This configuration will propagate once set. The route with the SOO attribute won't propagate to the neighbor already configured with this attribute.

Example:

Switch(config)#router bgp 100

Switch(config-router)#address-family ipv4 vrf DC1

Switch(config-router-af)#neighbor 11.1.1.64 remote 200

Switch(config-router-af)#neighbor 11.1.1.64 soo 100:10

After configuring this attribute, the switch won't propagate the remote route with the 100:10 rt attribute to 11.1.1.64. (To be clear, the soo attribute will be checked together with other rt attributes, that is to say, the neighbor will be treated as the original neighbor no matter it is or not, once the rt is configured with the same attributes. In fact, soo is usually configured separately with a value different with rt/rd, and is unique in the reachable area to describe the origin accurately).

3.3.16 rd

Command: rd <*ASN:nn_or_IP-address:nn*>

Function: Configure the RD (Route Distinguish) of VRF.

Parameters: ASN*:nn_or_IP-address:nn*：The IP address format of the switch ID

Default: Not configured.

Command Mode: VRF Configuration Mode.

Usage Guide: RD can uniquely identify the VPN route. VPN instances realize address space independence via RD, and thus realize the address overlap between different VPNs. Usually the configuration includes the AS number and an arbitrary number. RD can't be deleted directly.

Example:

Switch(config)#ip vrf VRF-A

Switch(config-vrf)#rd 300:3

Switch(config-vrf)#

3.3.17 route-target

Command: route-target {import | export | both} <*rt-value*>

no route-target {import | export | both} <*rt-value*>

Function: Configure the Route-Target of the specified VRF 的 Route-Target; The no operation will delete the configuration.

Parameters: import：Means to filter the import route, which means to judge whether the VPN route can be added into the VRF;

export：Means to use the route of this VRF as the Route-Target that will be added to when the VPNv4 route sends out messages, in order to filter the interface import;

both：Means the import and the export use the same Route-Target;

<*rt-value*>：Is the the route target value.

Default: Not configured.

Command Mode: VRF Configuration Mode.

Usage Guide: A RT is a BGP extended community, for filtering the VPN routes and controlling the VNP membership of directly connected site and route policies. For the configured import rule, enumerate all routes received by the bgp process and add routes matching the condition (the export route-target overlaps with the import route-target of this VRF) to the bgp process of this VRF and advertise the route update messages to the bgp private network neighbors of this VRF. For the configured export rule, enumerate all bgp routes stored in the bgp process related with this VRF, add an export-target to these routes and advertise the route update messages to the bgp public network neighbors. If

there is an import route-target of some other VRF matches the export route- target, copy the routes to the matching VRF and advertise the route update messages to the bgp private network neighbors of it.

Example:

Switch(config)#ip vrf VRF-A

Switch(config-vrf)#route-target both 100:1

Switch(config-vrf)#

3.3.18 show ip bgp vpnv4

Command: show ip bgp vpnv4 {all|rd <*rd-val*>|vrf <*vrf-name*>}

Function: Implementing this command will display all VRF of this switch or route information of the specified VRF.

Parameters: all: all VPNv4 peers.

rd-val: the route distinguisher, usually in a format of numbers (AS number of IP address), such as 100:10.

<vrf-name> the configured VPN instance name, whose length is 1 to 64.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display information of a specified RD or VRF.

Example:

Switch#show ip bgp vpn4 all

Network Next Hop Metric LocPrf Weight Path

Route Distinguisher: 100:10 (Default for VRF DC1)

*> 11.1.1.0/24 11.1.1.64 0 0 200 ?

*> 20.1.1.0/24 11.1.1.64 0 0 200 ?

3.3.19 show ip route vrf

Command: show ip route vrf <*vrf-name*> [bgp|datebase]

Function: Display information of the specified route protocol.

Parameters: <vrf-name>: the VRF name created with the “if vrf<vrf-name>” command.

bgp: the route imported via bgp;

database: the IP route table database.

Default: None.

Command Mode: Admin and Config mode.

Usage Guide: Display information of the specified route protocol.

Example:

Switch#show ip route vrf vrf-a bgp

Network Next Hop Metric LocPrf Weight Path

Route Distinguisher: 100:10 (Default for VRF DC1)

*> 11.1.1.0/24 11.1.1.64 0 0 200 ?

*> 20.1.1.0/24 11.1.1.64 0 0 200 ?

3.3.20 show ip vrf

Command: show ip vrf [<*vrf-name*>]

Function: Implementing this command will display the RIP instance information related with this VPN route/forwarding instance and the fallback global option of the interfaces bound with the VRF.

Parameters: <vrf-name> specifies the name of the VPN route/forwarding instance.

Default: No display by default.

Command Mode: Admin and Config mode.

Usage Guide: This command also exists in other route protocols. Implementing this command will also display the information of other related route protocol processes.

Example: Display the information of the RIP instances related with the IPI vrf route/forwarding instance.

Switch#show ip vrf IPI

VRF IPI, FIB ID 1

Router ID: 11.1.1.1 (automatic)

Interfaces:

Vlan1

!

VRF IPI; (id=1); RIP enabled Interfaces:

Ethernet1/8

Name	Interfaces
IPI	Vlan1

Name	Default RD	Interfaces
IPI		Vlan1

3.4 BGP MPLS VPN Typical Instances

3.4.1 Create BGP MPLS VPN between PE-CE via EBGP

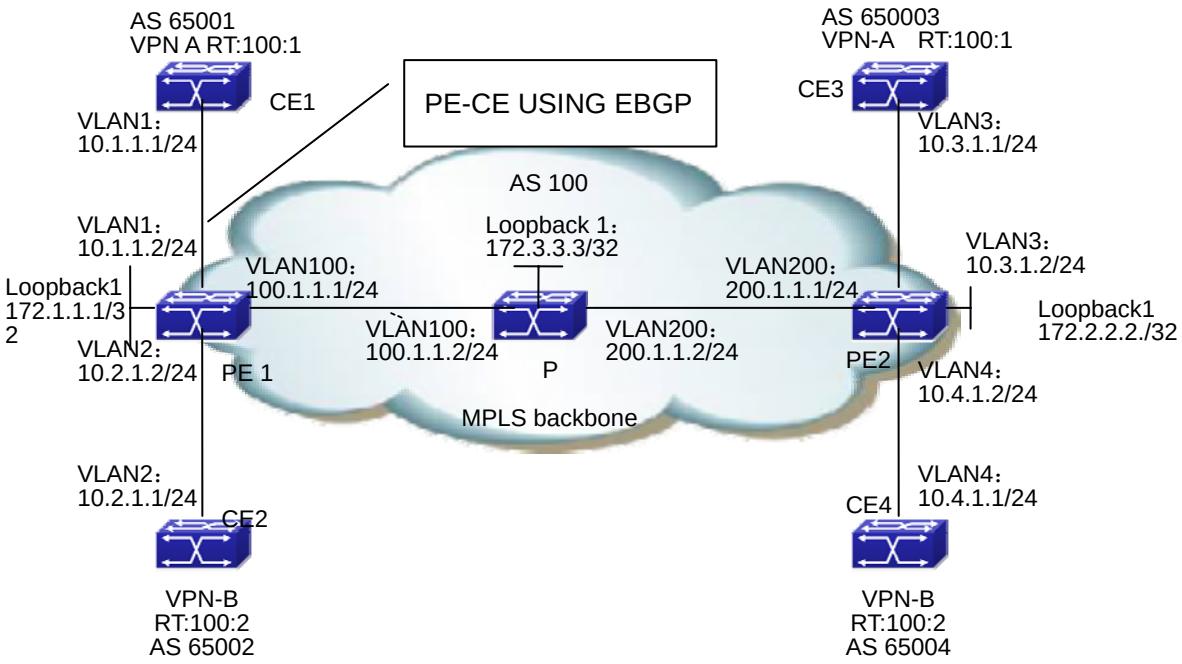

Fig 3-8 Create BGP MPLS VPN between PE-CE via EBGP

The configuration of CE1 is as follows : (the configurations of CE2~CE4 are similar)

CE1#config

CE1(config)# interface vlan 1

CE1(config-if-Vlan1)#ip address 10.1.1.1 255.255.255.0

CE1(config-if-Vlan1)#exit

CE1(config)# router bgp 65001

CE1(config-router)#neighbor 10.1.1.2 remote-as 100

CE1(config-router)#redistribute connect

CE1(config-router)#exit

The configuration of MPLS BGP on switch PE1 is as follows:

(1) Configure VPN instances

PE1#config

PE1(config)#ip vrf vpna

```
PE1(config-vrf)#rd 100:1
PE1(config-vrf)#route-target both 100:1
PE1(config)#ip vrf vpnb
PE1(config-vrf)#rd 100:2
PE1(config-vrf)#route-target both 100:2
```

(2) Configure to bind the interface with the VPN instances

```
PE1(config)# interface vlan 1
PE1(config-if-Vlan1)# ip vrf forwarding vpna
PE1(config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0
PE1(config-if-Vlan1)#exit
PE1(config)# interface vlan 2
PE1(config-if-Vlan2)# ip vrf forwarding vpnb
PE1(config-if-Vlan2)#ip address 10.2.1.2 255.255.255.0
PE1(config-if-Vlan2)#exit
```

(3) Globally enable MPLS and LDP

```
PE1(config)#mpls enable
PE1(config)#router ldp
PE1(config-router)#exit
```

(4) LDP Configure the interface and enable LDP

```
PE1(config)# interface loopback 1
PE1(config-if-Loopback1)# ip address 172.1.1.1 255.255.255.255
PE1(config-if-Loopback1)# exit
PE1(config)# interface vlan 100
PE1(config-if-Vlan100)#ip address 100.1.1.1 255.255.255.0
PE1(config-if-Vlan100)#label-switching
PE1(config-if-Vlan100) #ldp enable
PE1(config-if-Vlan100)#exit
```

(5) Enable OSPF to advertise the inner network routes

```
PE1(config)#router ospf
PE1(config-router)# ospf router-id 172.1.1.1
PE1(config-router)# network 0.0.0.0 0.0.0.0 area 0
PE1(config-router)# redistribute connected
```

(6) Configure BGP

```
PE1(config)# router bgp 100
PE1(config-router)#neighbor 172.2.2.2 remote-as 100
PE1(config-router)#neighbor 172.2.2.2 update-source 172.1.1.1
PE1(config-router)#address-family vpnv4
PE1(config-router-af)#neighbor 172.2.2.2 active
```

PE1(config-router-af)#exit

PE1(config-router)# address-family ipv4 vrf

PE1(config-router)# address-family ipv4 vrf vpna

PE1(config-router-af)#neighbor 10.1.1.1 remote-as 65001

PE1(config-router-af)#redistribute connected

PE1(config-router-af)#exit

PE1(config-router)# address-family ipv4 vrf vpnb\

PE1(config-router-af)#neighbor 10.2.1.1 remote-as 65002

PE1(config-router-af)#redistribute connected

PE1(config-router-af)#exit

PE1(config-router)#exit

The configuration of router P is as follows:

(1) Globally enable MPLS and configure LDP on related interfaces.

P#config

P(config)#mpls enable

P(config)#router ldp

P(config-router)#exit

P(config)# interface loopback 1

P(config-if-Loopback1)# ip address 172.3.3.3 255.255.255.255

P(config-if-Loopback1)# exit

P(config)#interface vlan 100

P(config-if-Vlan100)#ip address 100.1.1.2 255.255.255.0

P(config-if-Vlan100)#label-switching

P(config-if-Vlan100)#ldp enable

P(config-if-Vlan100)#exit

P(config)#interface vlan200

P(config-if-Vlan200)#ip address 200.1.1.2 255.255.255.0

P(config-if-Vlan200)#label-switching

P(config-if-Vlan200)#ldp enable

P(config-if-Vlan200)#exit

(2) Configure OSPF

P(config)#router ospf

P(config-router)# ospf router-id 172.3.3.3

P(config-router)# network 0.0.0.0 0.0.0.0 area 0

P(config-router)# redistribute connected

The configuration of switch PE2 is as follows:

(1) Configure VPN instances

PE2#config

PE2(config)#ip vrf vpna

PE2(config-vrf)#rd 100:1

PE2(config-vrf)#route-target both 100:1

PE2(config)#ip vrf vpnb

PE2(config-vrf)#rd 100:2

PE2(config-vrf)#route-target both 100:2

(2) Configure to bind the interface with the VPN instances

PE2(config)# interface vlan 3

PE2(config-if-Vlan3)# ip vrf forwarding vpna

PE2(config-if-Vlan3)#ip address 10.3.1.2 255.255.255.0

PE2(config-if-Vlan3)#exit

PE2(config)# interface vlan 4

PE2(config-if-Vlan4)# ip vrf forwarding vpnb

PE2(config-if-Vlan4)#ip address 10.4.1.2 255.255.255.0

PE2(config-if-Vlan4)#exit

(3) Globally enable MPLS and LDP

PE2(config)#mpls enable

PE1(config)#router ldp

PE1(config-router)#exit

(4) LDP Configure the interface and enable LDP

PE2(config)# interface loopback 1

PE2(config-if-Loopback1)# ip address 172.2.2.2 255.255.255.255

PE2(config-if-Loopback1)# exit

PE2(config)# interface vlan 200

PE2(config-if-Vlan200)#ip address 200.1.1.1 255.255.255.0

PE2(config-if-Vlan200)#label-switching

PE2(config-if-Vlan200) #ldp enable

PE2(config-if-Vlan200)#exit

(5) Enable OSPF to advertise the inner network routes

PE2(config)#router ospf

PE2(config-router)# ospf router-id 172.2.2.2

PE2(config-router)# network 0.0.0.0 0.0.0.0 area 0

PE2(config-router)# redistribute connected

(6) Configure BGP

PE2(config)# router bgp 100

PE2(config-router)#neighbor 172.1.1.1 remote-as 100

PE2(config-router)#neighbor 172.1.1.1 update-source 172.2.2.2

PE2(config-router)#address-family vpnv4

PE2(config-router-af)#neighbor 172.1.1.1 active

PE2(config-router-af)#exit

PE2(config-router)# address-family ipv4 vrf

PE2(config-router)# address-family ipv4 vrf vpna

PE2(config-router-af)#neighbor 10.3.1.1 remote-as 65003

PE2(config-router-af)#redistribute connected

PE2(config-router-af)#exit

PE2(config-router)# address-family ipv4 vrf vpnb

PE2(config-router-af)#neighbor 10.4.1.1 remote-as 65004

PE2(config-router-af)#redistribute connected

PE2(config-router-af)#exit

PE2(config-router)#exit

3.4.2 Create BGP MPLS VPN between PE-CE via OSPF

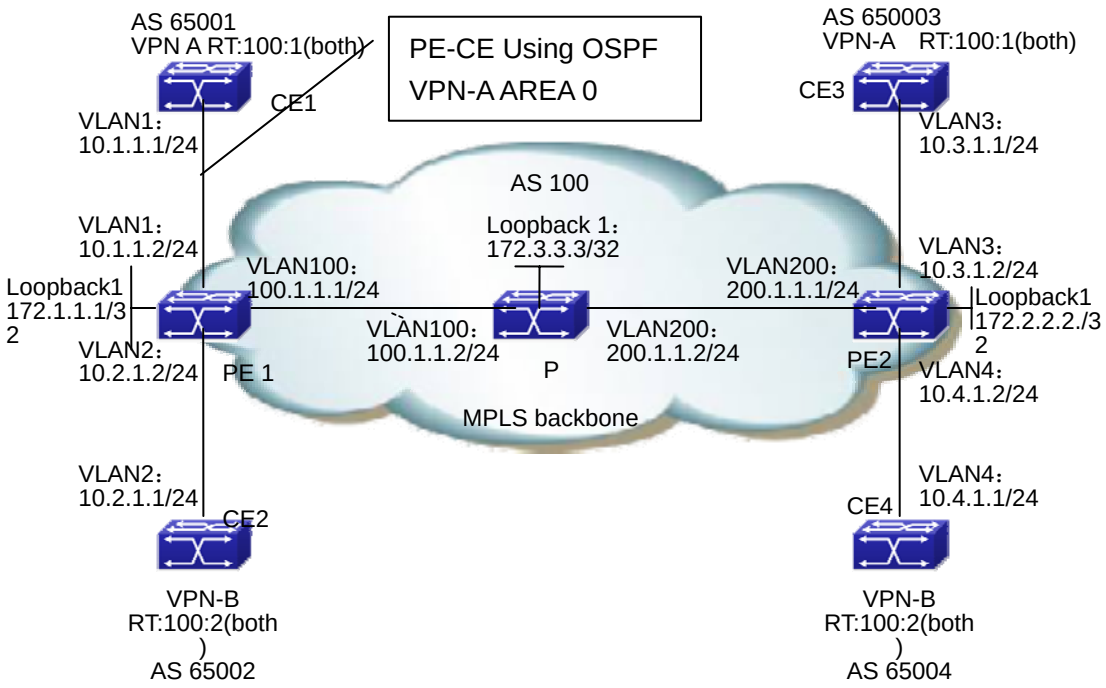

Fig 3-9 Create BGP MPLS VPN between PE-CE via OSPF

The configuration of CE1 is as follows : (the configurations of CE2~CE4 are similar)

CE1#config

CE1(config)# interface vlan 1

CE1(config-if-Vlan1)#ip address 10.1.1.1 255.255.255.0

CE1(config-if-Vlan1)#exit

CE1(config)# router ospf

CE1(config-router)#network 0.0.0.0 0.0.0.0 area 0

CE1(config-router)#redistribute connect

CE1(config-router)#exit

The confiugraiton of MPLS BGP on switch PE1 is as follows : (the configuration of PE2 is similar)

(1) Configure VPN instances

PE1#config

PE1(config)#ip vrf vpna

PE1(config-vrf)#rd 100:1

PE1(config-vrf)#route-target both 100:1

PE1(config)#ip vrf vpnb

PE1(config-vrf)#rd 100:2

PE1(config-vrf)#route-target both 100:2

(2) Configure to bind the interface with the VPN instances

PE1(config)# interface vlan 1

PE1(config-if-Vlan1)# ip vrf forwarding vpna

PE1(config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0

PE1(config-if-Vlan1)#exit

PE1(config)# interface vlan 2

PE1(config-if-Vlan2)# ip vrf forwarding vpnb

PE1(config-if-Vlan1)#ip address 10.2.1.2 255.255.255.0

PE1(config-if-Vlan1)#exit

(3) Globally enable MPLS and LDP

PE1(config)#mpls enable

PE1(config)#router ldp

PE1(config-router)#exit

(4) LDP Configure the interface and enable LDP

PE1(config)# interface loopback 1

PE1(config-if-Loopback1)# ip address 172.1.1.1 255.255.255.255

PE1(config-if-Loopback1)# exit

PE1(config)# interface vlan 100

PE1(config-if-Vlan100)#ip address 100.1.1.1 255.255.255.0

PE1(config-if-Vlan100)# label-switching

PE1(config-if-Vlan100) #ldp enable

PE1(config-if-Vlan100)#exit

(5) Enable OSPF to advertise the inner network routes

PE1(config)#router ospf

PE1(config-router)# ospf router-id 172.1.1.1

PE1(config-router)# network 0.0.0.0 0.0.0.0 area 0

PE1(config-router)# redistribute connected

PE1(config-router)#exit

(6) Enable OSPF VRF to advertise the private network routes

PE1(config)#router ospf 1 vpna

PE1(config-router)# network 0.0.0.0 0.0.0.0 area 0

PE1(config-router)#redistribute connected

PE1(config-router)#redistribute bgp

PE1(config-router)#exit

PE1(config)#router ospf 1 vpnb

PE1(config-router)# network 0.0.0.0 0.0.0.0 area 0

PE1(config-router)#redistribute connected

PE1(config-router)#redistribute bgp

PE1(config-router)#exit

(7) Configure BGP

PE1(config)# router bgp 100

PE1(config-router)#neighbor 172.2.2.2 remote-as 100

PE1(config-router)#neighbor 172.2.2.2 update-source 172.1.1.1

PE1(config-router)#address-family vpnv4

PE1(config-router-af)#neighbor 172.2.2.2 active

PE1(config-router-af)#exit

PE1(config-router)# address-family ipv4 vrf vpna

PE1(config-router-af)#redistribute connected

PE1(config-router-af)#redistribute ospf

PE1(config-router-af)#exit

PE1(config-router)# address-family ipv4 vrf vpnb

PE1(config-router-af)#redistribute connected

PE1(config-router-af)#redistribute ospf

PE1(config-router-af)#exit

PE1(config-router)#exit

The configuration of router P is as follows:

(1) Globally enable MPLS and configure LDP on related interfaces.

P#config

P(config)#mpls enable

P(config)#router ldp

P(config-router)#exit

P(config)# interface loopback 1

P(config-if-Loopback1)# ip address 172.3.3.3 255.255.255.255

P(config-if-Loopback1)# exit

P(config)#interface vlan 100

P(config-if-Vlan100)#ip address 100.1.1.2 255.255.255.0

P(config-if-Vlan100)#label-switching

P(config-if-Vlan100)#ldp enable

P(config-if-Vlan100)#exit

P(config)#interface vlan200

P(config-if-Vlan200)#ip address 200.1.1.2 255.255.255.0

P(config-if-Vlan200)#label-switching

P(config-if-Vlan200)#ldp enable

P(config-if-Vlan200)#exit

(2) Configure OSPF

P(config)#router ospf

P(config-router)# ospf router-id 172.3.3.3

P(config-router)# network 0.0.0.0 0.0.0.0 area 0

P(config-router)# redistribute connected

3.4.3 Create BGP MPLS VPN between PE-CE via RIP

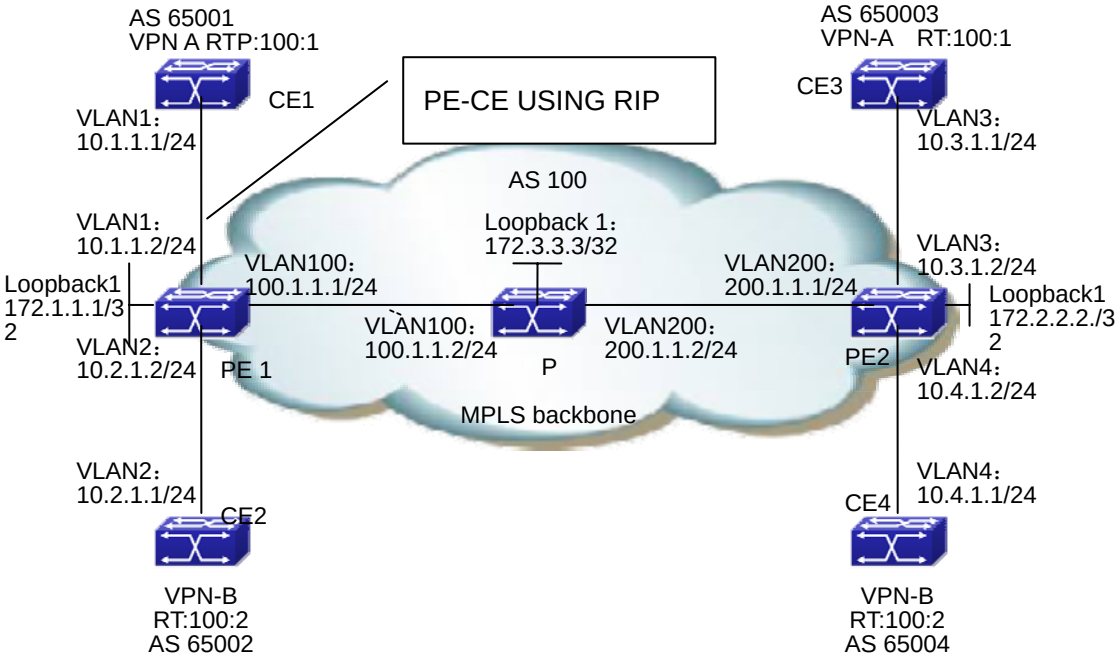

Fig 3-10 Create BGP MPLS VPN between PE-CE via RIP

The configuration of CE1 is as follows : (the configurations of CE2~CE4 are similar)

CE1#config

CE1(config)# interface vlan 1

CE1(config-if-Vlan1)#ip address 10.1.1.1 255.255.255.0

CE1(config-if-Vlan1)#exit

CE1(config)# router rip

CE1(config-router)#network 0.0.0.0/0

CE1(config-router)#redistribute connect

CE1(config-router)#exit

The confiugraiton of MPLS BGP on switch PE1 is as follows : (the configuration of PE2 is similar)

(1) Configure VPN instances

PE1#config

PE1(config)#ip vrf vpna

PE1(config-vrf)#rd 100:1

PE1(config-vrf)#route-target both 100:1

PE1(config)#ip vrf vpnb

PE1(config-vrf)#rd 100:2

PE1(config-vrf)#route-target both 100:2

(2) Configure to bind the interface with the VPN instances

PE1(config)# interface vlan 1

PE1(config-if-Vlan1)# ip vrf forwarding vpna

PE1(config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0

PE1(config-if-Vlan1)#exit

PE1(config)# interface vlan 2

PE1(config-if-Vlan2)# ip vrf forwarding vpnb

PE1(config-if-Vlan1)#ip address 10.2.1.2 255.255.255.0

PE1(config-if-Vlan1)#exit

(3) Globally enable MPLS and LDP

PE1(config)#mpls enable

PE1(config)#router ldp

PE1(config-router)#exit

(4) LDP Configure the interface and enable LDP

PE1(config)# interface loopback 1

PE1(config-if-Loopback1)# ip address 172.1.1.1 255.255.255.255

PE1(config-if-Loopback1)# exit

PE1(config)# interface vlan 100

PE1(config-if-Vlan100)#ip address 100.1.1.1 255.255.255.0

PE1(config-if-Vlan100)#label-switching

PE1(config-if-Vlan100) #ldp enable

PE1(config-if-Vlan100)#exit

(5) Enable OSPF to advertise the inner network routes

PE1(config)#router ospf

PE1(config-router)# ospf router-id 172.1.1.1

PE1(config-router)# network 0.0.0.0 0.0.0.0 area 0

PE1(config-router)# redistribute connected

PE1(config-router)#exit

(6) Enable OSPF VRF to advertise the private network routes

PE1(config)#router rip

PE1(config-router)#address-family ipv4 vrf vpna

PE1(config-router-af)#network 0.0.0.0/0

PE1(config-router-af)#redistribute connected

PE1(config-router-af)#redistribute bgp

PE1(config-router-af)#exit

PE1(config-router)#address-family ipv4 vrf vpnb

PE1(config-router-af)#network 0.0.0.0/0

PE1(config-router-af)#redistribute connected

PE1(config-router-af)#redistribute bgp

PE1(config-router-af)#exit

PE1(config-router)#exit

(7) Configure BGP

PE1(config)# router bgp 100

PE1(config-router)#neighbor 172.2.2.2 remote-as 100

PE1(config-router)#neighbor 172.2.2.2 update-source 172.1.1.1

PE1(config-router)#address-family vpnv4

PE1(config-router-af)#neighbor 172.2.2.2 active

PE1(config-router-af)#exit

PE1(config-router)# address-family ipv4 vrf vpna

PE1(config-router-af)#redistribute connected

PE1(config-router-af)#redistribute ospf

PE1(config-router-af)#exit

PE1(config-router)# address-family ipv4 vrf vpnb

PE1(config-router-af)#redistribute connected

PE1(config-router-af)#redistribute ospf

PE1(config-router-af)#exit

PE1(config-router)#exit

The configuration of switch P is as follows

(1) Globally enable MPLS and configure LDP on related interfaces.

P#config

P(config)#mpls enable

P(config)#router ldp

P(config-router)#exit

P(config)# interface loopback 1

P(config-if-Loopback1)# ip address 172.3.3.3 255.255.255.255

P(config-if-Loopback1)# exit

P(config)#interface vlan 100

P(config-if-Vlan100)#ip address 100.1.1.2 255.255.255.0

P(config-if-Vlan100)#label-switching

P(config-if-Vlan100)#ldp enable

P(config-if-Vlan100)#exit

P(config)#interface vlan200

P(config-if-Vlan200)#ip address 200.1.1.2 255.255.255.0

P(config-if-Vlan200)#label-switching

P(config-if-Vlan200)#ldp enable

P(config-if-Vlan200)#exit

(2) Configure OSPF

P(config)#router ospf

P(config-router)# ospf router-id 172.3.3.3

P(config-router)# network 0.0.0.0 0.0.0.0 area 0

P(config-router)# redistribute connected

3.4.4 Create BGP MPLS VPN between PE-CE via Static Routes

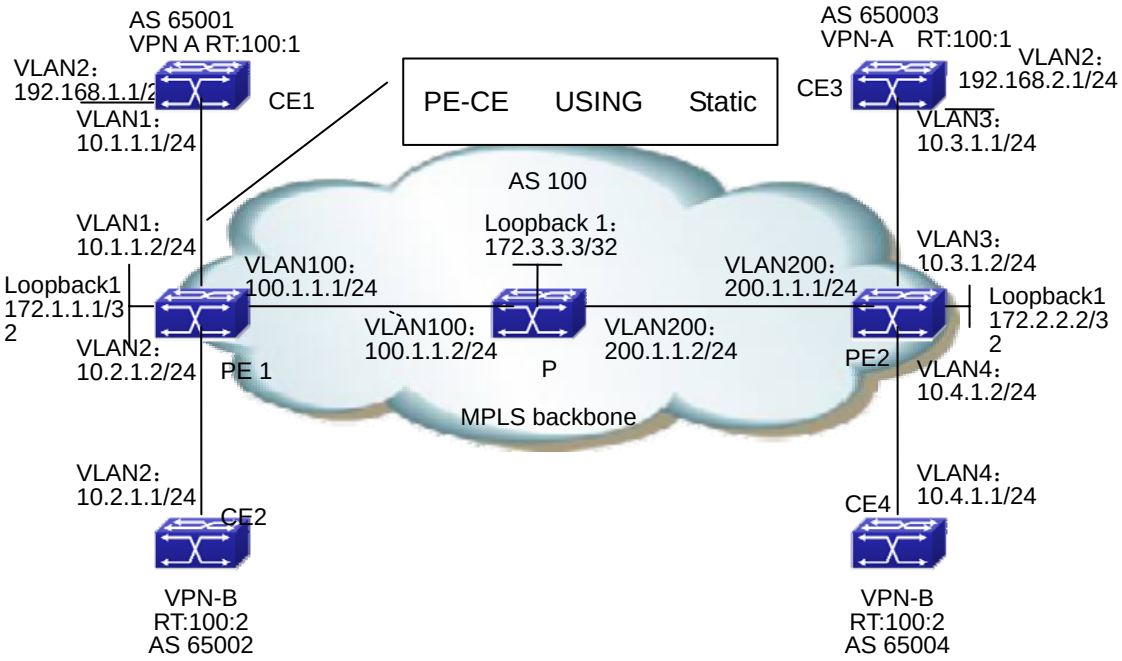

Fig 3-11 Create BGP MPLS VPN between PE-CE via Static Routes

The configuration of CE1 is as follows : (the configurations of CE2~CE4 are similar)

CE1#config

CE1(config)# interface vlan 1

CE1(config-if-Vlan1)#ip address 10.1.1.1 255.255.255.0

CE1(config-if-Vlan1)#exit

CE1(config)# interface loopback 1

CE1(config-if-Vlan1)#ip address 192.168.1.1 255.255.255.0

CE1(config-if-Vlan1)# exit

CE1(config)# ip route vrf vpna 192.168.2.1/24 10.1.1.2

The confiugraiton of MPLS BGP on switch PE1 is as follows : (the configuration of PE2 is similar)

(1) Configure VPN instances

PE1#config

PE1(config)#ip vrf vpna

PE1(config-vrf)#rd 100:1

PE1(config-vrf)#route-target both 100:1

PE1(config)#ip vrf vpnb

PE1(config-vrf)#rd 100:2

PE1(config-vrf)#route-target both 100:2

(2) Configure to bind the interface with the VPN instances

PE1(config)# interface vlan 1

PE1(config-if-Vlan1)# ip vrf forwarding vpna

PE1(config-if-Vlan1)#ip address 10.1.1.2 255.255.255.0

PE1(config-if-Vlan1)#exit

PE1(config)# interface vlan 2

PE1(config-if-Vlan2)# ip vrf forwarding vpnb

PE1(config-if-Vlan1)#ip address 10.2.1.2 255.255.255.0

PE1(config-if-Vlan1)#exit

(3) Globally enable MPLS and LDP

PE1(config)#mpls enable

PE1(config)#router ldp

PE1(config-router)#exit

(4) Configure the interface and enable LDP

PE1(config)# interface loopback 1

PE1(config-if-Loopback1)# ip address 172.1.1.1 255.255.255.255

PE1(config-if-Loopback1)# exit

PE1(config)# interface vlan 100

PE1(config-if-Vlan100)#ip address 100.1.1.1 255.255.255.0

PE1(config-if-Vlan100) #ldp enable

PE1(config-if-Vlan100)#exit

(5) Enable OSPF to advertise the inner network routes

PE1(config)#router ospf

PE1(config-router)# ospf router-id 172.1.1.1

PE1(config-router)# network 0.0.0.0 0.0.0.0 area 0

PE1(config-router)# redistribute connected

PE1(config-router)#exit

(6) Configure static private network routes

PE1(config)# ip route vrf vpna 192.168.1.1/24 10.1.1.2

PE1(config)# ip route vrf vpnb 192.168.2.1/24 10.1.1.2

PE1(config-router)#address-family ipv4 vrf vpna

PE1(config-router-af)#network 0.0.0.0/0

PE1(config-router-af)#redistribute connected

PE1(config-router)#exit

(7) Configure BGP

PE1(config)# router bgp 100

PE1(config-router)#neighbor 172.2.2.2 remote-as 100

PE1(config-router)#neighbor 172.2.2.2 update-source 172.1.1.1

PE1(config-router)#address-family vpnv4

PE1(config-router-af)#neighbor 172.2.2.2 active

PE1(config-router-af)#exit

PE1(config-router)# address-family ipv4 vrf vpna

PE1(config-router-af)#redistribute connected

PE1(config-router-af)#redistribute static

PE1(config-router-af)#exit

PE1(config-router)# address-family ipv4 vrf vpnb

PE1(config-router-af)#redistribute connected

PE1(config-router-af)# redistribute static

PE1(config-router-af)#exit

PE1(config-router)#exit

The configuration of switch P is as follows

(1) Globally enable MPLS and configure LDP on related interfaces.

P#config

P(config)#mpls enable

P(config)#router ldp

P(config-router)#exit

P(config)# interface loopback 1

P(config-if-Loopback1)# ip address 172.3.3.3 255.255.255.255

P(config-if-Loopback1)# exit

P(config)#interface vlan 100

P(config-if-Vlan100)#ip address 100.1.1.2 255.255.255.0

P(config-if-Vlan100)#ldp enable

P(config-if-Vlan100)#exit

P(config)#interface vlan200

P(config-if-Vlan200)#ip address 200.1.1.2 255.255.255.0

P(config-if-Vlan100)#ldp enable

P(config-if-Vlan200)#exit

(2) Configure OSPF

P(config)#router ospf

P(config-router)# ospf router-id 172.3.3.3

P(config-router)# network 0.0.0.0 0.0.0.0 area 0

P(config-router)# redistribute connected

3.5 MPLS BGP VPN Troubleshooting

When configuring and using MPLS BGP VPN, some problems like incorrect physical connections, configuration errors may cause it to fail, so please pay attention to the following notices to avoid them:

- ☞ First, make sure the creation of OSPF neighbors between PE1, P and PE2, the advertisement of routes including the loopback interface and the creation of BGP neighbor between PE are correct.
- ☞ Second, make sure the LDP is globally enabled on PE1, P and PE2, and correctly enabled on active interfaces. Check whether the establishment of LDP sessions on PE1, P and PE2 is correct.
- ☞ Then, make sure the PE-CE route advertisement mode used when creating the VPN and corresponding configuration are correct. Check whether CE advertises related private network route to the remote PE. Please notice that CE needs no VRF instance. If EBGP is used to advertise the private network routes, the BGP ASN between CE1 and CE2 shouldn't be the same, or the loop detection of BGP will filter the corresponding private network routes.
- ☞ Next, make sure the BGP VPN instances on PE are correctly configured. When using OSPF or RIP to create and advertise PE-CE routes, please import BGP routs and import corresponding OSPF and RIP routes to the BGP VPN instances. Implementing "show ip bgp vpnv4 all" on PE1 will display the route information of CE1 and CE2, if the configuration is correct. Implementing "show mpls vrf-table" on PE will display that the labels are distributed to corresponding private network routes, and the state is UP. If the Oper status in the vrf-table of the corresponding private network routes, use "show mpls ftn-table" to check whether the corresponding FEC create ftn.
- ☞ At last, if all above steps are correct, use "show ip route" on CE1 and CE2 to check the correct route information in the VPN. It is not recommended for users to create VPN via the static routes unless very familiar with BGP MPLS VPN.
- ☞ Besides, if no remote CE device can be checked on CE after saving the correction configuration and rebooting the device, please be patience, since the establishing OSPF, LDP, BGP connections and advertising routes are time-consuming.

Chapter 4 Public Network Access of MPLS VPN

4.1 Public Network Access Introduction

Public network access of VPN means the ability of VPN sites to access public Internet. RFC4364 defines the basic protocol regulations, including 4 methods for VPN to access Internet:

- ☞ Non-VRF Internet Access Mode
- ☞ VRF Internet Access Mode 1
- ☞ VRF Internet Access Mode 2
- ☞ VRF Internet Access Mode 3

4.1.1 Non-VRF Internet Access Mode

As demonstrated in the next figure, in non-VRF Internet Access Mode, PE routers communicate with Internet gateways via non-VFP interface; and the Internet access traffic of VPN sites are forwarded according to the global route table of PE routers. The CE and PE routers capable of accessing Internet have two connections, one with the public network interface of PE (public network connection), the other with the priviate network interface of PE (private network connection). The global route table of PE routes can contain the whole or part of Internet routes, or only a default routes pointing to the Internet gateway. CE routers learn Interet routs via the public network connection, and advertise to PE via the public network connection the globally registered IP address sub-net routes in the VPN site, which will be advertised to the Internet gateway by PE and finally to Internet. The Internet access traffic of VPN sites is also sent and received by the public network connection. The private network connection between CE and PE is for the route learning of CE and advertising the private network routes in tehe VPN. The VPN sites also communicate via private network connections, and forward according to the VRF route table of PE routers. In this mode, the global and VRF rout table of PE routers are completely isolated ; and the distribution of VPN routes and Internet routes are completely independent.

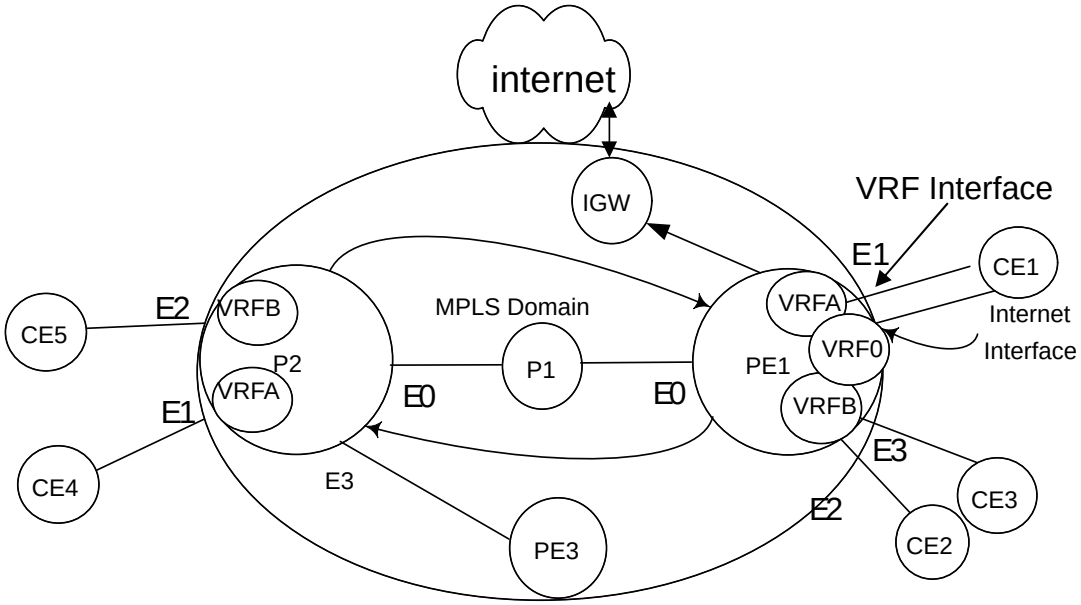

Fig 4-1 Non-VRF Internet Access Mode

4.1.2 VRF Internet Access Mode 1

As demonstrated in the next figure, in VRF Internet Access Mode 1, PE routers communicate with Internet gateways via non-VFP interface. The Internet access traffic of VPN sites and the traffic between VPN sites are sent and received via the private netwrok connections between CE and PE. PE routes contain the whole or part of Internet routes, or only a default routes pointing to the Internet gateway. When the IP packets accessing Internet from VPN reach the VRF interfaces of PE, a failed lookup in the VRF route table will cause a lookup in the global route table. If a match is found, the pakce will be forwarded to the Internet gateway, and finaly to Internet via the gateway. To emable the Internet hosts access VPN sites, a special static route needs to be registered in the PE global route table, whose destiantion segment is the IP address sub-net address which is globally registered in the VPN site, egress interface is the private network interface pointing to the VPN site, and next-hop is CE router. This static route is advertised to the internet gateway by PE, and then to Internet by the gateway. When the packets from the Internet to the VPN reach the pbulic network interface of PE, it will be forwarded to the next-hop via the private network interface if it matches the static route in the PE's global route tabel poinging to the VPN site. In this mode, the global route table and VRF route tabel of PE routers are not completely isolated, since the global one contains part of VPN routes.

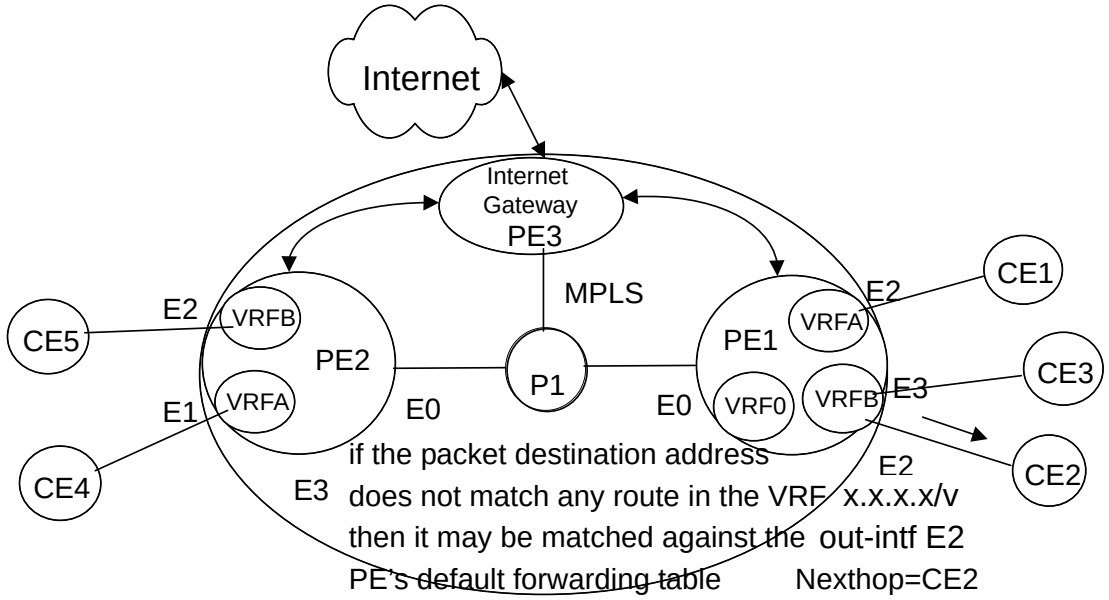

Fig 4-2 VRF Internet Access Mode 1

4.1.3 VRF Internet Access Mode 2

In VRF Internet Access Mode 2, VPN sites access the internet via the private public connections between PE and CE. The VRF route table of PE contains non-VPN routes. If the PE router conatins a non-VPN default route, according to which, the IP pakcets accessing Internet received by its VRF interface will be forwarded to the next-hop, where the packets will be forwarded after matching more accurate routes. Im applications, this non-VPN route may be like ip route vrf vrf-name 0.0.0.0/0 nexthop global, the global keyword means the next-hop of this route will be analysed according to the global route table. The packets from VPN to Internet will match the non-VPN default route in the VRF route table. After looking up for the next-hop in the global route table with the next-hop address of the default non-VPN route being the destiantion address, the packets will be fworared according to the found result. To enable the Internet accessing VPN sites, the process needed is similar to that in VRF Internet Access Mode 1, that is, ceating a static route pointing to VPN sites and advertise it to the Internet. Currently, this mode is not supported.

4.1.4 VRF Internet Access Mode 3

In VRF Internet Access Mode 3, as demonstrated in the next figure, VPN site access the Internet via private network connections between PE and CE. The VRF route tabl eof

PE routers contain Internet routes, which are learnt via the PE routers conencted with the Internet gateway (Internet PE). Internet PE will create an Internet VRF, and connect withe Internet gateway withe the interface bound with the Internet VRF. Thus , the Internet gateway will be able to advertise Inernet routes to the VRF route table of the Internet PE. There routes then will be advertised to VRF of other PE routers as VPNv4 routes. PE routers connected with the VPN sites needing to access the internet will advertise correspondng VRF routes (only those routes whose destiatnion segments are globally registered IP addess sub-net in the VPN) to Internet PE via VPNv4 route. These routes will be added into the Internet VRF and then advertised to Internet by the Internet gateway. The import and export policy of these routes depend on the route-target configuration of MBGP and vrf. Please notice that, in this mode, no overlap of address or route is allowed between the VPN sites capable of accessing the Internet.

It is not recommended for users to access the public network in this mode, for a large number of Internet routes will be imported to PE.

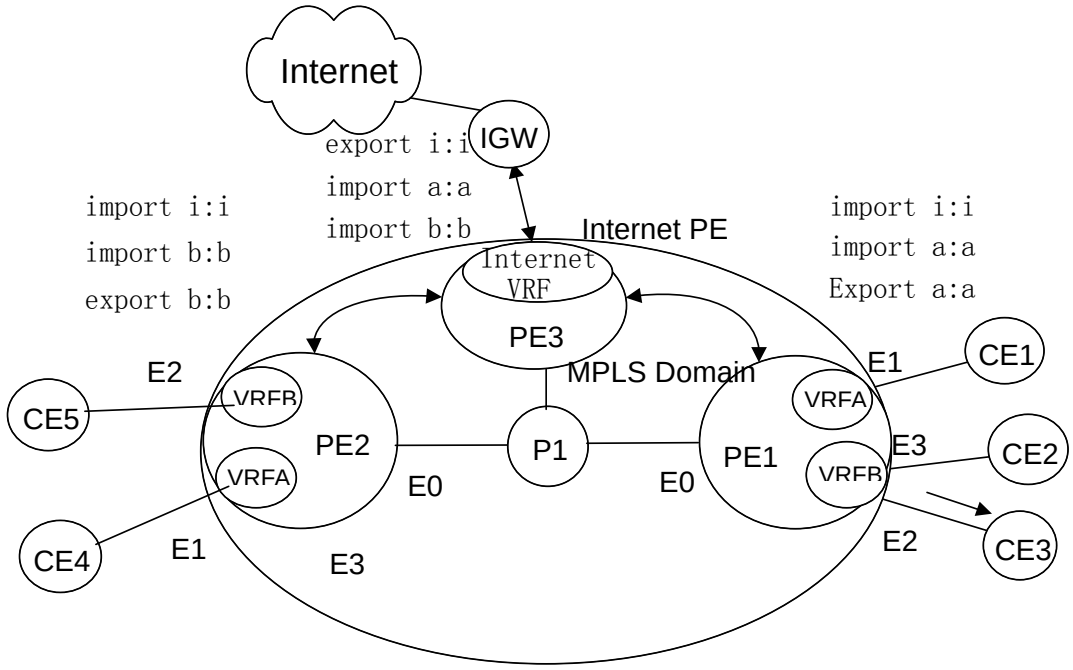

Fig 4-3 VRF Internet Access Mode 3

4.2 Public Network Access Configuration

Public Network Access Configuration Task Sequence:

1. Configure non-VRP Internet access mode
   (1) Configure regular L3VPN
   (2) Add a public connection between CE and PE, the connection interface is a non-VRF one.
   (3) Filter routes on CE; advertise public network routes to PE via the public network

connection.

(4) Configure proper filter policy on the public network interface, to filter the packets whose source and destination addresses are private network addresses.

(5) Configure default routes

1) IGW import the default routes to BGP

2) PE advertise the default routes to CE via the public network connection

3) CE advertise the default routes to PE via the private network connection, and then to other CE.

(6) Configure the static route

1) Configure the static route pointing to Internet on CE1

2) Configure the static route pointing to the public network interface of CE on PE1

2. Configure VRP Internet access mode 1

(1) Configure regular L3VPN

(2) Configure ip vrf forwarding VPNA fallback global on the private network interface of PE

(3) Configure 3 static routes:

1) Configure a default route on CE, whose next-hop is the proxy server

2) Add a default route to Internet on PE, whose next-hop is IGW. PE advertises a default route via OSPF, whose next-hop is the PE itself.

3) Add a static route form Internet to proxy server to the global route table of PE, whose destination is VPN public network address, next-hop is proxy server; and advertise this route to other PE via OSPF

Configure non-VRF Internet Access Mode

This configuration concerns no extra command line other than the configuration sequence. Please refer to the configuration instruction of the corresponding function for details about commands

Configure VRP Internet access mode 1

1. Configure VRP Internet access mode 1

(1) Configure regular L3VPN

(2) Configure ip vrf forwarding VPNA fallback global on the private network interface of PE

(3) Configure 3 static routes

1) Configure a default route on CE, whose next-hop is the proxy server

2) Add a default route to Internet on PE, whose next-hop is IGW. PE advertises a default route via OSPF, whose next-hop is the PE itself.

3) Add a static route form Internet to proxy server to the global route table of PE, whose destination is VPN public network address, next-hop is proxy server; and advertise this route to other PE via OSPF

Command	Explanation
Configure regular L3VPN	Refer to the BGP MPLS VPN configuration

Interface Configuration Mode	
[no] ip vrf forwarding <*vrf_name*> fallback global	Necessary Configure the global second lookup function of VRF route table. It is not configured by default. Before this configuration, cancel the VRF configuration in the interface view.
Global Configuration Mode	
[no] ip route vrf <*vrf-name*> {<ip-prefix> <mask>|<ip-prefix/<prefix-length>} {<gateway-address>|null0}	Necessary Configure static routes, Only three are needed: one is the default route of CE1, another is the default route to Internet on PE3 and the other is the static route form Internet to the proxy server on PE1

4.3 Public Network Access Typical Instances

4.3.1 Non-VRF Internet Access Mode

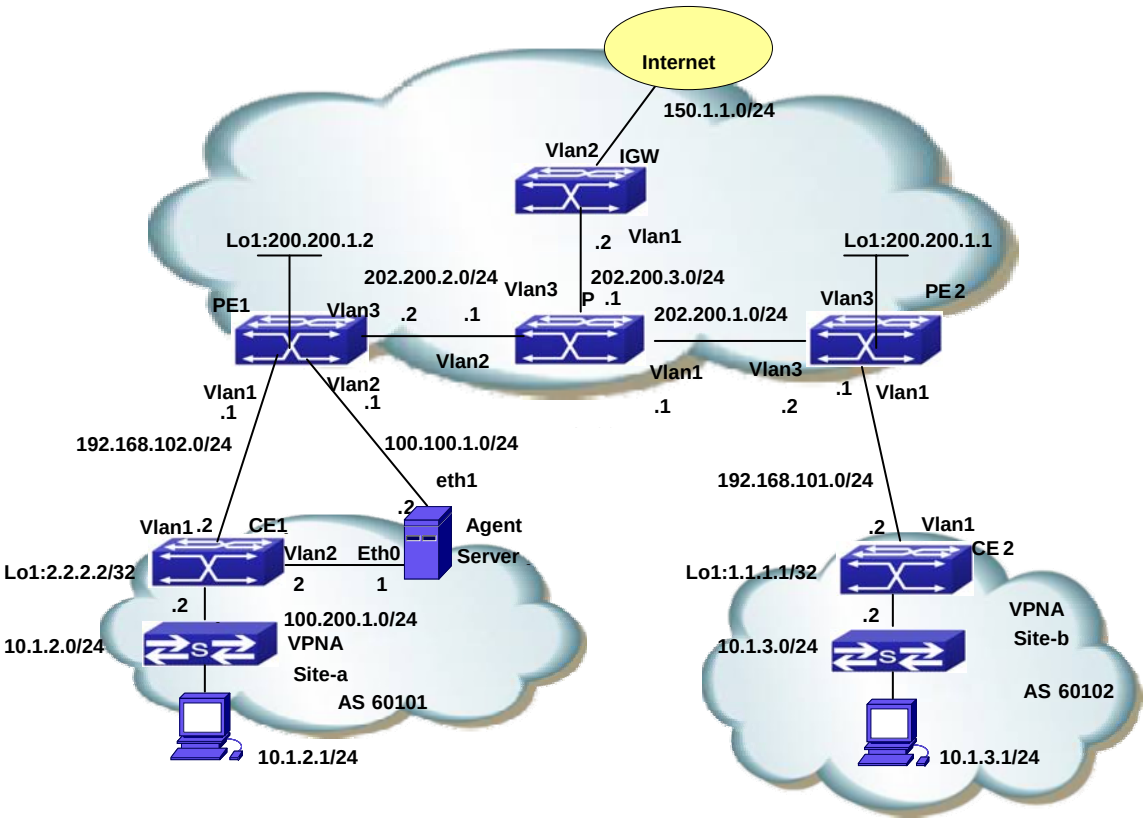

Fig 4-4 Non-VRF Internet Access Mode

The configuration of CE1 is as follows:

```
CE1#config
CE1(config)#access-list 1 deny 100.100.1.0 0.0.0.255
CE1(config)#access-list 1 deny 100.200.1.0 0.0.0.255
CE1(config)#access-list 1 permit any-source
CE1(config)#access-list 2 permit 120.1.1.0 0.0.0.255
CE1(config)#access-list 2 permit 120.1.2.0 0.0.0.255
CE1(config)#access-list 2 deny any-source
CE1(config)# interface vlan 1
CE1(config-if-Vlan1)#ip address 192.168.102.2 255.255.255.0
CE1(config-if-Vlan1)#exit
CE1(config)# interface vlan 2
CE1(config-if-Vlan1)#ip address 100.200.1.2 255.255.255.0
CE1(config-if-Vlan1)#exit
CE1(config)# interface vlan 3
CE1(config-if-Vlan1)#ip address 10.1.2.2 255.255.255.0
CE1(config-if-Vlan1)#exit
CE1(config)# interface loopback 1
CE1(config-if-Vlan1)#ip address 2.2.2.2 255.255.255.255
CE1(config-if-Vlan1)# exit
CE1(config)#router bgp 60102
CE1(config-router)#network 120.1.1.0/24
CE1(config-router)#network 120.1.2.0/24
CE1(config-router)#network 10.1.2.0/24
CE1(config-router)#redistribute connected
CE1(config-router)#neighbor 100.100.1.1 remote-as 100
CE1(config-router)#neighbor 100.100.1.1 ebgp-multihop
CE1(config-router)#neighbor 100.100.1.1 distribute-list 2 out
CE1(config-router)#neighbor 192.168.102.1 remote-as 100
CE1(config-router)#neighbor 192.168.102.1 default-originate
CE1(config-router)#neighbor 192.168.102.1 distribute-list 1 out
CE1(config-router)#exit
CE1(config)# ip route 100.100.1.1 255.255.255.0 100.200.1.1
CE1(config)# ip route 0.0.0.0 255.255.255.0 100.200.1.1
CE1(config)# exit
```

The configuration of PE1 is as follows:

```
PE1#config
PE1(config)#access-list 100 deny ip 10.1.2.0 0.0.0.255 any-destination
```

```
PE1(config)#access-list 100 deny ip 10.1.2.0 0.0.0.255 any-destination
PE1(config)#access-list 100 deny ip 10.1.3.0 0.0.0.255 any-destination
PE1(config)#access-list 100 deny ip anysource 200.200.1.0 0.0.0.255
PE1(config)#access-list 100 deny ip anysource 202.200.0.0 0.0.255.255
PE1(config)#firewall enable
PE1(config-vrf)#ip vrf VRF-A
PE1(config-vrf)#rd 100:10
PE1(config-vrf)#route-target both 100:10
PE1(config-vrf)#exit
PE1(config)#interface vlan1
PE1(config-if-Vlan1)#ip vrf forwarding VRF-A
PE1(config-if-Vlan1)#ip address 192.168.102.1 255.255.255.0
PE1(config-if-Vlan1)#exit
PE1(config)#interface vlan2
PE1(config-if-Vlan2)#ip address 100.100.1.1 255.255.255.0
PE1(config-if-Vlan2)#ip access-group 1 in
PE1(config-if-Vlan2)#exit
PE1(config)# interface vlan3
PE1(config-if-Vlan3)#label-switching
PE1(config-if-Vlan3)#enable-ldp
PE1(config-if-Vlan3)#ip address 202.200.2.2 255.255.255.0
PE1(config-if-Vlan3)#exit
PE1(config)#interface Loopback1
PE1(config)#ip address 200.200.1.2 255.255.255.255
PE1(config)#router ospf
PE1(config-router)#network 200.200.1.2/32 area 0
PE1(config-router)#network 202.200.2.0/24 area 0
PE1(config-router)#exit
PE1(config)#router bgp 100
PE1(config-router)#neighbor 100.200.1.2 remote-as 60102
PE1(config-router)#neighbor 100.200.1.2 ebgp-multihop
PE1(config-router)#neighbor 200.200.1.1 remote-as 100
PE1(config-router)#neighbor 202.200.3.2 remote-as 100
PE1(config-router)#neighbor 202.200.3.2 next-hop-self
PE1(config-router)#address-family vpnv4 unicast
PE1(config-router-af)#neighbor 200.200.1.1 activate
PE1(config-router-af)#exit-address-family
PE1(config-router)#address-family ipv4 vrf VRF-A
```

PE1(config-router-af)#neighbor 192.168.102.2 remote-as 60102

PE1(config-router-af)#no neighbor 192.168.102.2 send-community extended

PE1(config-router-af)#exit-address-family

PE1(config-router)#exit

PE1(config)# router ldp

PE1(config-router)#ip route 100.200.1.2 255.255.255.0 100.100.1.2

The configuration of P is as follows:

P#config

P(config)#interface Vlan1

P(config-if-Vlan1)#label-switching

P(config-if-Vlan1)#ldp enable

P(config-if-Vlan1)#ip address 202.200.1.1 255.255.255.0

P(config-if-Vlan1)#exit

P(config)#interface Vlan2

P(config-if-Vlan2)#label-switching

P(config-if-Vlan2)#enable-ldp

P(config-if-Vlan2)#ip address 202.200.2.1 255.255.255.0

P(config-if-Vlan2)#exit

P(config)#interface Vlan3

P(config-if-Vlan3)#ip address 202.200.3.1 255.255.255.0

P(config-if-Vlan3)#exit

P(config)#router ospf

P(config-router)#network 202.200.1.0/24 area 0

P(config-router)#network 202.200.2.0/24 area 0

P(config-router)#network 202.200.3.0/24 area 0

P(config-router)#exit

P(config)#router ldp

The configuration of PE2 is as follows:

PE2#config

PE2(config)#ip vrf VRF-A

PE2(config-vrf)#rd 100:10

PE2(config-vrf)#route-target both 100:10

PE2(config-vrf)#exit

PE2(config)#interface Vlan1

PE2(config-if-Vlan1)#ip vrf forwarding VRF-A

PE2(config-if-Vlan1)#ip address 192.168.101.1 255.255.255.0

PE2(config-if-Vlan1)#exit

PE2(config)#interface Vlan2

PE2(config-if-Vlan2)#label-switching

PE2(config-if-Vlan2)#enable-ldp

PE2(config-if-Vlan2)#ip address 202.200.1.2 255.255.255.0

PE2(config-if-Vlan2)#exit

PE2(config)#interface Loopback1

PE2(config-if-loopback1)#ip address 200.200.1.1 255.255.255.255

PE2(config-if-loopback1)#exit

PE2(config)#router ospf

PE2(config-router)#network 200.200.1.1/32 area 0

PE2(config-router)#network 202.200.1.0/24 area 0

PE2(config-router)#exit

PE2(config)#router bgp 100

PE2(config-router)#address-family vpnv4 unicast

PE2(config-router-af)#neighbor 200.200.1.1 activate

PE2(config-router-af)#exit-address-family

PE2(config-router)#address-family ipv4 vrf VRF-A

PE2(config-router-af)#neighbor 192.168.101.2 remote-as 60101

PE2(config-router-af)#no neighbor 192.168.101.2 send-community extended

PE2(config-router-af)#exit-address-family

PE2(config-router)#exit

PE2(config)#router ldp

The configuration of CE2 is as follows:

CE2#config

CE2(config)#interface vlan 1

CE2(config-if-Vlan1)#ip address 192.168.101.2 255.255.255.0

CE2(config-if-Vlan1)#exit

CE2(config)#interface Loopback1

CE2(config-if-Loopback1)#ip address 1.1.1.1 255.255.255.255

CE2(config-if-Loopback1)#exit

CE2(config)#router bgp 60101

CE2(config-router)#network 10.1.3.0/24

CE2(config-router)#neighbor 192.168.101.1 remote-as 100

The configuration of IGW is as follows:

IGW#config

IGW(config)#interface Vlan1

IGW(config-if-Vlan1)#ip address 202.200.3.2 255.255.255.0

IGW(config-if-Vlan1)#exit

IGW(config)#interface Vlan2

IGW(config-if-Vlan2#ip address 150.1.1.1 255.255.255.0

IGW(config-if-Vlan2#exit

IGW(config)#router ospf

IGW(config-router)#network 202.200.3.0 0.0.0.255 area 0

IGW(config-router)#exit

IGW(config)#router bgp 100

IGW(config-router)#neighbor 202.200.2.2 remote-as 100

IGW(config-router)#neighbor 202.200.2.2 default-originate

4.3.2 VRF Internet Access Mode 1

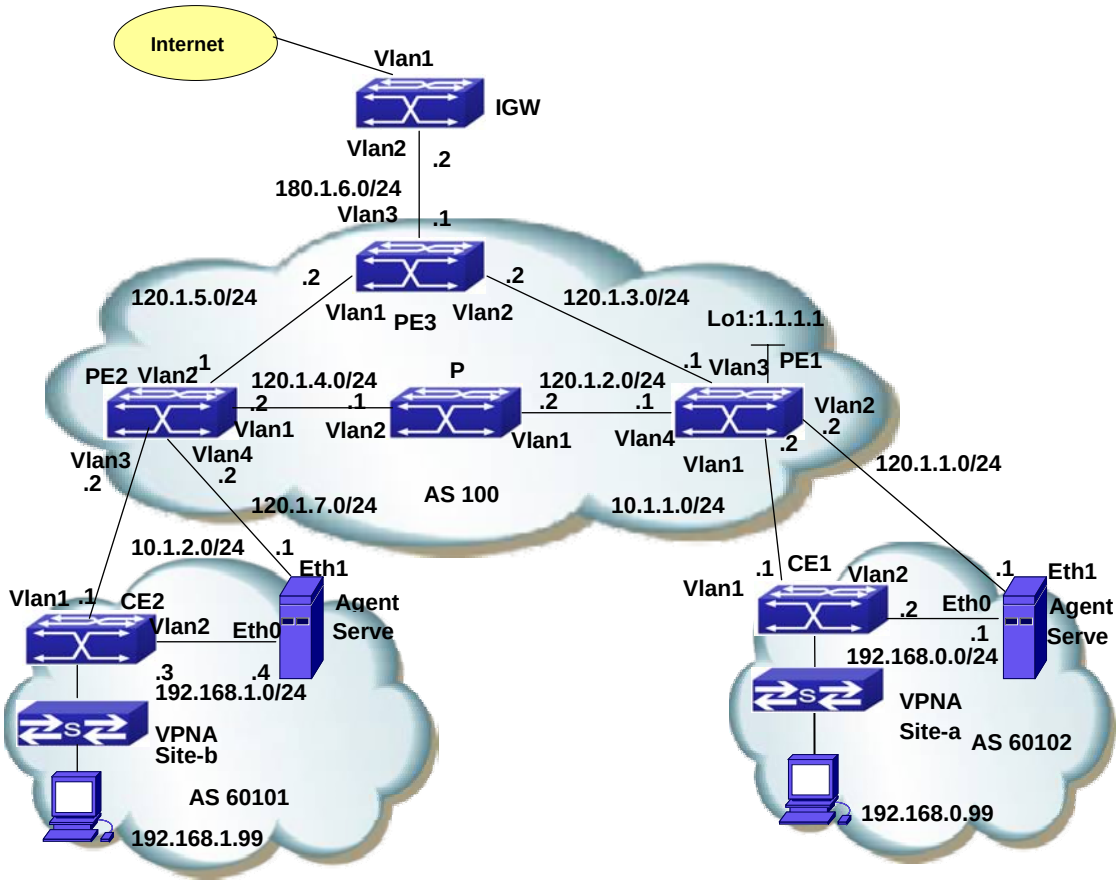

Fig 4-5 VRF Internet Access Mode 1

Site-a and site-b belong to VPNA; their users can intercommunicate and all need to access the Internet. Configure proxy servers separately in site-a and site-b to realize NAT when their users access Internet with the private network addresses.

The configuration of CE1 is as follows:

CE1#config

CE1(config)#interface Vlan1

CE1(config-if-Vlan1)#ip address 10.1.1.1 255.255.255.0

CE1(config-if-Vlan1)#exit

CE1(config)#interface Vlan2

CE1(config-if-Vlan2)#ip address 192.168.0.2 255.255.255.0

CE1(config-if-Vlan2)#exit

CE1(config)#interface loopback1

CE1(config-if-Loopback1)#ip address 11.11.11.11 255.255.255.255

CE1(config-if-Loopback1)#exit

CE1(config)#ip route 0.0.0.0 0.0.0.0 192.168.0.1

CE1(config)#router bgp 60101

CE1(config-router)#neighbor 10.1.1.2 remote-as 100

CE1(config-router)#network 192.168.0.0/24

The configuration of PE1 is as follows:

PE1#config

PE1(config)#ip vrf VPNA

PE1(config-vrf)#rd 100:10

PE1(config-vrf)#route-target both 100:10

PE1(config-vrf)#exit

PE1(config)#interface Vlan1

PE1(config-if-Vlan1)#ip vrf forwarding VPNA

PE1(config-if-Vlan1)#ip address 10.1.1.1 255.255.255.0

PE1(config-if-Vlan1)#exit

PE1(config)#interface Vlan2

PE1(config-if-Vlan2)#ip vrf forwarding VPNA fallback global

PE1(config-if-Vlan2)#ip address 120.1.1.2 255.255.255.0

PE1(config-if-Vlan2)#exit

PE1(config)#interface Vlan3

PE1(config-if-Vlan3)#ip address 120.1.3.1 255.255.255.0

PE1(config-if-Vlan2)#exit

PE1(config)#interface Vlan4

PE1(config-if-Vlan4)#label-switching

PE1(config-if-Vlan4)#ldp enable

PE1(config-if-Vlan4)#ip address 202.200.1.2 255.255.255.0

PE1(config-if-Vlan4)#exit

PE1(config)#interface loopback1

PE1(config-if-Loopback1)#ip address 1.1.1.1 255.255.255.255

PE1(config-if-Loopback1)#exit

PE1(config)#router ospf

PE1(config-router)#redistribute static

PE1(config-router)#network 1.1.1.1/32 area 0

PE1(config-router)#network 120.1.2.0/24 area 0

PE1(config-router)#network 120.1.3.0/24 area 0

PE1(config-router)#exit

PE1(config)#router bgp 100

PE1(config-router)#neighbor 2.2.2.2 remote-as 100

PE1(config-router)#neighbor 2.2.2.2 update-source 1.1.1.1

PE1(config-router)#address-family vpnv4 unicast

PE1(config-router-af)#neighbor 2.2.2.2 activate

PE1(config-router-af)#exit-address-family

PE1(config-router)#address-family ipv4 vrf VPNA

PE1(config-router-af)#network 120.1.1.0/24

PE1(config-router-af)#neighbor 10.1.1.1 remote-as 60101

PE1(config-router-af)#no neighbor 10.1.1.1 send-community extended

PE1(config-router-af)#exit-address-family

PE1(config-router)#exit

PE1(config)#router ldp

PE1(config-router)#exit

PE1(config)#ip route 120.1.1.0/24 vlan 2 120.1.1.1

The configuration of P is as follows:

P#config

P(config)#interface Vlan1

P(config-if-Vlan1)#label-switching

P(config-if-Vlan1)#ldp enable

P(config-if-Vlan1)#ip address 120.1.2.2 255.255.255.0

P(config-if-Vlan1)#exit

P(config)#interface Vlan2

P(config-if-Vlan2)#label-switching

P(config-if-Vlan2)#ldp enable

P(config-if-Vlan2)#ip address 120.1.4.1 255.255.255.0

P(config-if-Vlan2)#exit

P(config)#router ospf

P(config-router)#network 0.0.0.0/0 area 0

P(config-router)#exit

P(config)#router ldp

The configuration of PE2 is as follows:

PE2#config

```
PE2(config)#ip vrf VPNA
PE2(config-vrf)#rd 100:10
PE2(config-vrf)#route-target both 100:10
PE2(config-vrf)#exit
PE2(config)#interface Vlan1
PE2(config-if-Vlan1)#label-switching
PE2(config-if-Vlan1)#ldp enable
PE2(config-if-Vlan1)#ip address 120.1.4.2 255.255.255.0
PE2(config-if-Vlan1)#exit
PE2(config)#interface Vlan2
PE2(config-if-Vlan2)#ip address 120.1.5.1 255.255.255.0
PE2(config-if-Vlan2)#exit
PE2(config)#interface Vlan3
PE2(config-if-Vlan3)#ip vrf forwarding VPNA
PE2(config-if-Vlan1)#ip address 10.1.2.2 255.255.255.0
PE2(config-if-Vlan1)#exit
PE2(config)#interface Vlan4
PE2(config-if-Vlan4)#ip vrf forwarding VPNA fallback global
PE2(config-if-Vlan4)#ip address 120.1.7.2 255.255.255.0
PE2(config-if-Vlan4)#exit
PE2(config)#interface Loopback1
PE2(config-if-Loopback1)#ip address 2.2.2.2 255.255.255.255
PE2(config-if-Loopback)#exit
PE2(config)#router ospf
PE2(config-router)#redistribute static
PE2(config-router)#network 2.2.2.2/32 area 0
PE2(config-router)#network 120.1.4.0/24 area 0
PE2(config-router)#network 120.1.5.0/24 area 0
PE2(config-router)#exit
PE2(config)#router bgp 100
PE2(config-router)#neighbor 1.1.1.1 remote-as 100
PE2(config-router)#neighbor 1.1.1.1 update-source 2.2.2.2
PE2(config-router)#address-family vpnv4 unicast
PE2(config-router-af)#neighbor 1.1.1.1 activate
PE2(config-router-af)#exit-address-family
PE2(config-router)#address-family ipv4 vrf VPNA
PE2(config-router-af)#network 120.1.7.0/24
PE2(config-router-af)#neighbor 10.1.2.1 remote-as 60102
```

PE2(config-router-af)#no neighbor 10.2.1.1 send-community extended

PE2(config-router-af)#exit-address-family

PE2(config-router)#exit

PE2(config)#router ldp

PE2(config-router)#exit

PE2(config)#ip route 120.1.7.0/24 vlan 4 120.1.7.1

The configuration of PE3 is as follows:

PE3#config

PE3(config)#interface Loopback1

PE3(config-if-Loopback1)#ip address 3.3.3.3 255.255.255.255

PE3(config-if-Loopback1)#exit

PE3(config-if-Vlan1)#interface Vlan1

PE3(config-if-Vlan1)#ip address 120.1.5.2 255.255.255.0

PE3(config-if-Vlan1)#exit

PE3(config)#interface Vlan2

PE3(config-if-Vlan2)#ip address 120.1.3.2 255.255.255.0

PE3(config-if-Vlan2)#exit

PE3(config)#interface Vlan3

PE3(config-if-Vlan3)#ip address 180.1.6.1 255.255.255.0

PE3(config-if-Vlan3)#exit

PE3(config)#router ospf 1

PE3(config-router)#default-information originate

PE3(config-router)# network 0.0.0.0 255.255.255.255 area 0

PE3(config-router)#exit

PE3(config)#router bgp 100

PE3(config-router)#network 120.1.1.0 mask 255.255.255.0

PE3(config-router)#network 120.1.7.0 mask 255.255.255.0

PE3(config-router)#neighbor 180.1.6.2 remote-as 200

PE3(config-router)#exit

PE3(config)#ip route 0.0.0.0/0 180.1.6.2

The configuration of CE2 is as follows:

CE2#config

CE2(config)#interface Vlan1

CE2(config-if-Vlan1)#ip address 10.1.2.1 255.255.255.0

CE2(config-if-Vlan1)#exit

CE2(config)#interface Vlan2

CE2(config-if-Vlan2)#ip address 192.168.1.3 255.255.255.0

CE2(config-if-Vlan2)#exit

CE2(config-if-Loopback1)#interface Loopback1

CE2(config-if- Loopback1)#ip address 22.22.22.22 255.255.255.255

CE2(config-if- Loopback1)#exit

CE2(config)#ip route 0.0.0.0 0.0.0.0 192.168.1.4

CE2(config)#router bgp 60101

CE2(config-router)#neighbor 10.1.2.2 remote-as 100

CE2(config-router)#network 192.168.1.0/24

CE2(config-router)#exit

The configuration of IGW is as follows:

IGW#config

IGW(config)#interface Vlan1

IGW(config-if-Vlan1)#ip address 180.1.5.2 255.255.255.0

IGW(config-if-Vlan1)#exit

IGW(config)#interface Vlan2

IGW(config-if-Vlan2)#ip address 180.1.6.2 255.255.255.0

IGW(config-if-Vlan2)#exit

IGW(config)#router bgp 200

IGW(config-router)#neighbor 180.1.6.1 remote-as 100

IGW(config-router)#exit

4.4 Public Network Access Troubleshooting

When configuring and using Public Network Access, some problems like incorrect physical connections, configuration errors may cause it to fail, so please pay attention to the following notices to avoid them:

- First, make sure the regular MPLS BGP VPN works correctly, and the intercommunication is normal in the private network. If the communication in VPN fails, please refer to the help on MPLS BGP VPN troubleshooting.
- Second, check the public network access mode in use is non-VRF or VRF, for their configurations differ a lot.
- In non-VRF mode, please remember to configure filter policy on the non-VRF interface of PE-CE, to block the private network route and traffic from entering PE through the public network interface. Otherwise, there might be security threats. Besides, make sure the advertisement of default routes and the NAT configuration to IGW are correct.
- In VRF mode, please make sure to use “ip vrf forwarding vrf_name fallback global” command while configuring the private network interface, to prevent look up the global route table for a second time if the attempt to find the private

network route fails. Besides, make sure the advertisement of default routes and the NAT configuration to IGW are correct.

- ☞ At last, if all above steps are correct, CE will be able to access Internet. No matter which networking mode mentioned above is used, other CE access Internet after forwarding traffic to PE via VPN; the traffic from Internet should also be forwarded after passing PE,