Nortel Secure Router 8000 Series

Troubleshooting - VPN

Release: 5.3
Document Revision: 01.01

www.nortel.com

NN46240-710 324768-A Rev01

Nortel Secure Router 8000 Series
Release: 5.3
Publication: NN46240-710
Document Revision: 01.01
Document status: Standard
Document release date: 30 March 2009

Printed in Canada, India, and the United States of America

LEGAL NOTICE

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

ATTENTION
For information about the safety precautions, read "Safety messages" in this guide.

For information about the software license, read "Software license" in this guide.

Contents

Figures

Tables

Contents

About this document

Overview

This part describes the organization of this document, product version, intended audience, conventions, and update history.

Related versions

The following table lists the product versions to which this document relates.

Product name	Version
Nortel Secure Router 8000 Series	V200R005

Intended audience

The intended audiences of this document are:

- Network operators
- Network administrators
- Network maintenance engineers

Organization

The following table identifies the five chapters in this document.

Chapter	Description
1 L2TP troubleshooting	This chapter describes the basic knowledge about the Layer 2 VPN tunneling protocol (L2TP), troubleshooting procedures for L2TP faults, troubleshooting cases, diagnostic tools, and FAQs.

Chapter	Description
2 GRE troubleshooting	This chapter describes the basic knowledge about Generic Routing Encapsulation (GRE), troubleshooting procedures for GRE faults, troubleshooting cases, diagnostic tools, and FAQs.
3 BGP/MPLS IP VPN troubleshooting	This chapter describes the basic knowledge about MultiProtocol Label Switching/Border Gateway Protocol (MPLS/BGP) IP virtual private networks (VPN), troubleshooting procedures for BGP/MPLS IP VPN faults, troubleshooting cases, diagnostic tools, and FAQs.
4 MPLS Layer 2 VPN troubleshooting	This chapter describes the basic knowledge about MPLS Layer 2 VPN (L2VPN), troubleshooting procedures for MPLS L2VPN faults, troubleshooting cases, diagnostic tools, and FAQs.
5 VPLS troubleshooting	This chapter describes the basic knowledge about VPLS, troubleshooting procedures for VPLS faults, troubleshooting cases, diagnostic tools, and FAQs.

Conventions

Symbol conventions

The following table defines the symbols in this document.

Symbol	Description
⚠ DANGER	Indicates a hazard with a high level of risk that, if you do not avoid, results in death or serious injury.
⚠ WARNING	Indicates a hazard with a medium or low level of risk which, if you do not avoid, can result in minor or moderate injury.
⚠ CAUTION	Indicates a potentially hazardous situation that, if you do not avoid, can cause equipment damage, data loss, and performance degradation or unexpected results.
TIP	Indicates a tip that can help you solve a problem or save time.
NOTE	Provides additional information to emphasize or supplement important points of the main text.

General conventions

Convention	Description
Times New Roman	Normal paragraphs use Times New Roman.
Boldface	Names of files, directories, folders, and users use **boldface**. For example, log in as user **root**.
Italic	Book titles use *italics*.
`Courier New`	Terminal display uses `Courier New`.

Command conventions

Convention	Description
Boldface	The keywords of a command line use **boldface**.
Italic	Command arguments use *italics*.
[ ]	Items (keywords or arguments) in square brackets [ ] are optional.
{ x | y | ... }	Alternative items are grouped in braces and separated by vertical bars. Select one of the items.
[x | y | ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. Select one or none of the items.
{ x | y | ... } *	Alternative items are grouped in braces and separated by vertical bars. Select a minimum of one or a maximum of all of the items.
[x | y | ...] *	Optional alternative items are grouped in square brackets and separated by vertical bars. Select many or none of the items.
&<1-n>	You can repeat the parameter before the ampersand sign (&) 1 to n times.
#	A line that begins with the number sign (#) indicates comments.

GUI conventions

Convention	Description
Boldface	Buttons, menus, parameters, tabs, windows, and dialog titles use **boldface**. For example, click **OK**.

Convention	Description
>	Multilevel menus use **boldface** and a greater-than sign (>) separates the menu choices. For example, choose **File** > **Create** > **Folder**.

Keyboard operation

Format	Description
Key	Press the key. For example, press **Enter** and press **Tab.**
Key 1+Key 2	Press the keys concurrently. For example, press **Ctrl+Alt+A** means you press the three keys at the same time.
Key 1, **Key 2**	Press the keys in turn. For example, press **Alt**, **A** means you press the two keys one after the other.

Mouse operation

Action	Description
Click	Press and release the primary mouse button without moving the pointer.
Double-click	Quickly press the primary mouse button twice without moving the pointer.
Drag	Press and hold the primary mouse button and move the pointer to a specific position.

Update history

Updates between document versions are cumulative. The latest document version contains all updates made to previous versions.

Updates in Issue 1.0 (6 June 2008)

The first commercial release.

Contents

Figures

Tables

1 L2TP troubleshooting

About this chapter

The following table lists the contents of this chapter.

Section	Describes
1.1 L2TP overview	This section describes the concepts that you should know before troubleshooting Layer Two Tunneling Protocol (L2TP).
1.2 VPDN troubleshooting on the L2TP	This section contains the L2TP configuration notes, the troubleshooting flowchart, and the procedures for troubleshooting in the L2TP Virtual Private Data Network (VPDN) networking environment.
1.3 Troubleshooting L2TP access to the Layer 3 VPN	This section contains notes for configuring L2TP access to the L3 Virtual Private Network (VPN), the troubleshooting flowchart, and the detailed troubleshooting procedures.
1.4 Troubleshooting cases	This section presents troubleshooting cases.
1.5 FAQs	This section lists frequently asked questions (FAQ) and their answers.
1.6 Diagnostic tools	This section lists the diagnostic tools, including the **display** command and **debugging** command.

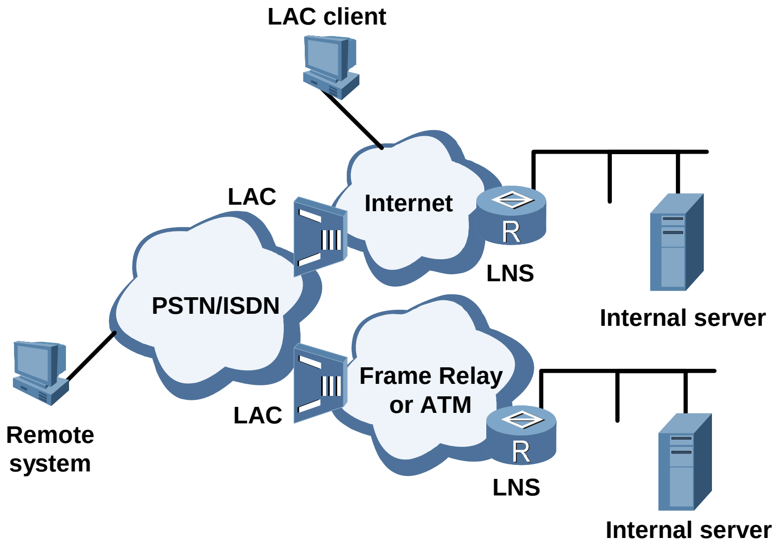
1.1 L2TP overview

L2TP is a VPDN tunnel protocol. This protocol supports transmission in a tunnel that is encapsulated by the PPP link and is applicable to remote access, such as remote user access to the internal source of the enterprise.

1.1.1 Two typical L2TP tunnel modes

The tunnel modes of PPP frames, which are between the user and L2TP Network Server (LNS), and between the user and L2TP Access Concentrator (LAC) clients (hosts running L2TP), are shown in Figure 1-1.

Figure 1-1 Typical L2TP tunnel modes



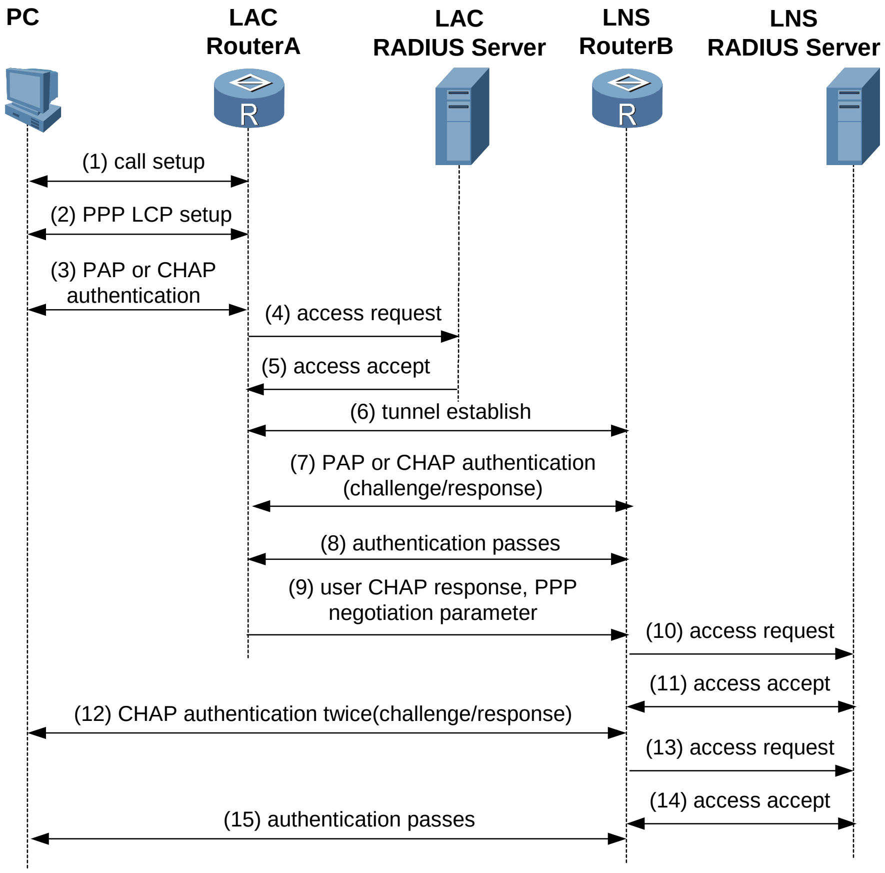
The methods of establishing a tunnel are as follows:

- NAS-initialized: Initiated by remote dial-up users. The remote system dials LAC through the Public Switched Telephone Network (PSTN) or Integrated Services Digital Network (ISDN). LAC sends a request to establish a tunnel connection to LNS through the Internet. The addresses of the dial-up users are assigned by LNS. The agent on LAC or LNS performs the authentication and accounting of remote dial-up users.
- Client-initialized: Initiated directly by LAC users who support L2TP. In this case, LAC users can directly send a request to establish a tunnel connection to LNS, without the need to pass through another LAC device. The addresses of the LAC users are assigned by LNS.

1.1.2 L2TP tunnel session setup

Figure 1-2 shows the process for setting up an L2TP tunnel.

Figure 1-2 The process flow for setting up an L2TP tunnel


PC
LAC RouterA
LAC RADIUS Server
LNS RouterB
LNS RADIUS Server
R
R
(1) call setup
(2) PPP LCP setup
(3) PAP or CHAP authentication
(4) access request
(5) access accept
(6) tunnel establish
(7) PAP or CHAP authentication (challenge/response)
(8) authentication passes
(9) user CHAP response, PPP negotiation parameter
(10) access request
(11) access accept
(12) CHAP authentication twice(challenge/response)
(13) access request
(14) access accept
(15) authentication passes

The procedure for setting up an L2TP tunnel is as follows:

1. The PC on the user side sends a connection request.
2. The PC and LAC device (Router A) negotiate the PPP LCP.
3. LAC carries out PAP or CHAP authentication based on the information from the PC.
4. LAC sends an access request with the VPN user name and password to the RADIUS server for identity authentication.
5. The RADIUS server authenticates this user and sends an access accept message, such as the LNS address. After the authentication succeeds, LAC is ready to start a new tunnel request.
6. LAC makes a tunnel request to the LNS specified by the RADIUS server.
7. LAC informs LNS of a CHAP challenge, and LNS sends a CHAP response and its CHAP challenge. LAC then sends back a CHAP response.
8. The authentication succeeds.
9. LAC transmits the information about the CHAP response, response identifier, and PPP negotiation parameters to LNS.

10. LNS sends an access request to the RADIUS server for authentication.
11. The RADIUS server reauthenticates this access request and sends back a response if authentication succeeds.
12. If local mandatory CHAP authentication is configured at LNS, LNS authenticates the VPN user by sending a challenge. The VPN user at the PC side sends back a response.
13. LNS resends this access request to the RADIUS server for authentication.
14. The RADIUS server reauthenticates this access request and sends back a response if authentication is successful.
15. After all authentications pass, the VPN user can use the internal resources of the enterprise.

1.2 VPDN troubleshooting on the L2TP

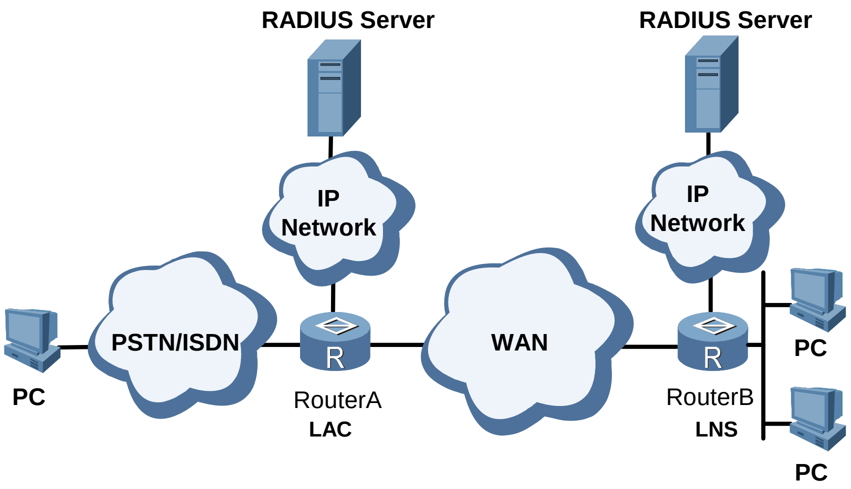
The section describes the following topics:

- Networking environment
- Configuration notes
- Diagnostic flowchart
- Troubleshooting procedure

1.2.1 Networking environment

Figure 1-3 shows the networking of the L2TP tunnel.

Figure 1-3 Networking of the L2TP tunnel



Router A works on the LAC side and Router B works on the LNS side. The user from the LAC side sends the request for connection to the LNS side. This achieves the interconnection with other PCs.

1.2.2 Configuration notes

Item	Sub-item	Description
Configuring AAA	Configure the authentication mode	To use the default local authentication, you need to configure the user name and the password in the AAA mode. To use any other authentication, such as RADIUS, you must configure the RADIUS authentication.
	Configure the domain and the authentication mode	You must configure the items for domain user access.
	Configure the address pool	Configure an address pool on the LNS side. You need to configure common users to access an address pool in the AAA mode and configure domain users to access an address pool in the domain mode.
	Configure the user name and password	The user names and passwords on the user side, the LAC side, and the LNS side must be consistent.
Configuring VT	Configure the PPP authentication	After the LCP renegotiation on the LNS side is executed, you need to configure the PPP authentication mode on the virtual interface template. Otherwise, the user cannot pass the authentication.
	Appointment of the address pool	To configure an address pool for a user, the number of address pool configured here must be the same as that configured in the AAA view.
	Configure the MTU	Nortel recommends that you configure the MTU value as 1450.
Configuring L2TP	Enable the L2TP	Configure the L2TP only after the L2TP is enabled.
	Source interface of the tunnel on the LAC side	You can specify the loopback interface, Ethernet interface, and GigabitEthernet interface as the source interface of the tunnel.
	The name of the tunnel	The name of the tunnel on the LAC side must be consistent with the name of the remote end to receive the tunnel on the LNS side.
	The authentication of the tunnel	The configuration for tunnel authentication on the LAC side must be the same as that on the LNS side.
	The password of the authentication of the tunnel	After tunnel authentication is enabled, the passwords on both the LAC side and the LNS side must be consistent.

Item	Sub-item	Description
	The list separator of the user postfix	If you establish the connection with L2TP through the domain, you need to run the **l2tp domain** command to configure the separator of the user postfix.
	The static route on the LAC side	When the LNS side uses the IP address of the loopback interface as the IP address of the L2TP group, you must configure the route to be reachable to the LNS loopback interface on the LAC side.
	The request for the connection with the L2TP allowed on the LNS side	If the number of the L2TP is 1, you need not specify the *remote-name*. If you specify the remote name in the L2TP group 1 view, L2TP group 1 does not work as the default L2TP group.
	The IP address of the L2TP group bound on the LNS side	The IP address of the Ethernet interface, GigabitEthernet interface, and loopback interface can be used as the IP address of an L2TP group. After the loopback interface is bound, it cannot be used for other services.
	The user authentication on the LNS side	After the LCP renegotiation is configured on the LNS side, you need to configure the PPP authentication mode on the correct virtual interface template. Otherwise, the user cannot pass the authentication.
Domain	—	Generally, bind VTs and configure address pools in the domain view when L2TP users access Layer 3 VPN groups. In other cases, bind VTs in the L2TP group view.

As an example for the configuration notes for the L2TP LNS, consider users in different domains that access the VPN.

1. Configure the interface of the LNS and LAC Ethernet2/0/0 and the address.

```
[Nortel] interface ethernet2/0/0
[Nortel-Ethernet2/0/0] ip address 10.1.1.3 255.255.255.0
[Nortel-Ethernet2/0/0] quit
```

2. Create a virtual template (VT) required by the L2TP group.

```
[Nortel] interface virtual-template 1
[Nortel-Virtual-Template1] ip address 35.1.1.1 255.255.255.0
[Nortel-Virtual-Template1] mtu 1450
[Nortel-Virtual-Template1] ppp authentication-mode pap
[Nortel-Virtual-Template1] quit
```

   The VT executes the LCP and PAP negotiation with the user.

3. Configure the loopback interface required by the L2TP group.

```
[Nortel] interface LoopBack 0
```

```
[Nortel-LoopBack0] ip address 100.1.1.1 255.255.255.255
[Nortel-LoopBack0] quit
```

As the terminal IP of the tunnel, the interface is responsible for decompressing the L2TP header and preparing for the next forwarding.

4. Configure the attributes on the L2TP group to be consistent with those on the LAC side.

   # Enable the L2TP.

   ```
   [Nortel] l2tp enable
   ```

   # Set the identifier of the domain to be the @ symbol.

   ```
   [Nortel] l2tp domain suffix-separator @
   ```

   # Create the L2TP group.

   ```
   [Nortel] l2tp-group 1
   ```

   # Configure the name of the local tunnel as LNS.

   ```
   [Nortel-l2tp1] tunnel name LNS
   ```

   # Specify the VT to negotiate with the user, and the remote name (you do not need to configure the remote name if the L2TP group number is 1).

   ```
   [Nortel-l2tp1] allow l2tp virtual-template 1 remote LAC
   ```

   # Configure the tunnel authentication to be consistent with the LAC.

   ```
   [Nortel-l2tp1] tunnel authentication
   ```

   # Configure the password of the tunnel to be the same as the LAC.

   ```
   [Nortel-l2tp1] tunnel password simple 12345
   ```

   # Configure the destination number of the tunnel to be loopback 0.

   ```
   [Nortel-l2tp1] tunnel destination loopback 0
   [Nortel-l2tp1] quit
   ```

5. Create a domain and bind the virtual template and the corresponding address pool in the domain.

   ```
   [Nortel] aaa
   [Nortel-aaa] domain nortel1.com
   [Nortel-aaa-domain-nortel1.com] ip pool 8 8.1.1.2 8.1.1.10
   [Nortel-aaa-domain-nortel1.com] quit
   [Nortel-aaa] domain nortel2.com
   [Nortel-aaa-domain-nortel2.com] ip pool 9 9.1.1.2 9.1.1.10
   [Nortel-aaa-domain-nortel2.com] quit
   ```

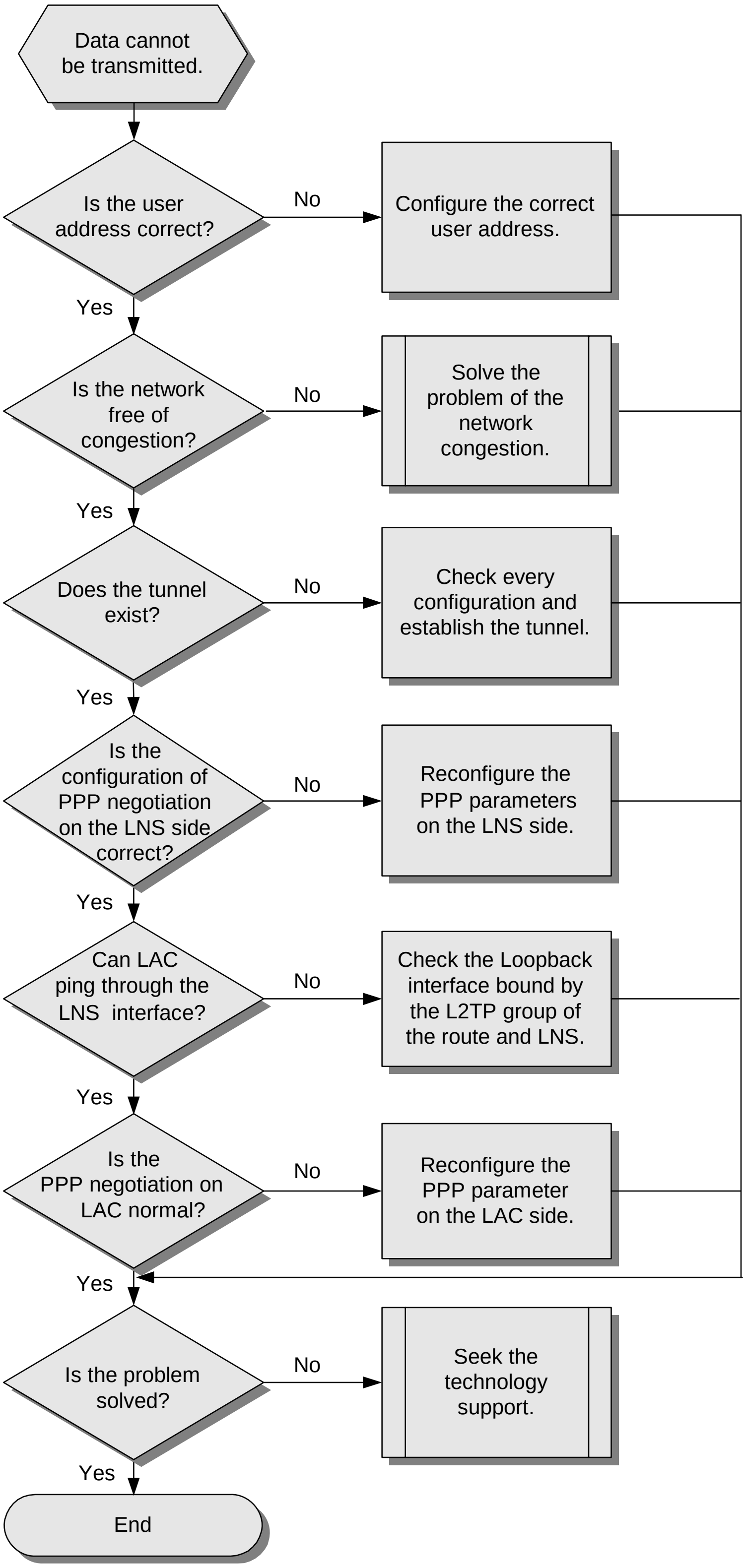
6. Create two user names and passwords.

   ```
   [Nortel-aaa] local-user vpdn@nortel1.com password simple 11111
   [Nortel-aaa] local-user vpdn@nortel2.com password simple 22222
   ```

1.2.3 Diagnostic flowchart

Figure 1-4 shows the flowchart for diagnosing faults on L2TP.

Figure 1-4 The flowchart for diagnosing faults on L2TP


Data cannot be transmitted.
Is the user address correct?
No
Configure the correct user address.
Yes
Is the network free of congestion?
No
Solve the problem of the network congestion.
Yes
Does the tunnel exist?
No
Check every configuration and establish the tunnel.
Yes
Is the configuration of PPP negotiation on the LNS side correct?
No
Reconfigure the PPP parameters on the LNS side.
Yes
Can LAC ping through the LNS interface?
No
Check the Loopback interface bound by the L2TP group of the route and LNS.
Yes
Is the PPP negotiation on LAC normal?
No
Reconfigure the PPP parameter on the LAC side.
Yes
Is the problem solved?
No
Seek the technology support.
Yes
End

1.2.4 Troubleshooting procedures

The troubleshooting procedures are as follows.

Step 1 Determining that the user address is correct

Step 2 Checking whether network congestion occurs

Step 3 Checking that the tunnel exists

Step 4 Checking the state of PPP negotiation on the LNS side

Step 5 Checking that the LAC can ping through the loopback interface of the LNS

Step 6 Checking the status of PPP negotiation on the LAC side

----End

The following sections describe the troubleshooting steps.

Determining that the user address is correct

The LNS can assign the address to the user, or the user can specify the address. If the assigned address and the specified address are not in the same network segment, the data transmission fails. Nortel recommends that the LNS assign the address. The two cases are as follows:

- When the user accesses LNS with the full name, LNS checks that the correct address pool is bound in the VT. You must configure the address pool in the AAA view correctly. Run the **remote address pool** *pool-number* command to bind the address pool.
- When the user accesses LNS with the domain name, LNS checks whether a correct address pool is configured in the domain view. You can use the **ip pool** *pool-number first-address* [*last-address*] command to configure the address pool in the domain view. Then, use the **remote address pool** *pool-number* command in the VT interface view to bind the address pool to this interface.

Checking whether network congestion occurs

L2TP transmits data based on the User Datagram Protocol (UDP). The UDP does not implement error control on the packets. If you apply L2TP when the link is unstable, the data transmission can fail.

Checking that the tunnel exists

You can use the **display l2tp tunnel** command to check whether the tunnel is established on the LAC and LNC. If no corresponding tunnel exists, check the configuration using the following methods:

1. Run the **display this** command in the L2TP group view on the LAC end to check whether the LNS address with the **start l2tp** command is correctly configured. The address should be the same as the loopback address on the LNS end. If they are different, you need to reconfigure the LNS address.
2. Run the **display this** command in the L2TP group view on the LAC side to check whether the LNS address is correct in the **allow l2tp** command. The address must be consistent with the IP address of the loopback interface on the LNS end. If they are inconsistent, you must reconfigure them.

3. Check whether the tunnel authentication and the password are correctly configured on the LAC and LNS ends. The request for the tunnel authentication can be initiated from either the LAC or the LNS. If one end starts the tunnel authentication, the tunnel can be established only when the remote end also starts the tunnel authentication and the passwords of both ends are consistent. Run the **display this** command in the L2TP group view on the LAC and LNS sides to check if the passwords of the tunnels are consistent. If one end is configured with the tunnel authentication but the passwords on both ends are inconsistent, use the **tunnel password** { **simple** | **cipher** } *password* command to configure the passwords.
4. Check whether the correct virtual template (VT) is bound on the LNS side.
5. If one end is forcibly disconnected, while the remote end does not receive the Disconnect packet, the tunnel between the two ends cannot be connected. This is because the remote end requires a period of time to test the disconnection of the link.
6. LNS does not accept the request for the connection of the tunnel from the LACs that have the same IP addresses. If the two LACs simultaneously send the request for the connection of the tunnel, the tunnel cannot be established.

Checking the state of PPP negotiation on the LNS side

1. Check that LCP renegotiation or forced CHAP authentication is configured.

   Run the **display this** command in the L2TP group view to check if LCP renegotiation or forced CHAP authentication is configured. When the device is connected with the LAC equipment of other companies, the user authentication on the LNS uses the LCP renegotiation. You can configure the LAC device according to actual requirements.

   After you configure LCP renegotiation on the LNS side, you must configure PPP authentication on the corresponding virtual interface template. Otherwise, the user cannot pass the authentication.

2. Check that the LNS configures the corresponding user name and the password.

   The two cases are as follows:

   - For local authentication, check whether the correct user name and password are configured in the AAA view. If they are incorrect, configure them by using the **local-user** *user-name* **password** { **simple** | **cipher** } *password* command.
   - For RADIUS authentication, see the section about VAS troubleshooting in *Nortel Secure Router 8000 Series Troubleshooting* - *VAS* (NN46240-709).
3. Use the **display ip pool** command to check whether the address pool is small or no address pool is configured.
4. Use the **display this** command in the VT view to check whether the authentication type is consistent with that of the LAC.

Checking that the LAC can ping through the loopback interface of the LNS

1. Ping the loopback interface from the LAC. If you can ping through the loopback interface, a reachable route between the LAC and LNS exists. If not, check whether the static route of the loopback interface on the LNS has been configured by the **display ip routing-table** command.
2. If a static route exists, you can use the **display this** command in the L2TP group view on the LNS side to check that the L2TP group binds the loopback interface. If no loopback interface is bound, use the **tunnel destination loopback** command to bind it.

Checking the status of PPP negotiation on the LAC side

The user needs to pass the PPP authentication on the LAC end before the L2TP tunnel and session are established. The methods are as follows:

1. If the LAC end uses local authentication, you can use the **local-user** *user-name* **password** { **simple** | **cipher** } *password* command in the AAA mode to check that the correct user name and password are configured on the LAC end.
2. If the LAC end uses RADIUS authentication, see the section about VAS troubleshooting in *Nortel Secure Router 8000 Series Troubleshooting - VAS* (NN46240-709).
3. If access with the full user name is used, you can use the **display local-user** command to check that the corresponding user is configured and the user matches with the name of the client. If not, modify the user name of either end. Use the **start l2tp ip** *ip-address* **fullusername** *user-name* command to modify the user name on the LAC end.
4. If access with the domain name is used, check that the postfix of the domain name matches the domain name of the end user, and check if the list separator of the domain name postfix corresponding with the end user is configured. If they do not match, modify the postfix of the domain name with the **start l2tp ip** *ip-address* **domain** *domain-name* command. If no list separator of the domain name postfix exists, use the **l2tp domain suffix-separator** command to configure it.
5. Check whether the PPP authentication mode configured on the user interface on the LAC end is consistent with that on the LNS side. The command for PPP authentication is **ppp authentication** { **pap** | **chap** }.
6. Check whether the authentication mode on the LAC end is consistent with that on the user end. If not, modify the authentication end on one end. For example, the default authentication mode of the VPN connection created by Windows 2000 is MSCHAP. If the LAC does not support MSCHAP, change the mode to CHAP.

If the preceding configurations are correct, the user can pass the authentication on the LAC end. If you still cannot resolve the L2TP faults, contact Nortel technical support.

1.3 Troubleshooting L2TP access to the Layer 3 VPN

The section describes the following topics:

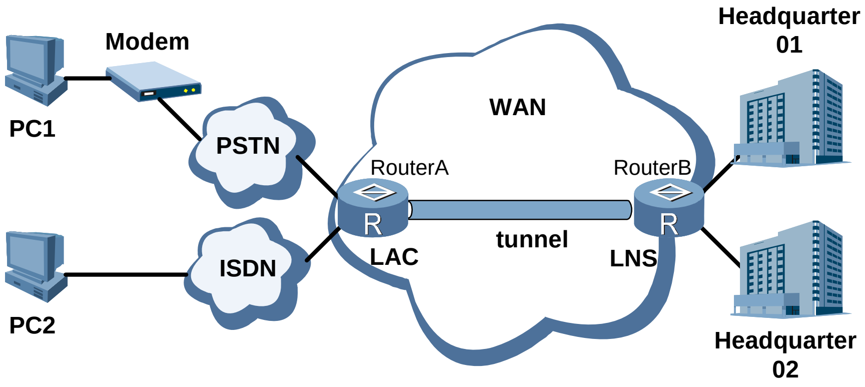
- Networking environment
- Configuration notes
- Diagnostic flowchart
- Troubleshooting procedure

1.3.1 Networking environment

If many enterprises use one LNS and users of an enterprise need to communicate with their own headquarters, but the network address is a private IP address, for example 10.8.0.0, the users cannot access the internal server of the enterprise through the Internet. To enable users to access the internal network of the enterprise, you can establish a VPN that supports multiple instances.

As shown in Figure 1-5, the domain name of headquarters of the 01 enterprise is 263.net and PC1 is the user of the enterprise. The domain name of headquarters of the 02 enterprise is 163.net and PC2 is the user of the enterprise.

Figure 1-5 Networking of the L2TP access to the Layer 3 VPN



1.3.2 Configuration notes

Item	Sub-item	Description
Configuring AAA	Configure the authentication mode	To use the default local authentication, you need to configure the user name and the password in the AAA mode. To use any other authentication, such as RADIUS, you must configure the RADIUS authentication.
	Configure the domain and the authentication mode	You must configure the items for domain user access.
	Configure the address pool	Configure an address pool on the LNS side. You need to configure common users to access an address pool in the AAA mode, and configure domain users to access an address pool in the domain mode.
	Configure the user name and password	The user names and passwords on the user side, the LAC side, and the LNS side must be consistent.
Configuring VT	Configure PPP authentication	After the LCP renegotiation on the LNS side is executed, you need to configure the PPP authentication mode on the virtual interface template. Otherwise, the user cannot pass the authentication.
	Assign the address pool	To configure an address pool for a user, the number of address pool configured here must be the same as that configured in the AAA view.
	Configure the MTU	Nortel recommends that you configure the MTU value to 1450.

Item	Sub-item	Description
	Bind the VPN	Bind the corresponding VPN in the VT view.
Configuring L2TP	Enable L2TP	L2TP can be configured only after L2TP is enabled.
	The source interface of the tunnel on the LAC side	You can specify the loopback interface, Ethernet interface, and GigabitEthernet interface as the source interface of the tunnel.
	The name of the tunnel	The name of the tunnel on the LAC side must be consistent with the name of the remote end to receive the tunnel on the LNS side.
	The authentication of the tunnel	The configuration for whether to enable tunnel authentication on the LAC side must be the same as that on the LNS side.
	The password of the authentication of the tunnel	After tunnel authentication is enabled, the passwords on both the LAC and LNS ends must be consistent.
	The list separator of the user postfix	If you establish the connection with the L2TP through the domain, you need to run the **l2tp domain** command to configure the separator of the user postfix.
	The static route on the LAC side	When the LNS side uses the IP address of the loopback interface as the IP address of the L2TP group, you must configure the route to be reachable to the LNS loopback interface on the LAC side.
	The request for the connection with the L2TP allowed on the LNS side	If the number of the L2TP group is 1, you need not specify the remote name. If you specify the remote name in the L2TP group 1 view, the L2TP group 1 does not work as the default L2TP group.
	The IP address of the L2TP group bound on the LNS side	You can use the IP address of the Ethernet interface, GigabitEthernet interface, and loopback interface as the IP address of an L2TP group. After the loopback interface is bound, it cannot be used for other services.
	The user authentication on the LNS side	After LCP renegotiation is configured on the LNS side, you need to configure the PPP authentication mode on the corresponding virtual interface template. Otherwise, the user cannot pass the authentication.

Item	Sub-item	Description
Domain	—	Generally, bind VTs and configure address pools in the domain view when L2TP users access Layer 3 VPN groups. In other cases, bind VTs in the L2TP group view.
VPN	Configure the VPN instances	Configure the VPN instances and then associate them to the VT.

The following section describes the configuration based on the preceding networking environment.

1. Configure the user side.

   Establish a dial-up network. The number is the access number of the Nortel1 router. The dial-up network receives the address assigned by the LNS server.

   In PC1, enter the user name vpdn@263.net in the dial-up terminal window with the password 11111. (The user name and the password must be registered in LNS.)

   In PC2, enter the user name vpdn@163.net in the dial-up terminal window with the password 22222. (The user name and the password must be registered in LNS.)

2. Configure the LAC side.

   # Configure the user authentication on the LAC side.

   # Configure the L2TP group and relative attributes.

   # Start the tunnel authentication and configure the password of the tunnel authentication.

   # Configure the separator of the domain name postfix.

   # Configure the user name, the password, and the access domain name to be the same as those on the client side.

3. Configure the LNS side.

   # Configure the interface Ethernet2/0/0 of the LNS and LAC interfaces and configure the address.

```
[Nortel] interface ethernet2/0/0
[Nortel-Ethernet2/0/0] ip address 10.1.1.3 255.255.255.0
[Nortel-Ethernet2/0/0] quit
```

   # Create a virtual template for the L2TP group.

```
[Nortel] interface virtual-template 1
[Nortel-Virtual-Template1] ip address 35.1.1.1 255.255.255.0
[Nortel-Virtual-Template1] mtu 1450
[Nortel-Virtual-Template1] ppp authentication-mode pap
[Nortel-Virtual-Template1] quit
```

   # Create a loopback interface for the L2TP group.

```
[Nortel] interface LoopBack 0
[Nortel-LoopBack0] ip address 100.1.1.1 255.255.255.255
[Nortel-LoopBack0] quit
```

   # Create an L2TP group and configure its attributes (consistent with that on the LAC side).

```
[Nortel] l2tp enable
[Nortel] l2tp domain suffix-separator @
[Nortel] l2tp-group 1
[Nortel-l2tp1] tunnel name LNS
[Nortel-l2tp1] allow l2tp virtual-template 1
[Nortel-l2tp1] tunnel authentication
[Nortel-l2tp1] tunnel password simple 12345
[Nortel-l2tp1] tunnel destination loopback 0
```

# When the Nortel LAC device is connected with the device of another company, the user authentication on the LNS side uses LCP renegotiation. You can configure the Nortel LAC device according to your actual requirements.

```
[Nortel-l2tp1] mandatory-lcp
[Nortel-l2tp1] quit
```

# Create two domains and configure the corresponding address pool in the domain.

```
[Nortel] aaa
[Nortel-aaa] domain 263.net
[Nortel-aaa-domain-263.net] binding virtual-template 8
[Nortel-aaa-domain-263.net] ip pool 8 8.1.1.2 8.1.1.10
[Nortel-aaa-domain-263.net] quit
[Nortel-aaa] domain 163.net
[Nortel-aaa-domain-163.net] binding virtual-template 9
[Nortel-aaa-domain-163.net] ip pool 9 9.1.1.2 9.1.1.10
[Nortel-aaa] quit
```

# Create two VPN instances.

```
[Nortel] ip vpn-instance vpn1
[Nortel–vpn-instance-vpn1] route-distinguisher 1:10
[Nortel–vpn-instance-vpn1] vpn-target 1:10 export-extcommunity
[Nortel–vpn-instance-vpn1] vpn-target 1:10 import-extcommunity
[Nortel–vpn-instance-vpn1] quit
[Nortel] ip vpn-instance vpn2
[Nortel–vpn-instance-vpn2] route-distinguisher 1:11
[Nortel–vpn-instance-vpn2] vpn-target 1:11 export-extcommunity
[Nortel–vpn-instance-vpn2] vpn-target 1:11 import-extcommunity
[Nortel-vpn-instance-vpn2] quit
```

# Create two corresponding virtual templates and bind them with VPN instances.

```
[Nortel] interface virtual-template 8
[Nortel-Virtual-Template8] ip binding vpn-instance vpn1
[Nortel-Virtual-Template8] ip address 8.1.1.1 255.255.255.0
[Nortel-Virtual-Template8] mtu 1450
[Nortel-Virtual-Template8] remote address pool 8
[Nortel-Virtual-Template8] ppp authentication-mode pap
[Nortel-Virtual-Template8] quit
[Nortel] interface virtual-template 9
[Nortel-Virtual-Template9] ip binding vpn-instance vpn2
[Nortel-Virtual-Template9] ip address 9.1.1.1 255.255.255.0
[Nortel-Virtual-Template9] mtu 1450
[Nortel-Virtual-Template9] remote address pool 9
[Nortel-Virtual-Template9] ppp authentication pap
[Nortel-Virtual-Template9] quit
```

# Create two user names and passwords.

```
[Nortel-aaa] local-user vpdn@263.net password simple 11111
[Nortel-aaa] local-user vpdn@163.net password simple 22222
```

In the preceding configuration, you need to modify the AAA configuration if the LNS end uses RADIUS authentication.

1.3.3 Diagnostic flowchart

The diagnostic flowchart is the same as the flowchart shown in Figure 1-4.

1.3.4 Troubleshooting procedure

The troubleshooting procedure is as follows:

Step 1 Check faults by using the steps in “VPDN troubleshooting on the L2TP.”

Step 2 Check that the correct VPN instances are bound on the VT on the LNS side.

Step 3 Check that the correct VT is bound in the AAA domain.

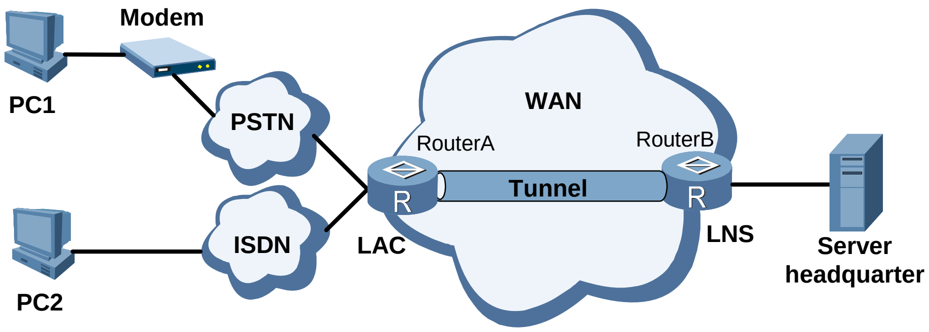
----End

1.4 Troubleshooting cases

1.4.1 The session disconnects as soon as it is set up

Networking environment

Figure 1-6 Networking of the disconnection of the L2TP session



Fault symptom

The sessions on both the LAC and LNS sides disconnect as soon as they are set up.

Fault analysis

The establishment of the session indicates that LAC and LNS are reachable. It also indicates that the request for the connection with the L2TP is initiated. Faults on the LNS may cause the disconnection of the session.

Enable debugging of the L2TP control on the LNS. By verifying the debugging information, you can determine whether the session is disconnected when the interface receives the Call Down message.

When you enable debugging of PPP on the LNS by using the **debugging ppp all** command, you can find abnormalities.

```
*0.2426289 Nortel PPP/8/debug2:Slot=1;
  PPP Event:
      Virtual-Template1:0 : Ask AAA peer's IP address
*0.2426417 Nortel PPP/8/debug2:Slot=1;
  PPP Event:
      Virtual-Template1:0 : WaitPeerIP Timer starting
*0.2426545 Nortel PPP/8/debug2:Slot=1;
  PPP Event:
      Virtual-Template1:0 : Receive Peer's IP address 0.0.0.0 from AAA
*0.2426705 Nortel PPP/8/debug2:Slot=1;
  PPP Event:
      Virtual-Template1:0 : WaitPeerIP Timer finished
*0.2426833 Nortel PPP/8/debug2:Slot=1;
```

The preceding information shows that the interface receives the IP address 0.0.0.0. To check the configuration, see the procedure in the section “VPDN troubleshooting on the L2TP.” You can find that the access user is the domain user and no configured address pool is in the domain. Although the VT is bound with the address pool, the domain user applies for the IP address from the address pool in the domain. So, when the application for the address and the IPCP negotiation of the PPP fail, the session is disconnected.

Troubleshooting procedure

Step 1 View the L2TP debugging information to determine that the interface receives the Call Down information.

Step 2 Viewing the PPP debugging information to determine that the interface does not apply for an IP address.

Step 3 Based on the configuration in the debugging information, you can find that no address pool is configured in the domain.

----End

Summary

The cause is a configuration error. To resolve the problem, you need to understand the differences between common user access and domain user access.

1.5 FAQs

- **Q: Why is the interface on the LAC side unable to ping through the loopback interface of the LNS?**

  A: A possible cause is that the LAC has no route to the loopback interface of the LNS.

- **Q: Why is the PPP negotiation between the user and the LAC unsuccessful?**

  A: A possible cause is that the authentication modes configured on the user and the LAC are different (one is PAP and the other is CHAP).

- **Q: Why is the PPP negotiation between the user and the LNS unsuccessful?**

  A: The possible causes are as follows.

  - The configured address pool on the LNS end is too small or no address pool is configured on the LNS end.
  - No corresponding user is configured on the LNS end.
  - The authentication of the tunnel between the LNS end and LAC does not pass.
  - The authentication of the VT and the user are different.
  - The IP address assigned by the LNS to the user conflicts with other addresses of the user.

- **Q: The data cannot be transmitted although the connection is established. Why does this occur?**

  A: The possible causes are as follows.

  - Either the Forward Information Base (FIB) entry of the loopback interface on the LNS has no decapsulation mark or the FIB entry of the user route on the LNS has no encapsulation mark.
  - Either network congestion or instability of the network quality occurs.
  - The user end is configured with the IP address, but the IP address is not in the same network segment as the VT.

- **Q: What are the differences between agent authentication, enforced CHAP authentication, and LCP renegotiation?**

  A: The LCP renegotiation has the highest authority. That is, if you configure the LCP renegotiation and the enforced CHAP authentication at the same time, the L2TP uses the LCP renegotiation in the mode configured on the VT.

  The enforced CHAP authentication has the secondary priority. That is, if you configure only the enforced CHAP authentication without the LCP renegotiation, the LNS end authenticates the user in CHAP mode. If the authentication does not pass, the session cannot be established.

  The agent authentication has the lowest authority. That is, if you do not configure the enforced CHAP authentication or the LCP renegotiation, the LNS uses the agent authentication. With agent authentication, the LAC transmits all authentication information it gets from the users and the authentication mode configured on the LAC end to the LNS. The LNS authenticates the users by the information and the authentication mode transmitted from the LAC end.

  The relationship between agent authentication and the authentication mode configured on the VT are is follows:

  - If you configure PAP authentication mode on LAC, while the authentication mode configured on the VT on LNS is CHAP, the LAC cannot pass authentication because the priority of CHAP on the LNS is higher.

- In other cases, the authentication mode sent by the LAC is used regardless of the type of authentication mode configured on the VT.

When the LCP is configured for renegotiation and no authentication is configured on the VT, the user is authenticated once. In other cases, the user is authenticated twice.

- **Q: What is the process of the L2TP tunnel authentication?**

  A: If two ends are configured with tunnel authentication, the L2TP tunnel authentication process is as follows. The tunnel authentication and the tunnel establishment are performed simultaneously.

  - When the LAC sends the request for SCCRQ to the LNS, a random character string is generated and sent to the LNS as the local CHAP challenge.
  - After the LNS receives the challenge, it generates a new character string by adding the locally configured password and SCCRP to the random character string, determines a 16-byte response by MD5, and sends the response in the SCCRP message with one random character string LNS Challenge to the LAC.
  - The LAC adds the locally configured password and the SCCRP to its CHAP challenge to generate a new character string. The LAC determines a 16-byte character string by MD5. The LAC compares the 16-byte character string with the LNS CHAP response received from the SCCRP. If they are identical, the LNS passes the authentication. Otherwise, the tunnel is disconnected.
  - The LNS authenticates the LAC in the same way: After the LAC finds the LNS CHAP challenge in the SCCRP, it adds the local password and the SCCN to the character string to generate a new character string. The LAC determines a 16-byte character string by MD5 and sends it, as the LAC CHAP response, to the LNS in the SCCCN message.
  - After the LNS receives the SCCCN message, it adds the local password and the SCCCN to the local CHAP challenge to make a character string. Then the LNS determines a 16-byte character string by MD5 and compares it with the LAC CHAP response received from the SCCCN message. If they are identical, the LAC passes the authentication; if not, the tunnel is disconnected.

- **Q: Are there special considerations if the LNS end is a Nortel router and the LAC end is not?**

  A: It is possible that the LNS end does not support certain parameters that are obtained through PPP prenegotiation between the LAC end and the client end, so the PPP session on the LNS end cannot be established. You need to configure the parameters of the PPP renegotiation on the LNS end and force the LNS and the client end to perform the PPP negotiation.

- **Q: Are there special considerations if the LAC end is a Nortel router and the LNS end is not?**

  A: It is possible that the LAC end does not support certain parameters that are obtained through PPP prenegotiation between the LNS end and the client end, so the PPP session on the LAC end cannot be established. During configuration, examine the parameters of the negotiation between the LNS end and the client end and ensure that these parameters are supported.

1.6 Diagnostic tools

1.6.1 Display commands

Command	Description
display l2tp tunnel	Displays the L2TP tunnel.
display l2tp session	Displays the L2TP session.
display access-user	Displays the access user.
display current-configuration configuration | include l2tp	Displays the current L2TP configuration.
display current-configuration configuration aaa	Displays the current AAA configuration.
display current-configuration interface	Displays the current interface configuration.

display l2tp tunnel

```
<Nortel> display l2tp tunnel
Total tunnel = 1
LocalTID  RemoteTID  RemoteAddress  Port  Sessions  RemoteName
 2       22849    11.1.1.1       1701     1      lns
```

Table 1-1 Description of the output of the **display L2tp tunnel** command

Item	Description
Total tunnel	The number of tunnels
LocalTID	The ID of the local tunnel
RemoteTID	The ID of the remote tunnel
RemoteAddress	The remote IP address
Port	The number of the remote interface
Sessions	The number of sessions on the tunnel
Remote Name	The name of the remote end

display l2tp session

```
<Nortel> display l2tp session
LocalSID     RemoteSID    LocalTID
 1           1            2
 Total session = 1
```

Table 1-2 Description of the output of the **display L2tp session** command

Item	Description
Total session	The number of sessions
LocalSID	The ID of the local session (the only identifier of the session)
RemoteSID	The ID of the remote session (the only identifier of the session)
LocalTID	The number of the local identifier

display access-user

# Check the information about the access user.

```
<Nortel> display access-user
--------------------------------------------------------------------------Total
users                    : 1
  Wait authen-ack                : 0
  Authentication success           : 1
  Accounting ready                : 1
  Accounting state                : 0
  Wait leaving-flow-query          : 0
  Wait accounting-start            : 0
  Wait accounting-stop            : 0
  Wait authorization-client        : 0
  Wait authorization-server        : 0
  -------------------------------------------------------------------
  Domain-name                   Online-user
  -------------------------------------------------------------------
  default                       : 0
  home                         : 1
  -------------------------------------------------------------------
  The used CID table are           :5
---------------------------------------------------------------------
```

The preceding information indicates that one access user belongs to the home domain and its ID is 5.

# Check the information about the access user (specify the ID of the user).

```
<Nortel-aaa> display access-user user-id 5
  -------------------------------------------------------------------
  User access index           : 5
  State                     : Used
  User name                 : vpdnuser@nortel.com
  User access VLAN/PVC        : 0
  User MAC                  : ffff-ffff-ffff
  User IP address            : 120.1.1.11
  Vpn-Instance               : Public
  User access type           : PPP
  User authentication type     : PPP authentication
  Current authen method       : Local authentication
```

```
 Authen result              : Success
 Current author method        : Local authorization
 Author result              : Success
 Action flag                : Idle
 Authen state               : Authed
 Author state               : Idle
 Accounting method           : No accounting
 Accounting start time        : 2005-11-25 09:04:45
 Accounting state            : Ready
 ACL-number                 : -
 Priority                  : -
 Up CAR enable              : NO
 Up average rate             : 0(bps)
 Up peak rate               : 0(bps)
 Down CAR enable             : NO
 Down average rate           : 0(bps)
 Down peak rate              : 0(bps)
 Up packets number(high,low)   : (0,20)
 Up bytes number(high,low)    : (0,2360)
 Down packets number(high,low) : (0,20)
 Down bytes number(high,low)   : (0,1120)
 -------------------------------------------------------------------
```

The preceding information shows detailed information about the user with the ID 5, including the user name, the IP address, the AAA, the online time, and the traffic.

display current-configuration configuration | include l2tp

# Check the current L2TP configuration.

```
<Nortel> display current-configuration configuration | include l2tp
#
L2tp enable
#
l2tp-group 1
 undo tunnel authentication
 allow l2tp virtual-template 1
 tunnel name lns
#
return
```

display current-configuration configuration aaa

# Check the current AAA configuration.

```
<Nortel> display current-configuration configuration aaa
#
aaa
 local-user vpdnuser@nortel.com password simple nortel
 ip pool 1 120.1.1.2 120.1.1.10
 #
 authentication-scheme default
 #
 authorization-scheme default
 #
 accounting-scheme default
 #
 domain default
 domain home
  ip pool 2 120.1.1.11  120.1.1.20
 #
#
return
```

display current-configuration interface

# Check the current interface configuration.

```
<Nortel> display current-configuration interface
#
interface Pos1/0/0
 clock master
 link-protocol ppp
 ip address 31.1.1.2 255.255.0.0
#
interface Virtual-Template1
 ip address 120.1.1.1 255.255.0.0
# interface Pos1/0/0
 ip address 19.60.1.12 255.0.0.0
#
return
```

1.6.2 Debugging commands

Command	Description
debugging l2tp all	Enables debugging of L2TP.
debugging l2tp control	Enables debugging of the L2TP control packet.
debugging l2tp dump	Enables debugging of the L2TP PPP packet.
debugging l2tp error	Enables debugging of L2TP errors.
debugging l2tp event	Enables debugging of L2TP events.
debugging l2tp hidden	Enables debugging of the Attribute Value Pair (AVP) hidden by the L2TP.
debugging l2tp payload	Enables debugging of the L2TP data packet.
debugging l2tp timestamp	Enables debugging of the timestamp displayed by the L2TP.
debugging ppp all	Checks the PPP debugging information about the domain user access to the LNS end.

Example of L2TP debugging of the domain user access to the LNS end

```
<Nortel> debugging l2tp control
*0.2679317 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::Recv mbuf vrfindex is 0
```

```
*0.2679393 Nortel L2TP/8/L2TDBG: L2TP::Proc Peer control type=1, len = 75
*0.2679473 Nortel L2TP/8/L2TDBG: L2TP::Tunnel 1 rcv SCCRQ in state 1  from 31.1.1.1
*0.2679569 Nortel L2TP/8/L2TDBG: L2TP::Tunnel 1 rcv SCCRQ fill vpn-index 0
*0.2679649 Nortel L2TP/8/L2TDBG: L2TP::Check SCCRQ MSG Type 1
*0.2679729 Nortel L2TP/8/L2TDBG: L2TP::Parse AVP Protocol version:  100
*0.2679809 Nortel L2TP/8/L2TDBG: L2TP::Parse AVP Host name, value: lac
*0.2679889 Nortel L2TP/8/L2TDBG: L2TP::Tunnel Password in l2tp Group:
*0.2679969 Nortel L2TP/8/L2TDBG: L2TP::Parse AVP Vendor name, value: Nortel
*0.2680049 Nortel L2TP/8/L2TDBG: L2TP::Parse AVP Framing capability : 3
*0.2680129 Nortel L2TP/8/L2TDBG: L2TP::Parse AVP Remote call number, value: 1
*0.2680225 Nortel L2TP/8/L2TDBG: L2TP::Parse AVP Receive window size, value: 128
*0.2680321 Nortel L2TP/8/L2TDBG: L2TP::Put AVP Message Type:
START_CONTROL_CONNECTION_REPLY
*0.2680417 Nortel L2TP/8/L2TDBG: L2TP::Put AVP Protocol version:  100
*0.2680497 Nortel L2TP/8/L2TDBG: L2TP::Put AVP Framing capability :3
*0.2680577 Nortel L2TP/8/L2TDBG: L2TP::Put AVP Host name: lns
*0.2680657 Nortel L2TP/8/L2TDBG: L2TP::Put AVP Assigned Tunnel ID: 1
*0.2680737 Nortel L2TP/8/L2TDBG: L2TP::Put AVP Bearer capability: 3
*0.2680817 Nortel L2TP/8/L2TDBG: L2TP::Put AVP Receive window size: 128
*0.2680897 Nortel L2TP/8/L2TDBG: L2TP:: O Tunnel  1 send START_CONTROL_CONNECTION_REPLY
to Tunnel 1
*0.2681025 Nortel L2TP/8/L2TDBG: L2TP::Tunnel 1 Create 60 seconds Hello timer
*0.2681121 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::Recv mbuf vrfindex is 0
*0.2681201 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::Recv mbuf vrfindex is 0
*0.2681281 Nortel L2TP/8/L2TDBG: L2TP::Proc Peer control type=3, len = 20
*0.2681361 Nortel L2TP/8/L2TDBG: L2TP::Tunnel 1 rcv SCCCN in state 3
*0.2681441 Nortel L2TP/8/L2TDBG: L2TP::Tunnel 1 Resume 60 second Hello timer
*0.2681521 Nortel L2TP/8/L2TDBG: L2TP::Check SCCCN MSG Type 3
*0.2681601 Nortel L2TP/8/L2TDBG: L2TP::Tunnel 1 Start Waiting Calls
*0.2681681 Nortel L2TP/8/L2TDBG: L2TP::Proc Peer control type=10, len = 68
*0.2681761 Nortel L2TP/8/L2TDBG: L2TP::Call 7834 recv ICRQ in state 2 from Call 0
*0.2681857 Nortel L2TP/8/L2TDBG: L2TP::Tunnel 1 Resume 60 second Hello timer
*0.2681937 Nortel L2TP/8/L2TDBG: L2TP::Check ICRQ MSG Type 10
*0.2682017 Nortel L2TP/8/L2TDBG: L2TP::Parse AVP Remote call ID 7256
*0.2682097 Nortel L2TP/8/L2TDBG: L2TP::Parse AVP Call serial number: 7256
*0.2682177 Nortel L2TP/8/L2TDBG: L2TP::Parse AVP Bearer type: 3
*0.2682257 Nortel L2TP/8/L2TDBG: L2TP::Parse AVP Physical channel ID:0
*0.2682337 Nortel L2TP/8/L2TDBG: L2TP::Parse AVP Dialed number: 8888
*0.2682417 Nortel L2TP/8/L2TDBG: L2TP::Put AVP Message Type: INCOMING_CALL_REPLY
*0.2682513 Nortel L2TP/8/L2TDBG: L2TP::Put AVP Assigned call ID: 7834
*0.2682593 Nortel L2TP/8/L2TDBG: L2TP::Call 7834 send INCOMING_CALL_REPLY to Remote Call
7256
*0.2682721 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::Recv mbuf vrfindex is 0
*0.2682801 Nortel L2TP/8/L2TDBG: L2TP::Proc Peer control type=12, len = 139
*0.2682882 Nortel L2TP/8/L2TDBG: L2TP::Call 7834 rcv ICCN in state 5 from Remote Call
7256
*0.2682977 Nortel L2TP/8/L2TDBG: L2TP::Tunnel 1 Resume 60 second Hello timer
*0.2683057 Nortel L2TP/8/L2TDBG: L2TP::Check ICCN MSG Type 12
*0.2683137 Nortel L2TP/8/L2TDBG: L2TP::Parse AVP Tx connect speed: 64000
*0.2683217 Nortel L2TP/8/L2TDBG: L2TP::Parse AVP Framing type: 3
*0.2683297 Nortel L2TP/8/L2TDBG: L2TP::Parse AVP Initial recv lcp configure request:
5  6 20 E3 DA 8F
*0.2683425 Nortel L2TP/8/L2TDBG: L2TP::Parse AVP Last sent lcp configure request: 3  4
C0 23  5  6  0 25 E8 7F
```

```
*0.2683553 Nortel L2TP/8/L2TDBG: L2TP::Parse AVP Last received lcp configure request:
5  6 20 E3 DA 8F
*0.2683681 Nortel L2TP/8/L2TDBG: L2TP::Parse AVP Proxy authenticate type 3.
*0.2683761 Nortel L2TP/8/L2TDBG: L2TP::Parse AVP Proxy authenticate name:yyh@home.
*0.2683857 Nortel L2TP/8/L2TDBG: L2TP::Parse AVP Proxy authentication ID: 40435440.
*0.2683953 Nortel L2TP/8/L2TDBG: L2TP::Parse AVP Proxy authenticate response:31 32 33
*0.2684049 Nortel L2TP/8/L2TDBG: L2TP::Parse AVP Private group ID
*0.2684129 Nortel L2TP/8/L2TDBG: L2TP::Parse AVP (Rx)connect speed 64000
*0.2684209 Nortel L2TP/8/L2TDBG: L2TP::Call 7834 established , Send Call Struct to IO
slot 1
*0.2684305 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::IPC Recv Src IPC ID=11 Dst node=7 Dst IPC
ID=11 Len=172
*0.2684433 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::IPC rec data type=100 len=172
*0.2684513 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::IPC Proc IPC data result 0
*0.2684609 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::IO: Proc ctrl L2TP_INCALL_ESTABLISHED
from main
*0.2684721 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::IO:: rec main establish call ID 7834 group
1 VT 1
*0.2684833 Nortel L2TP/8/L2TDBG: L2TP::IPC Recv Src IPC ID=11 Dst node=1 Dst IPC ID=11
Len=16
*0.2684945 Nortel L2TP/8/L2TDBG: L2TP::IPC rec data type=16 len=16
*0.2685025 Nortel L2TP/8/L2TDBG: L2TP::IPC Proc IPC data result 0
*0.2685105 Nortel L2TP/8/L2TDBG: L2TP::Put AVP Message Type: SET_LINK_INFO
*0.2685185 Nortel L2TP/8/L2TDBG: L2TP::Put AVP ACCM: 0 0
*0.2685249 Nortel L2TP/8/L2TDBG: L2TP:: O Call 7834 send SLI
*0.2685313 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::IPC Recv Src IPC ID=11 Dst node=7 Dst IPC
ID=11 Len=1384
*0.2685441 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::IPC rec data type=100 len=1384
*0.2685521 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::IPC Proc IPC data result 0
*0.2685601 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::IO: Proc ctrl L2TP_PHY_READY from main
*0.2685697 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::LNS Virtual Access for Call :7834 UP
*0.2685793 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::LNS Link IO Ctrl Recv Phy CMD 23
*0.2685889 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::LNS Link IO Ctrl Recv Phy CMD 24
*0.2685985 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::LNS Link IO Ctrl Recv Phy CMD 41
*0.2686081 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::Send ACCM. CALL = 7834
*0.2686161 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::IPC sent ctrl L2TP_INCALL_ESTABLISHED
len=16 result=0 to main
*0.2686289 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::Recv mbuf vrfindex is 0
*0.2686369 Nortel L2TP/8/L2TDBG: L2TP::Proc Peer control len = 12
*0.2699426 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::LNS Link IO Ctrl Recv Phy CMD 36
*0.2699521 Nortel L2TP/8/L2TDBG: L2TP::IPC Recv Src IPC ID=11 Dst node=1 Dst IPC ID=11
Len=16
*0.2699633 Nortel L2TP/8/L2TDBG: L2TP::IPC rec data type=4 len=16
*0.2699713 Nortel L2TP/8/L2TDBG: L2TP::IPC Proc IPC data result 0
*0.2699793 Nortel L2TP/8/L2TDBG: L2TP::Proc Call Down , Call in State 9
*0.2699873 Nortel L2TP/8/L2TDBG: L2TP::Put AVP Message Type: CALL_DISCONNECT_NOTIFY
*0.2699969 Nortel L2TP/8/L2TDBG: L2TP::Put AVP Result code: LOSS_OF_CARRIER
*0.2700049 Nortel L2TP/8/L2TDBG: L2TP::Put AVP Assigned call ID: 7834
*0.2700129 Nortel L2TP/8/L2TDBG: L2TP:: O Call 7834 send CALL_DISCONNECT_NOTIFY
*0.2700225 Nortel L2TP/8/L2TDBG: L2TP::Clean Call Structure ID = 7834
*0.2700305 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::IPC Recv Src IPC ID=11 Dst node=7 Dst IPC
ID=11 Len=32
*0.2700417 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::IPC rec data type=100 len=32
*0.2700497 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::IPC Proc IPC data result 0
```

```
*0.2700577 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::IPC sent ctrl L2tp down to main len=16
result=0 to main
*0.2700705 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::IO: Proc ctrl L2TP_LNSINCALL_CLEAR from
main
*0.2700801 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::Call 7834 Proc main call clear
*0.2700881 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::LNS Link IO Ctrl Recv Phy CMD 2
*0.2700977 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::LNS Link IO Ctrl Recv Phy CMD 11
*0.2701073 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::IO:: Call clear 7834
*0.2701153 Nortel L2TP/8/L2TDBG:Slot=1; L2TP::Recv mbuf vrfindex is 0
*0.2701248 Nortel L2TP/8/L2TDBG: L2TP::Proc Peer control len = 12
```

Example of PPP debugging of the domain user access to the LNS end

```
<Nortel> debugging ppp all
*0.2347645 Nortel PPP/8/debug2:Slot=1;
  PPP State Change:
      Virtual-Template1:0 LCP : initial --> reqsent
*0.2347761 Nortel PPP/8/debug2:Slot=1;
  PPP State Change:
      Virtual-Template1:0 LCP : reqsent --> ackrcvd
*0.2347889 Nortel PPP/8/debug2:Slot=1;
  PPP State Change:
      Virtual-Template1:0 LCP : ackrcvd --> opened
*0.2348017 Nortel PPP/8/debug2:Slot=1;
  PPP Event:
      Virtual-Template1:0 : PPP Notify low layer to send remote accm  0 , local
accm  0 Packet
*0.2348193 Nortel PPP/8/debug2:Slot=1;
  PPP Event:
      Virtual-Template1:0 PAP Initial  Event
      state Initial
*0.2348337 Nortel PPP/8/debug2:Slot=1;
  PPP Event:
      Virtual-Template1:0 PAP AAA Result Event
      state WaitAAA
*0.2348481 Nortel PPP/8/debug2:Slot=1;
  PPP Packet:
      Virtual-Template1:0 Output PAP(c023) Pkt, Len 52
      State WaitAAA, code Ack(02), id 0, len 48
      Msg Len: 43  Msg:Welcome to use Nortel ROUTER, Nortel Tech.
*0.2348769 Nortel PPP/8/debug2:Slot=1;
  PPP State Change:
      Virtual-Template1:0 PAP : WaitAAA --> ServerSuccess
*0.2348913 Nortel PPP/8/debug2:Slot=1;
  PPP Event:
      Virtual-Template1:0 : Ask AAA peer's IP address
*0.2349041 Nortel PPP/8/debug2:Slot=1;
  PPP Event:
      Virtual-Template1:0 : WaitPeerIP Timer starting
*0.2349169 Nortel PPP/8/debug2:Slot=1;
  PPP Event:
      Virtual-Template1:0 : Receive Peer's IP address 120.1.1.11 from AAA
*0.2349329 Nortel PPP/8/debug2:Slot=1;
  PPP Event:
      Virtual-Template1:0 : WaitPeerIP Timer finished
*0.2349457 Nortel PPP/8/debug2:Slot=1;
```

```
  PPP Event:
     Virtual-Template1:0 IPCP Open  Event
     state initial
*0.2349601 Nortel PPP/8/debug2:Slot=1;
  PPP State Change:
     Virtual-Template1:0 IPCP : initial --> starting
*0.2349729 Nortel PPP/8/debug2:Slot=1;
  PPP Event:
     Virtual-Template1:0 IPCP Lower Up  Event
     state starting
*0.2349889 Nortel PPP/8/debug2:Slot=1;
  PPP State Change:
     Virtual-Template1:0 IPCP : starting --> reqsent
*0.2350017 Nortel PPP/8/debug2:Slot=1;
  PPP Packet:
     Virtual-Template1:0 Output IPCP(8021) Pkt, Len 14
     State reqsent, code ConfReq(01), id 0, len 10
     IP Address(3), len 6, val 78010101
*0.2350273 Nortel PPP/8/debug2:Slot=1;
  PPP Packet:
     Virtual-Template1:0 Input  IPCP(8021) Pkt, Len 38
     State reqsent, code ConfReq(01), id 1, len 34
     IP Address(3), len 6, val 00000000
     Primary DNS Server Address(81), len 6, val 00000000
     Secondary DNS Server Address(83), len 6, val 00000000
     Primary NBNS Server Address(82), len 6, val 00000000
     Secondary NBNS Server Address(84), len 6, val 00000000
*0.2350833 Nortel PPP/8/debug2:Slot=1;
  PPP Event:
     Virtual-Template1:0 IPCP RCR-(Receive Config Bad Request)  Event
     state reqsent
*0.2351009 Nortel PPP/8/debug2:Slot=1;
  PPP Packet:
     Virtual-Template1:0 Output IPCP(8021) Pkt, Len 32
     State reqsent, code ConfRej(04), id 1, len 28
     Primary DNS Server Address(81), len 6, val 00000000
     Secondary DNS Server Address(83), len 6, val 00000000
     Primary NBNS Server Address(82), len 6, val 00000000
     Secondary NBNS Server Address(84), len 6, val 00000000
%Oct 20 03:51:14 2005 Nortel IFNET/5/UPDOWN:Slot=1;PPP IPCP protocol on the interface
Virtual-Template1:0 turns in UP state
*0.2352256 Nortel PPP/8/debug2:Slot=1;
  PPP Packet:
     Virtual-Template1:0 Input  IPCP(8021) Pkt, Len 14
     State reqsent, code ConfAck(02), id 0, len 10
     IP Address(3), len 6, val 78010101
*0.2352513 Nortel PPP/8/debug2:Slot=1;
  PPP Event:
     Virtual-Template1:0 IPCP RCA(Receive Config Ack)  Event
     state reqsent
*0.2352673 Nortel PPP/8/debug2:Slot=1;
  PPP State Change:
     Virtual-Template1:0 IPCP : reqsent --> ackrcvd
*0.2352801 Nortel PPP/8/debug2:Slot=1;
  PPP Packet:
     Virtual-Template1:0 Input  IPCP(8021) Pkt, Len 14
     State ackrcvd, code ConfReq(01), id 2, len 10
     IP Address(3), len 6, val 00000000
*0.2353057 Nortel PPP/8/debug2:Slot=1;
  PPP Event:
     Virtual-Template1:0 IPCP RCR-(Receive Config Bad Request)  Event
     state ackrcvd
*0.2353233 Nortel PPP/8/debug2:Slot=1;
  PPP Packet:
     Virtual-Template1:0 Output IPCP(8021) Pkt, Len 14
     State ackrcvd, code ConfNak(03), id 2, len 10
     IP Address(3), len 6, val 7801010b
*0.2353489 Nortel PPP/8/debug2:Slot=1;
  PPP Packet:
     Virtual-Template1:0 Input  IPCP(8021) Pkt, Len 14
     State ackrcvd, code ConfReq(01), id 3, len 10
     IP Address(3), len 6, val 7801010b
*0.2353745 Nortel PPP/8/debug2:Slot=1;
  PPP Event:
     Virtual-Template1:0 IPCP RCR+(Receive Config Good Request)  Event
     state ackrcvd
*0.2353921 Nortel PPP/8/debug2:Slot=1;
  PPP Packet:
     Virtual-Template1:0 Output IPCP(8021) Pkt, Len 14
     State ackrcvd, code ConfAck(02), id 3, len 10
     IP Address(3), len 6, val 7801010b
*0.2354177 Nortel PPP/8/debug2:Slot=1;
  PPP State Change:
     Virtual-Template1:0 IPCP : ackrcvd --> opened
*0.2354305 Nortel PPP/8/debug2:Slot=1;
  PPP Packet:
     Virtual-Template1:0 Input  IP(0021) Pkt, Len 100
*0.2354433 Nortel PPP/8/debug2:Slot=1;
  PPP Packet:
     Virtual-Template1:0 Output IP(0021) Pkt, Len 60
```

Contents

Figures

Tables

2 GRE troubleshooting

About this chapter

The following table describes the contents of this chapter.

Section	Describes
2.1 GRE overview	This section provides the knowledge you need before you troubleshoot the Generic Routing Encapsulation (GRE).
2.2 Troubleshooting GRE	This section provides notes about configuring GRE, the GRE troubleshooting flowchart, and the troubleshooting procedure in a typical GRE network.
2.3 Troubleshooting cases	This section presents several troubleshooting cases.
2.4 FAQs	This section lists frequently asked questions and their answers.
2.5 Diagnostic tools	This section describes common diagnostic tools: **display** commands, **debugging** commands, and alarms.

2.1 GRE overview

This section covers the following topics:

- Introduction to GRE
- Related concepts of GRE
- Applications of GRE

2.1.1 Introduction to GRE

Generic Routing Encapsulation (GRE) encapsulates packets of any network layer, such as Internetwork Packet Exchange (IPX), to enable their transmission by another network layer protocol such as IP.

GRE is a Layer 3 virtual private network (VPN) tunneling protocol that provides a tunnel for transparent transmission of various protocol packets.

A tunnel is a virtual point-to-point connection, and it can be considered as a virtual interface that supports point-to-point (P2P) connections only. The virtual interface provides a path for the transmission of data that can be encapsulated and decapsulated at both ends of the path.

2.1.2 Related concepts of GRE

Encapsulation and decapsulation of packets

Payload refers to the datagram received by the system for encapsulation and routing. The payload is first added with a GRE header. That is, the payload is encapsulated into GRE packets. The GRE packets are then encapsulated into IP packets to be transported over the IP layer.

Figure 2-1 shows the format of an encapsulated tunnel packet.

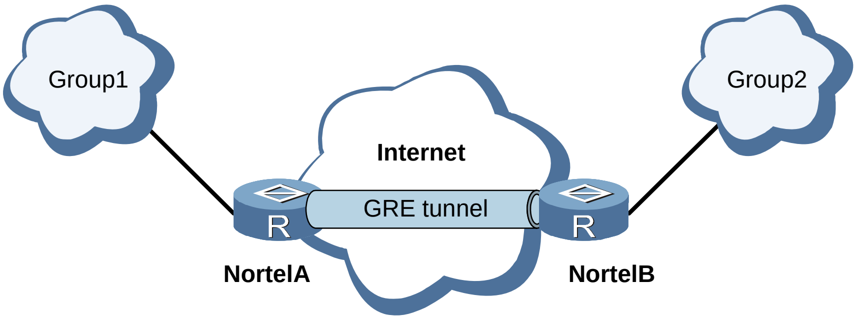
Figure 2-1 Format of an encapsulated tunnel packet

Delivery Header (Transport Protocol)
GRE Header (Encapsulation Protocol)
Payload Packet (Passenger Protocol)

Transmission of packets

The transmission of packets in the tunnel involves encapsulation and decapsulation. Use Figure 2-2 as an example to describe the process.

Figure 2-2 Two networks interconnecting through the GRE tunnel



Encapsulation process

After receiving an IP datagram, the interface on Nortel A that connects with Group 1 sends the datagram to the IP module for processing.

The IP module determines how to route this datagram based on the destination address contained in the IP header. If the network with the network number 1f passes its destination address (the virtual network ID of the tunnel), this datagram is sent to the tunnel interface of that network.

After receiving this datagram, the GRE module encapsulates it and sends it to the IP module. The IP module appends an IP header to the datagram and then sends it to the corresponding network interface based on the packet destination address and the routing table.

Decapsulation process

The decapsulation process is the reverse of the encapsulation process.

After receiving an IP packet from the GRE tunnel interface, Nortel B checks for the destination address of the packet. If the destination is found to be a local router, the IP header of the packet is removed. According to the protocol field in the IP header, the packet is determined to be a GRE packet and sent to the GRE module. After processing, the GRE module removes the GRE header and sends the datagram to the IP module according to the protocol field. The IP module then handles this datagram.

2.1.3 Applications of GRE

You can use GRE to perform the following functions:

- Transmit packets from multiprotocol local networks over a backbone network that runs a single protocol
- Connect discontinuous subnets to extend the operation space of the network whose routing protocol is limited in hops.
- Build VPNs.
- Resolve the defect of IPSec that cannot protect multicast packets in combination with IPSec.
- Provide two less strong security mechanisms, namely, checksum verification and key verification.

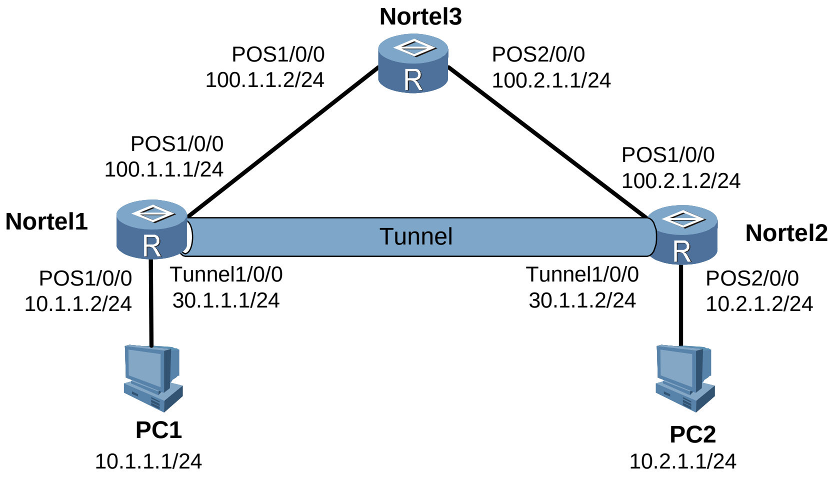
2.2 Troubleshooting GRE

This section covers the following topics:

- Typical networking
- Configuration notes
- Troubleshooting flowchart
- Troubleshooting procedure

2.2.1 Typical networking

Figure 2-3 Typical GRE networking diagram



As shown in Figure 2-3:

- A GRE tunnel is set up between Nortel 1 and Nortel 2.
- Nortel 1 and Nortel 3 directly connect.
- Nortel 2 and Nortel 3 directly connect.

2.2.2 Configuration notes

NOTE
If you create a tunnel interface on a distributed device, configure the same slot numbers for the tunnel interface and the tunnel source. Use the slot that sends out GRE packets to improve the forwarding efficiency.

Item	Subitem	Notes
Configuring the encapsulation mode on both ends of a tunnel	Tunnel protocol	The encapsulation mode must be the same on both ends of a tunnel.

Item	Subitem	Notes
Specifying the source address of the tunnel	Source	The source address of a tunnel is the IP address of the physical interface that sends the GRE packets. The source address of a tunnel can be ● Source interface ● IP address of the source interface ● Another tunnel interface
Specifying the destination address of the tunnel	Destination	The destination address of the tunnel is the IP address of the interface that receives GRE packets. You must specify the destination address as the IP address of the destination end. The source address and the destination address uniquely identify a tunnel. These configurations must be performed on both ends of a tunnel.
Assigning an IP address for the tunnel interface	IP address	If the tunnel supports dynamic routing protocols, you must configure an IP address or configure unnumbered IP addresses for the tunnel. The IP address of the tunnel interface does not need to be a public network address.
Configuring the routes forwarded by the tunnel	Static route or dynamic route	The routes on both ends of a tunnel must use routes that are forwarded by the tunnel to forward GRE-encapsulated packets correctly. Configure static or dynamic routes at both ends of the tunnel. While you configure static routes, note that the destination address is the address of the interface that receives the packet without the GRE encapsulation. The next hop is the address of the local tunnel interface. While you configure dynamic routes, you must enable the dynamic protocol on both the tunnel interface and the interface of the router that connects with the private network. To ensure that the correct route is chosen, do not choose the tunnel interface as the outgoing interface.
Configuring the GRE key (optional)	GRE key	If the GRE key is required, configure the key on both ends and specify the same key-number.

Use Figure 2-3 as an example to describe the notes about configuring GRE.

- Configuring a tunnel interface on Nortel 1

# Assign an IP address for POS 1/0/0:

```
[Nortel1] interface pos 1/0/0
[Nortel1-Pos1/0/0] ip address 100.1.1.1 255.255.255.0
```

# Assign an IP address for the tunnel interface:

```
[Nortel1] interface tunnel 1/0/0
[Nortel1-Tunnel1/0/0] ip address 30.1.1.1 255.255.255.0
```

# Specify the source address of the tunnel.

- Configuring the IP address of the interface that sends out packets as the source address::

```
[Nortel1-Tunnel1/0/0] source 100.1.1.1
```

- Or setting the interface that sends out packets as the source address:

```
[Nortel1-Tunnel1/0/0] source pos 1/0/0
```

# Specify the destination address of the tunnel:

```
[Nortel1-Tunnel1/0/0] destination 100.2.1.2
```

- Configuring a tunnel interface on Nortel 2

# Assign an IP address for POS 1/0/0:

```
[Nortel2] interface pos 1/0/0
[Nortel2-Pos1/0/0] ip address 100.2.1.2 255.255.255.0
```

# Assign an IP address for the tunnel:

```
[Nortel2] interface tunnel 1/0/0
[Nortel2-Tunnel1/0/0] ip address 30.1.1.2 255.255.255.0
```

# Specify the source address of the tunnel.

- Configuring the IP address of the interface that sends out packets as the source address:

```
[Nortel2-Tunnel1/0/0] source 100.2.1.2
```

- Or setting the interface that sends out packets as the source address:

```
[Nortel2-Tunnel1/0/0] source pos 1/0/0
```

# Specify the destination address of the tunnel:

```
[Nortel2-Tunnel1/0/0] destination 100.1.1.1
```

- Configuring routes to enable communication between Nortel 1 and Nortel 2

# Configure a static route to Nortel 2 on Nortel 1:

```
[Nortel1] ip route-static 100.2.1.0 255.255.255.0 100.1.1.2
```

# Configure a static route to Nortel 1 on Nortel 2:

```
[Nortel2] ip route-static 100.1.1.0 255.255.255.0 100.2.1.1
```

- Configuring carrier network routes or customer network routes forwarded by the tunnel
  - Configure carrier network routes forwarded by the tunnel:

```
[Nortel1] ip route-static 30.1.1.0 255.255.255.0 tunnel 1/0/0
[Nortel2] ip route-static 30.1.1.0 255.255.255.0 tunnel 1/0/0
```

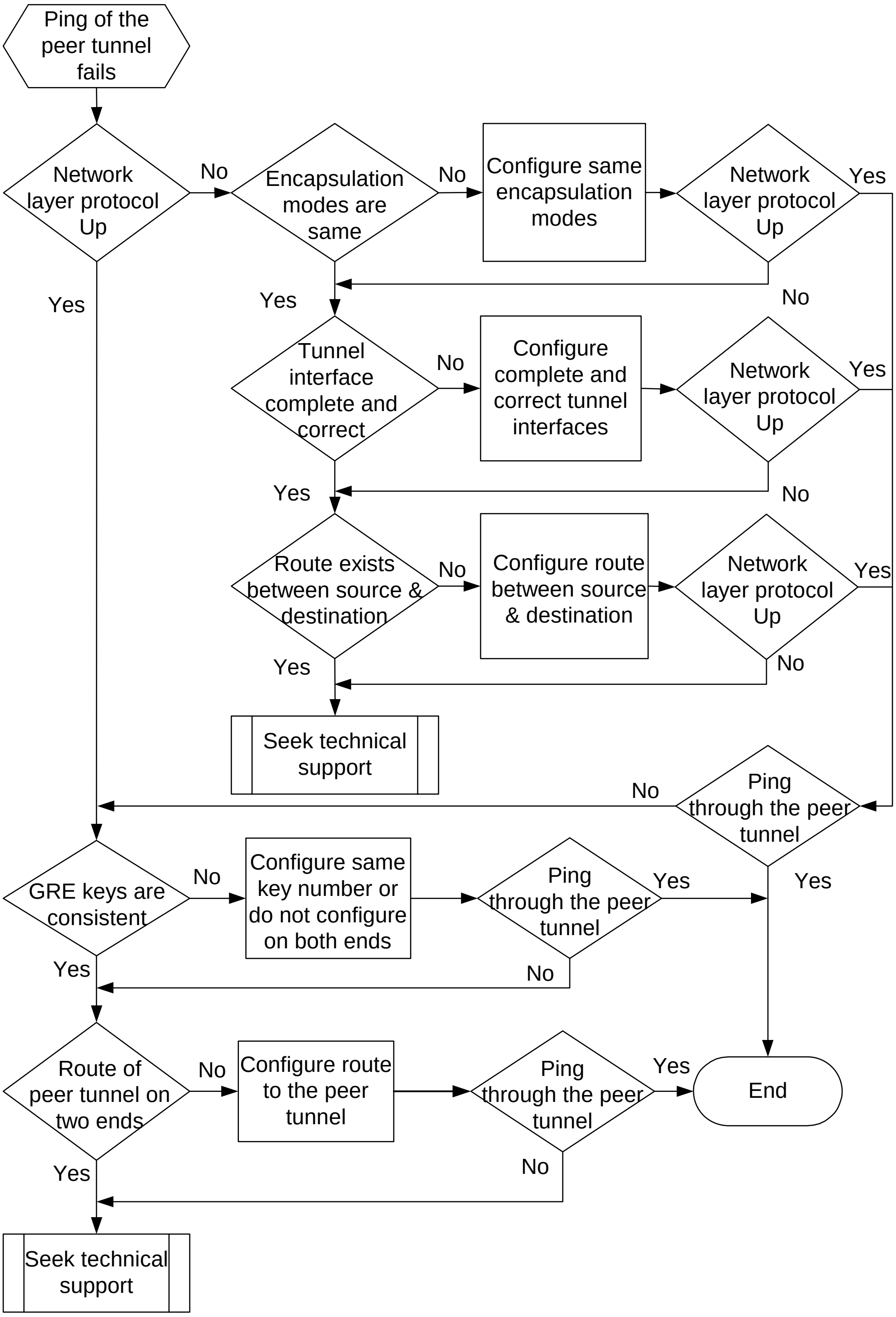
  - Or configure customer network routes forwarded by the tunnel:

```
[Nortel1] ip route-static 10.2.1.0 255.255.255.0 tunnel 1/0/0
[Nortel2] ip route-static 10.1.1.0 255.255.255.0 tunnel 1/0/0
```

2.2.3 Troubleshooting flowchart

Figure 2-4 shows the troubleshooting flowchart.

Figure 2-4 GRE troubleshooting flowchart


Ping of the peer tunnel fails
Network layer protocol Up
No
Encapsulation modes are same
No
Configure same encapsulation modes
Network layer protocol Up
Yes
Yes
Yes
No
Tunnel interface complete and correct
No
Configure complete and correct tunnel interfaces
Network layer protocol Up
Yes
Yes
No
Route exists between source & destination
No
Configure route between source & destination
Network layer protocol Up
Yes
Yes
No
Seek technical support
No
Ping through the peer tunnel
GRE keys are consistent
No
Configure same key number or do not configure on both ends
Ping through the peer tunnel
Yes
Yes
Yes
No
Route of peer tunnel on two ends
No
Configure route to the peer tunnel
Ping through the peer tunnel
Yes
End
Yes
No
Seek technical support

2.2.4 Troubleshooting procedure

This section provides the troubleshooting steps.

Two different situations are possible.

Network layer protocol of one end or both ends of the tunnel interface is down

Step 1 Check that both ends of the tunnel use a consistent encapsulation type.

Run the **display this interface** command in the tunnel interface view to check the encapsulation type. View the display of the tunnel interface to find the encapsulation type on both ends of the tunnel. The sample display is as follows:

```
[Nortel1-Tunnel1/0/0] display this interface
Tunnel1/0/0 current state : UP
Line protocol current state : UP
Description : Nortel Series, Tunnel1/0/0 Interface, Route Port
The Maximum Transmit Unit is 1500 bytes
Internet Address is 30.1.1.1/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 100.1.1.1 (Serial1/0/0), destination 100.2.1.2
Tunnel protocol/transport GRE/IP , key disabled
Checksumming of packets disabled
QoS max-bandwidth : 64 Kbps
Output queue : (Urgent queue : Size/Length/Discards)  0/50/0
Output queue : (Protocol queue : Size/Length/Discards) 0/1000/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
    5 minutes input rate 0 bytes/sec, 0 packets/sec
    5 minutes output rate 0 bytes/sec, 0 packets/sec
    0 packets input,  0 bytes
    0 input error
    0 packets output,  0 bytes
    0 output error
```

The tunnel currently supports three types of encapsulation:

- GRE (default type)
- IPv6-IPv4
- Multiprotocol Label Switching (MPLS) Traffic Engineering (TE)

You can find that the tunnel uses GRE encapsulation by viewing the information in boldface in the display.

If the same encapsulation type is set at both ends, go to step 2.

Step 2 Check that IP addresses, source addresses, and destination addresses are correct on the tunnel interfaces on both ends.

The source address of one end is the destination address of another end and the destination address of one end is the source address of another end. Otherwise, a tunnel cannot establish because a source and a destination address together identify a unique tunnel.

Run the **display this** command in the tunnel interface view to check the configuration at both ends of the tunnel.

For example, the correct tunnel configuration for Figure 2-3 is as follows:

# Tunnel configuration on Nortel 1

```
[Nortel1-Tunnel1/0/0] display this
#
interface Tunnel1/0/0
 ip address 30.1.1.1 255.255.255.0
 source 100.1.1.1
 destination 100.2.1.2
#
return
```

# Tunnel configuration on Nortel 2

```
[Nortel2-Tunnel1/0/0] display this
#
interface Tunnel1/0/0
 ip address 30.1.1.2 255.255.255.0
 source 100.2.1.2
 destination 100.1.1.1
#
return
```

If the display shows that both ends reverse the source address and the destination address, then run the **display this interface** command in the tunnel interface view. Go to the next step, if you find that Line protocol current state is down; it indicates that the tunnel status is down.

Step 3 Check that reachable routes exist between the tunnel source and destination addresses.

If the tunnel interface configuration at both ends is correct, but the status of the tunnel is still down, check for reachable routes between the source and destination interfaces of the tunnel.

- If the two interfaces do not directly connect, check for the route to the remote tunnel interface on each interface.
- If the two interfaces directly connect, no problem exists with routes.

Use the **display ip routing-table** command to check the routing table. If the table is correct, use the **display fib** command to view the Forwarding Information Base (FIB) table to see whether the data is forwarded correctly. The FIB must be consistent with the routing table.

Use Nortel 1 and Nortel 2 shown in Figure 2-3 as an example.

The output of the **display fib** command on Nortel 1 is as follows:

```
FIB Table:
 Total number of Routes : 10
Destination/Mask   Nexthop         Flag TimeStamp     Interface       Token
127.0.0.1/32       127.0.0.1       HU   t[0]          InLoop0         0x0
127.0.0.0/8        127.0.0.1       U    t[0]          InLoop0         0x0
100.1.1.1/32       127.0.0.1       HU   t[0]          InLoop0         0x0
100.1.1.0/24       100.1.1.1       U    t[0]          Pos1/0/0        0x0
10.1.1.2/32        127.0.0.1       HU   t[0]          InLoop0         0x0
10.1.1.0/24        10.1.1.2        U    t[0]          Pos2/0/0        0x0
30.1.1.1/32        127.0.0.1       HU   t[0]          InLoop0         0x0
30.1.1.0/24        30.1.1.1        U    t[0]          Tun1/0/0        0x0
The display of Nortel 2 is as follows:
FIB Table:
 Total number of Routes : 10

Destination/Mask   Nexthop         Flag TimeStamp     Interface       Token
```

```
127.0.0.1/32       127.0.0.1       HU   t[0]          InLoop0         0x0
127.0.0.0/8        127.0.0.1       U    t[0]          InLoop0         0x0
100.2.1.2/32       127.0.0.1       HU   t[0]          InLoop0         0x0
100.2.1.0/24       100.2.1.2       U    t[0]          Pos1/0/0        0x0
10.2.1.2/32        127.0.0.1       HU   t[0]          InLoop0         0x0
10.2.1.0/24        10.2.1.2        U    t[0]          Pos2/0/0        0x0
30.1.1.2/32        127.0.0.1       HU   t[0]          InLoop0         0x0
30.1.1.0/24        30.1.1.2        U    t[0]          Tun1/0/0        0x0
```

The preceding FIB shows that Nortel 1 has no route to Nortel 2 on the network segment 100.2.1.0; Nortel 2 has no route to Nortel 1 on the network segment 100.1.1.0. Therefore, the status of the tunnel interface at both ends is down, and the two ends cannot ping each other.

Configure a static route or dynamic routing protocol on Nortel 1 and Nortel 2 respectively. Then, Nortel 1 has routes from 100.1.1.0 to 100.2.1.0; Nortel 2 has routes from 100.2.1.0 to 100.1.1.0.

----End

If the network layer protocol is still down, contact Nortel technical personnel.

If the network layer protocol on both ends of the tunnel interface changes to up but the ping of the peer tunnel fails, perform the troubleshooting steps in the following section.

Network layer protocols on both ends of the tunnel interface are up

Step 1 Check that the configurations of the GRE keys on both ends are consistent.

Use the **display interface tunnel** *interface-number* command on both ends to check that the GRE keys are consistent.

The correct configuration is one of the following two situations:

- No GRE key is configured on either end.
- The same key-number is configured on both ends.

If the configuration is correct but the two ends cannot ping through each other, perform as follows.

Step 2 Check that reachable routes exist between the tunnel interfaces.

After you complete the previous step, the tunnel status at both ends is up and the physical interface can ping through each other. But you cannot ping the tunnel interface successfully. Check whether the IP addresses of the tunnel interfaces on both ends are on the same network segment; if not, configure routes to the IP address of the remote tunnel interface.

----End

If the GRE tunnel fault persists, contact Nortel technical personnel.

2.3 Troubleshooting cases

This section provides the following troubleshooting cases:

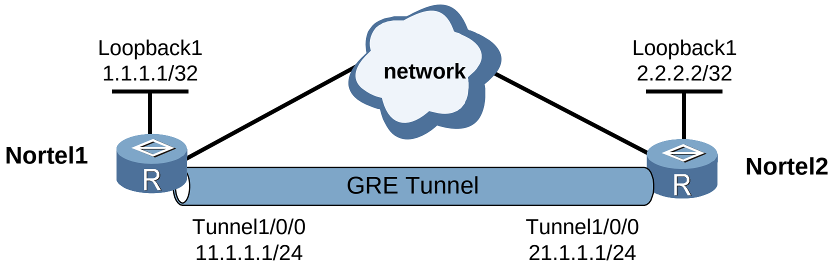
- Ping of the peer tunnel fails although the network layer protocols on both ends are up

- PCs cannot ping through each other although tunnel interfaces on two ends can ping each other successfully

2.3.1 Ping of the peer tunnel fails although the network layer protocols on both ends are up

Fault symptom

Figure 2-5 Networking diagram of the GRE troubleshooting I



The network layer protocols on both ends of the GRE tunnel are up. But, Tunnel 1/0/0 on Nortel 1 and Tunnel 1/0/0 on Nortel 2 cannot ping through each other.

Fault analysis

The possible causes are as follows:

- The GRE keys on both ends are inconsistent.
- The IP addresses of the tunnel interfaces on two ends are not in the same network segment and no reachable route exists between two ends of the tunnel

Use the **display interface tunnel** *interface-number* command on both ends to check whether the GRE keys are consistent.

The output of the command on Nortel 1 is as follows:

```
[Nortel1] display interface Tunnel 1/0/0
Tunnel1/0/0 current state : UP
Line protocol current state : UP
Description : Nortel Series, Tunnel1/0/0 Interface
The Maximum Transmit Unit is 1000 bytes
Internet Address is 11.1.1.1/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 1.1.1.1 (LoopBack1), destination 2.2.2.2
Tunnel protocol/transport GRE/IP , key 0x2
linkalive disabled
Checksumming of packets disabled
QoS max-bandwidth : 64 Kbps
Output queue : (Urgent queue : Size/Length/Discards)  0/50/0
Output queue : (Protocol queue : Size/Length/Discards) 0/1000/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/256/0
    5 minutes input rate 0 bytes/sec, 0 packets/sec
    5 minutes output rate 0 bytes/sec, 0 packets/sec
    0 packets input,  0 bytes
    0 input error
    0 packets output,  0 bytes
    0 output error
```

The output of the command on Nortel 2 is as follows:

```
 [Nortel2] display interface Tunnel 1/0/0
Tunnel1/0/0 current state : UP
Line protocol current state : UP
Description : Nortel Series, Tunnel1/0/0 Interface
The Maximum Transmit Unit is 1000 bytes
Internet Address is 21.1.1.1/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 2.2.2.2 (LoopBack1), destination 1.1.1.1
Tunnel protocol/transport GRE/IP , key disabled
linkalive disabled
Checksumming of packets disabled
QoS max-bandwidth : 64 Kbps
Output queue : (Urgent queue : Size/Length/Discards)  0/50/0
Output queue : (Protocol queue : Size/Length/Discards) 0/1000/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/256/0
    5 minutes input rate 0 bytes/sec, 0 packets/sec
    5 minutes output rate 0 bytes/sec, 0 packets/sec
    0 packets input,  0 bytes
    0 input error
    0 packets output,  0 bytes
0 output error
```

From the preceding output, you can see that Nortel 1 uses the GRE key with the key number 2; while Nortel 2 does not use a GRE key.

Perform one of the following configurations to remove the fault:

- Use the **undo gre key** command on Nortel 1 to disable the GRE key.
- Use the **gre key2** command on Nortel 2 to enable the GRE key.

If you cannot remove the fault, run the **display this** command in the interface view on both ends of the tunnel to view the IP addresses of the two ends.

The display on Nortel 1 is as follows:

```
#
interface Tunnel1/0/0
 ip address 11.1.1.1 255.255.255.0
 source LoopBack1
 destination 2.2.2.2
 gre key 2
 mtu 1000
#
```

The display on Nortel 2 is as follows:

```
#
interface Tunnel1/0/0
 ip address 21.1.1.1 255.255.255.0
 source LoopBack1
 destination 1.1.1.1
 gre key 2
#
```

From the preceding display, you can see that the IP addresses of both ends are 24-bit. They IP addresses are not in the same network segment: one is 11.1.1.1 and the other is 21.1.1.1.

Use the **display fib** command on both ends to check whether the route to the peer Tunnel 1/0/0 is configured on both ends.

The display on Nortel 1 is as follows:

```
FIB Table:
 Total number of Routes : 11

Destination/Mask   Nexthop         Flag TimeStamp     Interface       TunnelID
127.0.0.1/32       127.0.0.1       HU   t[138]        InLoop0         0x0
127.0.0.0/8        127.0.0.1       U    t[138]        InLoop0         0x0
1.1.1.1/32         127.0.0.1       HU   t[140437]     InLoop0         0x0
172.2.6.1/32       127.0.0.1       HU   t[407843]     InLoop0         0x0
172.2.6.0/24       172.2.6.1       U    t[407843]     Eth4/2/0        0x0
172.2.4.0/24       172.2.6.2       DGU  t[442303]     Eth4/2/0        0x0
2.2.2.2/32         172.2.6.2       DGHU t[442303]     Eth4/2/0        0x0
11.1.1.1/32        127.0.0.1       HU   t[494003]     InLoop0         0x0
11.1.1.0/24        11.1.1.1        U    t[494003]     Tun1/0/0        0x0
```

The display on Nortel 2 is as follows:

```
FIB Table:
 Total number of Routes : 13

Destination/Mask   Nexthop         Flag TimeStamp     Interface       Token
127.0.0.1/32       127.0.0.1       HU   t[0]          InLoop0         0x0
127.0.0.0/8        127.0.0.1       U    t[0]          InLoop0         0x0
172.2.4.1/32       127.0.0.1       HU   t[0]          InLoop0         0x0
21.1.1.1/32        127.0.0.1       HU   t[0]          InLoop0         0x0
2.2.2.2/32         127.0.0.1       HU   t[0]          InLoop0         0x0
172.2.4.0/24       172.2.4.1       U    t[0]          Eth3/2/0        0x0
172.2.6.0/24       172.2.4.2       DGU  t[0]          Eth3/2/0        0x0
1.1.1.1/32         172.2.4.2       DGHU t[0]          Eth3/2/0        0x0
```

From the preceding display, you can see that no route to the remote tunnel interface is configured on both ends. Therefore, configure the route to peer Tunnel 1/0/0 on both ends:

- Configure **ip route-static 21.1.1.0 24 tunnel 1/0/0** on Nortel 1.
- Configure **ip route-static 11.1.1.0 24 tunnel 1/0/0** on Nortel 2.

After you complete the configuration, on both Nortel 1 and Nortel 2, ping their peer Tunnel 1/0/0 separately and receive the response packets. A GRE tunnel establishes normally.

If the fault persists after the preceding configuration, contact Nortel technical personnel.

Troubleshooting procedure

Step 1 Check that the GRE keys are consistent on both ends of the tunnel interface.

Step 2 Check that the route to the peer tunnel interface is configured on both ends.

----End

Summary

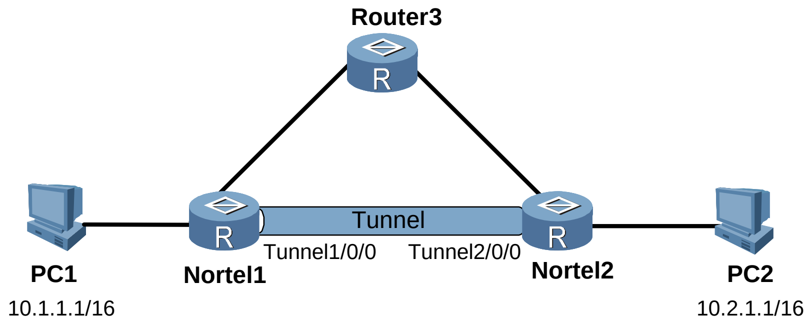
Because the network layer protocols of the tunnel interfaces on both ends of the GRE tunnel are up does not guarantee that the GRE tunnel is configured correctly. Two additional requirements exist:

- The GRE keys on both ends are consistent.
- The route to the peer tunnel interface is configured on both ends.

2.3.2 PCs cannot ping through each other although tunnel interfaces on two ends can ping each other successfully

Fault symptom

Figure 2-6 Networking diagram of the GRE troubleshooting II



In Figure 2-6, the interfaces on both ends of the tunnel are configured correctly and they can ping each other successfully. However, PC1 and PC2 cannot ping through each other.

Fault analysis

The possible causes are:

- No route to PC1 exists on Nortel 1.
- No route to PC2 exists on Nortel 2.
- PC1 does not specify Nortel 1 as its default gateway.
- PC2 does not specify Nortel 2 as its default gateway.

Use the **display ip routing-table** command on Nortel 1 and Nortel 2 to view:

- Whether a route passes through Tunnel 1/0/0 to 10.2.0.0/16 on Nortel 1.
- Whether a route passes through Tunnel 2/0/0 to 10.1.0.0/16 on Nortel 2.

If the two routes do not exist, use the **ip route-static** command in the system view to configure them.

For example, on Nortel 1, the configuration command is [Nortel1] **ip route-static 10.2.0.0 255.255.0.0 tunnel 1/0/0**.

After you complete the configuration, ping the peer tunnel on Nortel 1 and Nortel 2 to receive the response packets.

If the PCs cannot ping through each other, check that PC1 specifies Nortel 1 as the default gateway and PC2 specifies Nortel 2 as the default gateway.

Troubleshooting procedure

Step 1 Check that a route passes through Tunnel 1/0/0 to 10.2.0.0/16 on Nortel 1.

Step 2 Check that a route passes through Tunnel 2/0/0 to 10.1.0.0/16 on Nortel 2.

Step 3 Check that PC1 specifies Nortel 1 as its default gateway.

Step 4 Check that PC2 specifies Nortel 2 as its default gateway.

----End

Summary

To ensure that the GRE encapsulated packet forwards normally, routes must pass through the tunnel on both the source router and the destination router.

2.4 FAQs

Q: The system supports specifying the source address of the tunnel by using the source interface. When I use this method, the tunnel status is not up. After running the display this interface command in the interface view, I find that the tunnel source is 0.0.0.0. Why?

A: The cause is that no IP address is specified for the tunnel source interface.

Assign an IP address for the source interface and specify this interface as the source address of the tunnel.

Q: Why is the tunnel status not up after completing these steps: following the sequence of configuring an IP address for the tunnel, specifying IP addresses for the source and destination, and specifying the IP address for the source interface while configuring a tunnel?

A: The possible cause is that two tunnels are established by using the same source and destination addresses.

One tunnel uses the IP address as the tunnel source address and the other uses the source interface as the tunnel source address. In this case, if an IP address is specified for the source interface, only the status of the tunnel that uses the source interface is up, whereas the status of the tunnel that uses the IP address cannot be up. To resolve this, specify different source and destination addresses.

Q: Why is the tunnel source interface found to be another interface when the display this interface command is run in the interface view? This happens when specifying an IP address as the tunnel source address, and this IP address belongs to some source interface.

A: The reason is that after tunnel configuration, the IP address assigned for the tunnel source is transferred to another interface.

After the tunnel detects that the source interface where its source address is located has changed, it updates the source interface of the tunnel source.

Q: Why is the status of the tunnel still down after the IP address, source address, and destination address are specified for the tunnel?

A: To change the tunnel status to up, the following conditions must be met:

- An IP address is assigned for the tunnel interface.
- The source and destination addresses are specified.
- Reachable routes exist between the source and destination addresses.

If the status of the tunnel is down even after you meet all three conditions, check for reachable routes between the source and destination addresses. If no reachable routes exist, use the **ip route-static** command to configure a static route or run a dynamic routing protocol to allow reachable routes between the source and destination addresses of the tunnel.

Q: Why can I not ping the IP address of the remote tunnel interface? All the configurations are complete, a reachable route exists between the source and destination addresses, and the tunnel is up.

A: The possible causes are as follows:

- The IP addresses of the tunnel interfaces on two ends are not in the same network segment.
- The GRE keys on the two ends are inconsistent. If only one end is configured with the GRE key or the key-numbers of two ends are different, the fault occurs.

Q: Why does the ping fail even after I configure a multilayer embedding tunnel?

A: A tunnel supports up to three-layer embedding. If this specification is exceeded, the ping will fail. Check the tunnel layers.

Q: Suppose three routers exist: Router A, Router B, and Router C. Router A and Router B directly connect; Router B and Router C directly connect; I need a tunnel between Router A and Router C. In this case, what configurations should be performed to establish the tunnel successfully?

A: You need to perform the following configurations:

- First, complete the interface configuration on Router A, Router B, and Router C, and create a tunnel interface on both Router A and Router C.
- On Router A, specify the physical interface of Router A that connects with Router B as the tunnel source interface and specify the physical interface of Router C that connects with Router B as the tunnel destination address.

- On Router C, specify the physical interface of Router C that connects with Router B as the tunnel source interface; specify the physical interface of Router A that connects with Router B as the tunnel destination interface.
- Configure a static route from Router A to Router C and from Router C to Router A.

You can set up a tunnel that spans multiple routers using the preceding method.

Q: Why do packets not forward correctly even after a GRE tunnel establishes successfully?

A: The source router and the destination router must use the routes that are forwarded by the tunnel. Only packets with GRE encapsulation forward correctly.

You can configure a static route or a dynamic routing protocol that is required on both ends of the tunnel.

You can use the **ip route-static** *dest-ip-address* { *mask* | *mask-length* } **tunnel** *tunnel-number* command to configure a static route. *dest-ip-address* is not the IP address of the tunnel destination interface but the destination address of the packet prior to GRE encapsulation. The outgoing interface must be the local tunnel interface, with the next hop as the address of the remote tunnel interface.

If you choose to configure a routing protocol, you must enable it on the tunnel interface and on the router interface that connects with the private network. To ensure that a correct route is chosen, do not configure the next hop of the route to the physical address of the tunnel destination as the tunnel interface.

2.5 Diagnostic tools

2.5.1 display commands

Command	Description
display this	Displays the basic configuration of this tunnel. Run this command in the tunnel interface view.
display this interface	Displays information on this tunnel interface. Run this command in the tunnel interface view.
display fib	Displays information on the FIB.

display this

```
[Nortel-Tunnel4/0/0] display this
#
interface Tunnel4/0/0
 ip address 2.2.2.2 255.255.255.0
 source Ethernet3/2/0
 destination 192.168.1.1
 gre key 10
 gre checksum
#
```

```
Return
```

Table 2-1 Description of the **display this** command output

Item	Description
ip address 2.2.2.2 255.255.255.0	The IP address of the tunnel interface is 2.2.2.2 and the mask is 255.255.255.0.
source Ethernet3/2/0	The source interface of the tunnel interface is Ethernet 3/2/0.
destination 192.168.1.1	The destination address of the tunnel interface is 192.168.1.1.
gre key 10	The key number of the tunnel interface is 10.
gre checksum	Checksum is enabled on the tunnel interface.

display this interface

```
[Nortel-Tunnel1/0/0] display this interface
Tunnel1/0/0 current state : UP
Line protocol current state : UP
Description : Nortel Series, Tunnel1/0/0 Interface, Route Port
The Maximum Transmit Unit is 1500 bytes
Internet Address is 30.1.1.2/24
Encapsulation is TUNNEL, loopback not set
Tunnel source 100.1.1.1 (Serial1/0/0), destination 100.1.1.2
Tunnel protocol/transport GRE/IP , key disabled
Checksumming of packets disabled
QoS max-bandwidth : 64 Kbps
Output queue : (Urgent queue : Size/Length/Discards)  0/50/0
Output queue : (Protocol queue : Size/Length/Discards) 0/1000/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
    5 minutes input rate 0 bytes/sec, 0 packets/sec
    5 minutes output rate 0 bytes/sec, 0 packets/sec
    0 packets input,  0 bytes
    0 input error
    0 packets output,  0 bytes
    0 output error
```

Table 2-2 Description of the **display this interface** command output

Item	Description
Tunnel1/0/0 current state : UP	The status of the tunnel interface is Up.
Line protocol current state : UP	The protocol status of the tunnel interface is Up.
The Maximum Transmit Unit is 1500 bytes	The MTU of the tunnel interface is 1500 bytes.
Internet Address is 30.1.1.2/24	The IP address of the tunnel interface is 30.1.1.2. The mask is 24-bit, namely, 255.255.255.0.

Item	Description
Tunnel source 100.1.1.1 (Serial1/0/0), destination 100.1.1.2	The source address of the tunnel interface is 100.1.1.1 (source interface is Serial 1/0/0) and the destination address is 100.1.1.2.
Tunnel protocol/transport GRE/IP , key disabled	The tunnel protocol is GRE. The network layer protocol is IP. The GRE key is disabled on the tunnel interface.
Checksumming of packets disabled	Checksum of the packet is disabled on the tunnel interface.
QoS max-bandwidth : 64 Kbps	The maximum bandwidth of the tunnel interface is 64 Kb/s.

display fib

```
<Nortel> display fib
 FIB Table:
 Total number of Routes : 8
Destination/Mask   Nexthop         Flag TimeStamp     Interface       Token
127.0.0.1/32       127.0.0.1       HU   t[0]          InLoop0         0x0
127.0.0.0/8        127.0.0.1       U    t[0]          InLoop0         0x0
1.1.1.3/32         127.0.0.1       HU   t[0]          InLoop0         0x0
1.1.1.0/24         1.1.1.3         U    t[0]          Eth3/1/0        0x0
192.168.1.3/32     127.0.0.1       HU   t[0]          InLoop0         0x0
192.168.1.0/24     192.168.1.3     U    t[0]          Eth3/2/0        0x0
2.2.2.2/32         127.0.0.1       HU   t[0]          InLoop0         0x0
2.2.2.0/24         2.2.2.2         U    t[0]          Tun4/0/0        0x0
```

Use the **display fib** command to check the reachability of other interfaces of the router.

When the status of this tunnel is down, you can use the **display fib** command to check for a reachable route between the source and the destination addresses of the tunnel.

2.5.2 debugging commands

Command	Description
debugging tunnel	Displays the debug information on the tunnel.
debugging ip packet acl	Displays information on packets that match access control list rules.
debugging ip icmp	Displays information on ping packets.

debugging tunnel

Use the output of the **debugging tunnel** command as an example.

```
*0.93688561 PE TUNNEL/8/ATKDBG:Slot=2;Tunnel2/0/0-Out: Mbuf length = 84 from GRE Tunnel
out
```

The preceding information shows the tunnel interface (Tunnel2/0/0) on which packets are encapsulated as well as the packet length.

```
*0.93688656 PE TUNNEL/8/ATKDBG:Slot=2;Tunnel2/0/0-Out: GRE/IP encapsulated
192.168.1.3->192.168.1.2(len = 108).
```

The preceding information shows the source and the destination addresses in the IP header of the encapsulated packet.

```
*0.93688784 PE TUNNEL/8/ATKDBG:Slot=2;Tunnel-In: Get packet,the tunnel is
src(192.168.1.2)/dest(192.168.1.3),length = 108 .
*0.93688928 PE TUNNEL/8/ATKDBG:Slot=2;
    Judge keepalive finished. NOT keepalive packet.
```

The preceding information shows the IP address resolved from the response packet and the packet length.

```
(4) Reply from 1.1.1.2: bytes=56 Sequence=2 ttl=255 time=4 ms
```

The preceding information shows that the response is received from the remote tunnel interface. Parameters of the packet are also shown.

```
(5)*0.93689024 PE TUNNEL/8/ATKDBG:Slot=2;Tunnel-In: Enter Tunnel Input and GRE mode
found.
```

The preceding information shows that received packets are sent to the tunnel-input queue.

```
(6)*0.93689120 PE TUNNEL/8/ATKDBG:Slot=2;Tunnel2/0/0-In: GRE decapsulated IP
1.1.1.2->1.1.1.3(len = 84).
```

The preceding information shows that packets are resolved, with the tunnel IP address removed from the GRE header.

debugging ip packet acl

The display of the **debugging ip packet acl** command is as follows:

```
*0.94698304 PE IP/8/debug_case:Slot=2;
Sending, interface = Tunnel2/0/0, version = 4, headlen = 20, tos = 0,
pktlen = 84, pktid = 9490, offset = 0, ttl = 255, protocol = 1,
checksum = 37520, s = 1.1.1.3, d = 1.1.1.2
prompt: Sending the packet from local at Tunnel2/0/0
*0.94698640 PE IP/8/debug_case:
Delivering, interface = Tunnel2/0/0, version = 4, headlen = 20, tos = 0,
pktlen = 84, pktid = 36363, offset = 0, ttl = 255, protocol = 1,
checksum = 10647, s = 1.1.1.2, d = 1.1.1.3
prompt: IP packet is delivering up!
```

The output contains packets that match access control list (ACL) rules.

NOTE

The ACL rules used in this example are:

#

acl number 3001

rule 5 permit ip source 1.1.1.2 0 destination 1.1.1.3 0

rule 10 permit ip source 1.1.1.3 0 destination 1.1.1.2 0

2.5.3 Alarms

Item	Description
Alarm message	Same tunnel exist
Meaning	The same tunnel exists.
Possible cause	With the same source and the destination address, only one tunnel can establish. You cannot configure the same source and destination address on different tunnel interfaces encapsulated with the same protocol. The source and the destination address identify a tunnel uniquely.
Solution	Use the other source address or destination address.

Contents

Figures

3 BGP/MPLS IP VPN troubleshooting

About this chapter

The following table describes the contents of this chapter.

Section	Describes
3.1 BGP/MPLS IP VPN overview	This section describes the knowledge you need before you troubleshoot the Border Gateway Protocol (BGP)/Multiprotocol Label Switching (MPLS) IP virtual private network (VPN).
3.2 MPLS L3VPN troubleshooting	This section provides notes about configuring MPLS Layer 3VPN, the MPLS Layer 3 VPN troubleshooting flowchart, and the troubleshooting procedure in a typical MPLS Layer 3 VPN Network.
3.3 Troubleshooting cases	This section presents several troubleshooting cases.
3.4 FAQs	This section lists frequently asked questions and their answers.
3.5 Diagnostic tools	This section describes common diagnostic tools: **display** commands, **debugging** commands, alarms, and logs.

3.1 BGP/MPLS IP VPN overview

This section covers the following topics:

- Introduction to VPN
- Network topology
- Operation model

3.1.1 Introduction to VPN

A public network is a set of uncorrelated systems that can exchange information freely with each other. A private network is owned and managed by a single organization, formed by a group of devices that share information.

In a private network, different sites use a dedicated leased line to realize interconnection, ensuring that the connection between sites is exclusive. A private network is used only by the enterprise that deploys it.

Though a single VPN service model can simplify network operations, it cannot meet the requirements of various customers. Customer requirements can differ in such aspects such as: security, number of sites, number of users, route complexity, key application, traffic model, traffic volume, experience in network operation, and the willingness to outsource network services. To address the requirements, service operators must offer a series of services, including diversifying VPN service models.

The following multiple VPN service models exist:

- Traditional VPN
- Frame relay (Layer 2)
- Asynchronous Transfer Mode (ATM) (Layer 2)
- Customer premise equipment (CPE)-based VPN
- Layer 2 Tunneling Protocol (L2TP) and Point-to-Point Tunneling Protocol (PPTP) (Layer 2)
- IPsec (Layer 3)
- VPN deployed by service providers
- MPLS Layer 2 VPN (Layer 2)
- BGP/MPLS IP VPN or RFC2547bis (Layer 3)

RFC2547bis defines a mechanism, which allows service providers to use their own IP backbone to provide VPN services. This mechanism is called BGP/MPLS VPNs where BGP transfers VPN routing information from one site to another and MPLS establishes a tunnel that carries traffic from one provider edge (PE) to another on the backbone network.

3.1.2 Network topology

Figure 3-1 BGP/MPLS VPN network topology

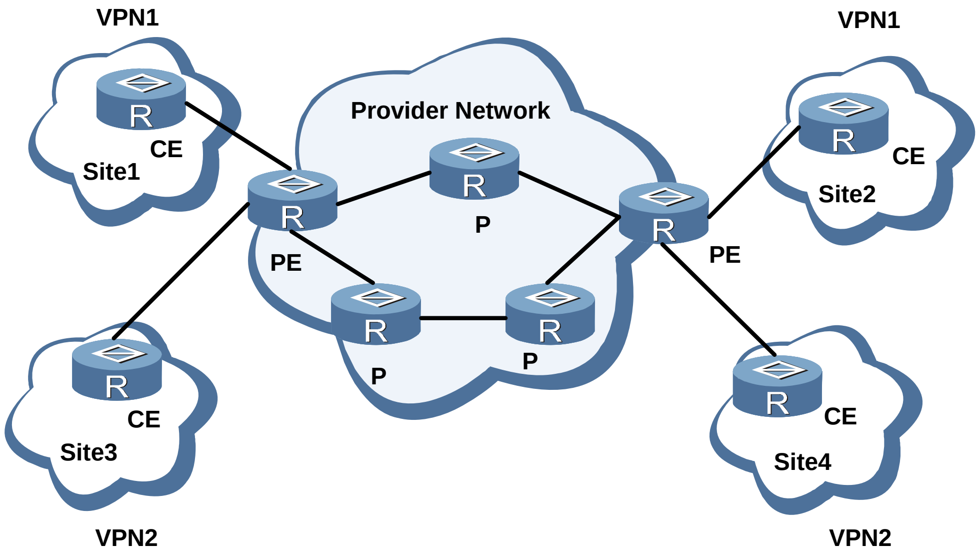


Figure 3-1 shows a basic BGP/MPLS VPN network topology. In a basic BGP/MPLS VPN network topology, the customer edge (CE) can be a host, switch, or router. An adjacency establishes between the CE and its directly-connected PE. The CE sends its VPN routes to the PE and learns remote VPN routes from the PE.

The PE exchanges routing information with the CE through a static route, Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (IS-IS) or Exterior BGP (EBGP). Every PE router maintains a VPN routing and forwarding (VRF) table for every directly-connected site. A PE router can maintain multiple VRFs. You can associate a VRF with multiple interfaces. After learning local VPN routes from local CEs, the PE router exchanges them with other peer PEs using Interior BGP (IBGP).

The provider router (P) is a router that exists in the operator network that does not directly connect with the CE. The P acts as an MPLS Label Switching Router (LSR), used to forward VPN traffic between PEs. Because the MPLS backbone uses a two-level label stack, the P only needs to maintain the routes to the PE rather than VPN routing information.

3.1.3 Operation model

The BGP/MPLS VPN uses two types of communication traffic:

- Control traffic: traffic used to distribute and switch VPN routes, and establish label switch paths
- Data traffic: data traffic of users

The process to forward BGP/MPLS VPN traffic is as follows:

- Routing information exchange
- LSP
- Forward data traffic

Figure 3-2 BGP/MPLS VPN instances

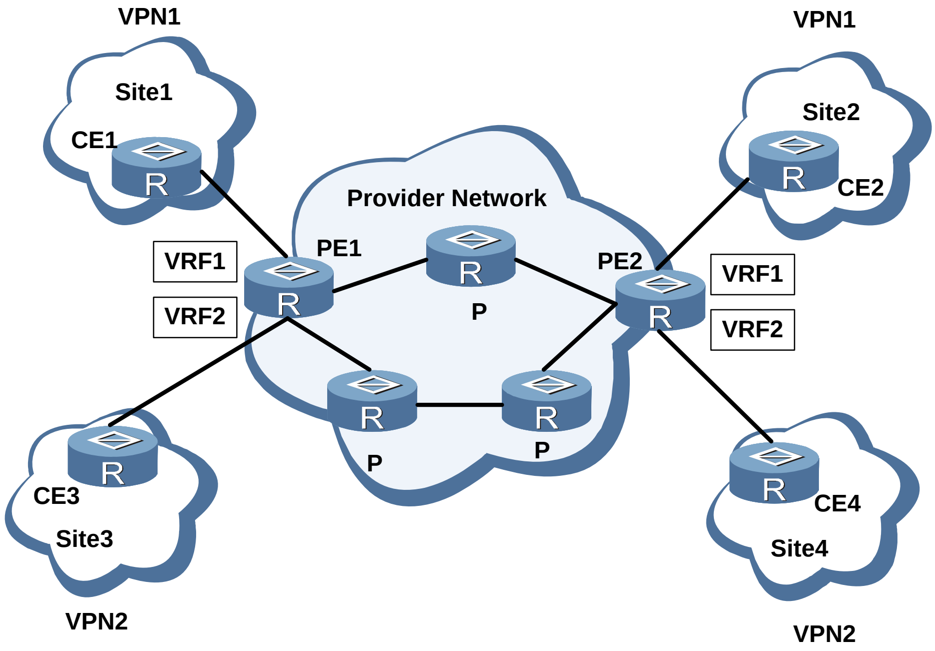


Figure 3-2 shows a BGP/MPLS VPN topology. In a basic BGP/MPLS VPN network topology, a service operator provides BGP/MPLS VPN service to multiple enterprises. Two PEs connect with four different customer sites.

Routing information exchange

As shown in Figure 3-2, the CE1-bound interface or subinterface on PE1 is associated with VRF1. When CE1 advertises the route with the prefix of 10.1.0.0/16 to PE1, PE1 adds this route to VRF1.

The PE1 marks 10.1.0.0/16 with the private and public label successively, and sends it to PE2.

The PEs uses Multiple Protocol IBGP (MP-IBGP) to carry VPN Target (VT) and Route Distinguisher (RD) information and use the loopback address as the next hop of the IBGP route. This process resolves the problem of the repeated address realm and simplifies the route filtering.

By using the RD and VPN-IPv4 address family (defined in RFC 1918), RFC2547bis supports the overlapping address space. By using the technique of BGP extension attribute-based filtering, RFC2547bis implements forced route exchange between PE routers.

Upon receiving the routing information from PE1, PE2 filters it according to the existing BGP extension attribute. The PE2 also determines whether to add the 10.1.0.0/16 route to VRF1. Once the 10.1.0.0/16 route is added to VRF1, PE2 will advertise it to CE2.

LSP establishment

To transfer VPN routes transparently from one PE to another, you can use the Label Distribution Protocol (LDP) or Reservation Protocol (RSVP) to establish LSPs on the network of the service operator. To ensure interoperation between devices from different vendors, all PE and P routers should support LDP. The LSP based on LDP and that based on RSVP establish between a pair of PE routers. You can establish one LSP or multiple parallel LSPs between PE routers. The LSPs can implement a variety of Quality of Service (QoS) functions through configuration.

Forward data traffic

Use Figure 3-2 as an example. If Site 2 has the host (10.2.3.4/16), CE2 performs the longest-match on the destination IP address and forwards packets to PE2.

The MPLS uses two layers of labels to forward packets from PE2 to PE1.

For this data stream, PE2 is the ingress LSR of the LSP, and PE1 is the egress LSR of the LSP.

The PE2 pushes a label (109569, for example) into the label stack, which serves as the inner label before transmission of packets.

PE1 distributes routing information to the 10.1.0.0/16 segment by using IBGP. When PE2 receives the routing information, label 109569 is allocated to VRF1.

The PE2 pushes the original MPLS label from the next hop (the P router) to the label stack, which will make it act as the outer label.

After the label enters the stack and once PE2 receives packets, PE2 searches for routes in VRF1. The following information can be obtained:

- Private network label distributed by PE1 (with the label value being 109569)
- BGP next hop of the route (loopback address of PE1)
- Egress interface (or subinterface) of the LSP from PE2 to PE1
- Original MPLS label from PE2 to PE1

Along the LSP, PE2 forwards MPLS packets from the egress interface to the first P. The P router exchanges packets based on the outer label. The penultimate P pops the outer label and forwards packets to the PE1.

After receiving packets, based on the inner label 109596, the PE1 identifies the next hop to the 10.1/16 segment is the directly connected CE1. The PE1 forwards IPv4 packets to CE1. The CE1 then forwards them to the server 10.1.3.8/16 of Site 1.

3.2 MPLS L3VPN troubleshooting

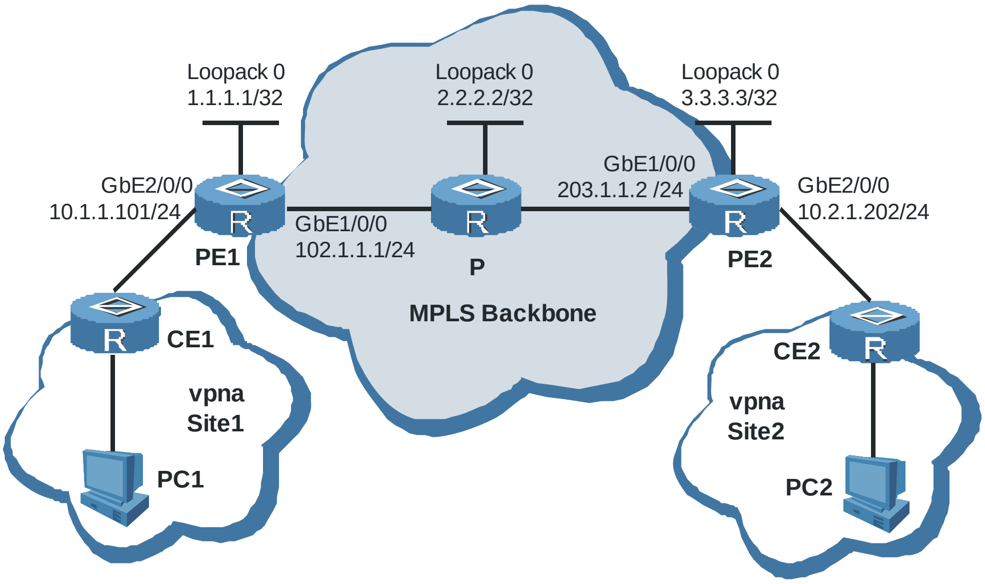
This section covers the following topics:

- Typical networking
- Configuration notes
- Troubleshooting flowchart
- Troubleshooting procedure

3.2.1 Typical networking

Figure 3-3 shows a typical MPLS L3VPN networking. Consider this networking to discuss MPLS L3VPN troubleshooting as follows:

Figure 3-3 BGP/MPLS VPN networking



In Figure 3-3, the following solution is used:

- CE1 and PC1 belong to Site 1 of vpna; CE2 and PC2 belong to Site 2 of vpna.
- EBGP connections are used between PE1 and CE1, and between PE2 and CE2.
- An IBGP adjacency establishes between PE1 and PE2 to transfer VPNv4 routing information that contains inner labels.
- Both MPLS and LDP are enabled on PE1, P, and PE2.

3.2.2 Configuration notes

Item	Subitem	Notes
VPN instance	Route distinguisher	The local route distinguisher (RD) is used to distinguish routes of different VPN instances.
	Export VPN target	The export VPN target marks the attributes of exported routes, which must be consistent with the import VPN target of the remote PE.
	Import VPN target	The import VPN target marks the attributes of imported routes, which must be consistent with the export VPN target of the remote PE.
	Binding VPNs and interfaces	The binding of VPNs and interfaces must be configured in the view of the interface that connects to CE. After the interface is bound with VPN, the configuration of the network layer, for example, IP addresses, are deleted.

Item	Subitem	Notes
MPLS	LSR-ID	LSR ID is similar to router ID. An LSR ID specifies an address. LDP, by default, uses this address to establish LDP sessions, The reachability to the LSR ID must be ensured. Two ways exist to configure an LSR ID. ● Generally, the LSR ID is the address of the loopback interface. ● If the **mpls ldp transport-address** command is configured on the interface that connects to the public network, LDP uses the address specified by this command to establish an LDP session.
	MPLS	Enable MPLS in the system view and on the interface that connects with the public network. You must configure the policy to trigger the setup of LSPs in the MPLS view.
	LDP	Enable LDP in the system view and on the interface that connects with the public network.
BGP	AS	-
	IBGP	Specify the remote PE as the local IBGP peer in the BGP view.
	The interface used by BGP connections	Specify the loopback interface (with a 32-bit mask) as the egress interface of the session that is used to set up an IBGP connection between PEs.
	VPNv4 address family	The IBGP peer must be enabled in VPNv4 address family.
	VPN instances of IPv4 address family	Specify the directly connected CE as the EBGP peer. Import the routes of the network segment between PE and CE to BGP.

Use PE1 as an example to explain configuration notes for MPLS L3VPN.

NOTE

The following section covers only the commands related to MPLS L3VPN. For details about the configuration, see *Nortel Secure Router 8000 Series Configuration Guide - VPN* (NN46240-507).

1. Configuration concerning VPN instances

# Create a VPN instance:

```
[PE1] ip vpn-instance vpna
```

# Specify an RD:

```
[PE1-vpn-instance-vpna] route-distinguisher 100:101
```

# Specify the export VPN target, which must be consistent with the import VPN target of the peer PE:

```
[PE1-vpn-instance-vpna] vpn-target 100:1 export-extcommunity
```

# Specify the import VPN target, which must be consistent with the export VPN target of the peer PE:

```
[PE1-vpn-instance-vpna] vpn-target 100:1 import-extcommunity
```

# Bind the CE-bound interface with the VPN instance. After the binding, the interface belongs to this VPN, and its address is visible only in this VPN and in its interactive VPNs:

```
[PE1] interface gigabitethernet 2/0/0
[PE1-GigabitEthernet2/0/0] ip binding vpn-instance vpna
```

# Assign a private IP address for the interface:

```
[PE1-GigabitEthernet2/0/0] ip address 10.1.1.101 255.255.255.0
```

2. MPLS capability configuration

# Configure an LSR ID:

```
[PE1] mpls lsr-id 1.1.1.1
```

# Globally enable MPLS:

```
[PE1] mpls
```

# Configure a policy for triggering the setup of LSPs. You can specify ACL or other parameters to restrict the triggering. In this scenario, you can use the parameter all for the sake of simplicity:

```
[PE1-mpls] lsp-trigger all
```

# Globally enable MPLS LDP:

```
[PE1] mpls ldp
```

# Enable MPLS on the interface that connects with the public network:

```
[PE1] interface gigabitethernet 1/0/0
[PE1-GigabitEthernet1/0/0] mpls
```

# Enable MPLS LDP on the interface that connects with the public network:

```
[PE1-GigabitEthernet1/0/0] mpls ldp
```

3. Configuration concerning BGP

# Add PE to AS 100. Specify the same AS for PE1, P, and PE2:

```
[PE1] bgp 100
```

# Configure a BGP peer for PE:

```
[PE1-bgp] peer 3.3.3.3 as-number 100
```

# Specify the loopback interface as the interface used to set up BGP Peer (TCP) connections with the peer PE:

```
[PE1-bgp] peer 3.3.3.3 connect-interface loopback 0
```

# Receive VPNv4 routes according to the VPN target policy. This is a default setting:

```
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpnv4] policy vpn-target
```

# Enable EBGP peer in VPNv4 address family:

```
[PE1-bgp-af-vpnv4] peer 3.3.3.3 enable
```

NOTE

VPNv4 routes can transport only after an EBGP peer is established in VPNv4 address family. You can view all VPNv4 BGP peers by using the **display bgp vpnv4 all peer** command.

# Import routes of the directly connected network segment between PE and CE to vpna:

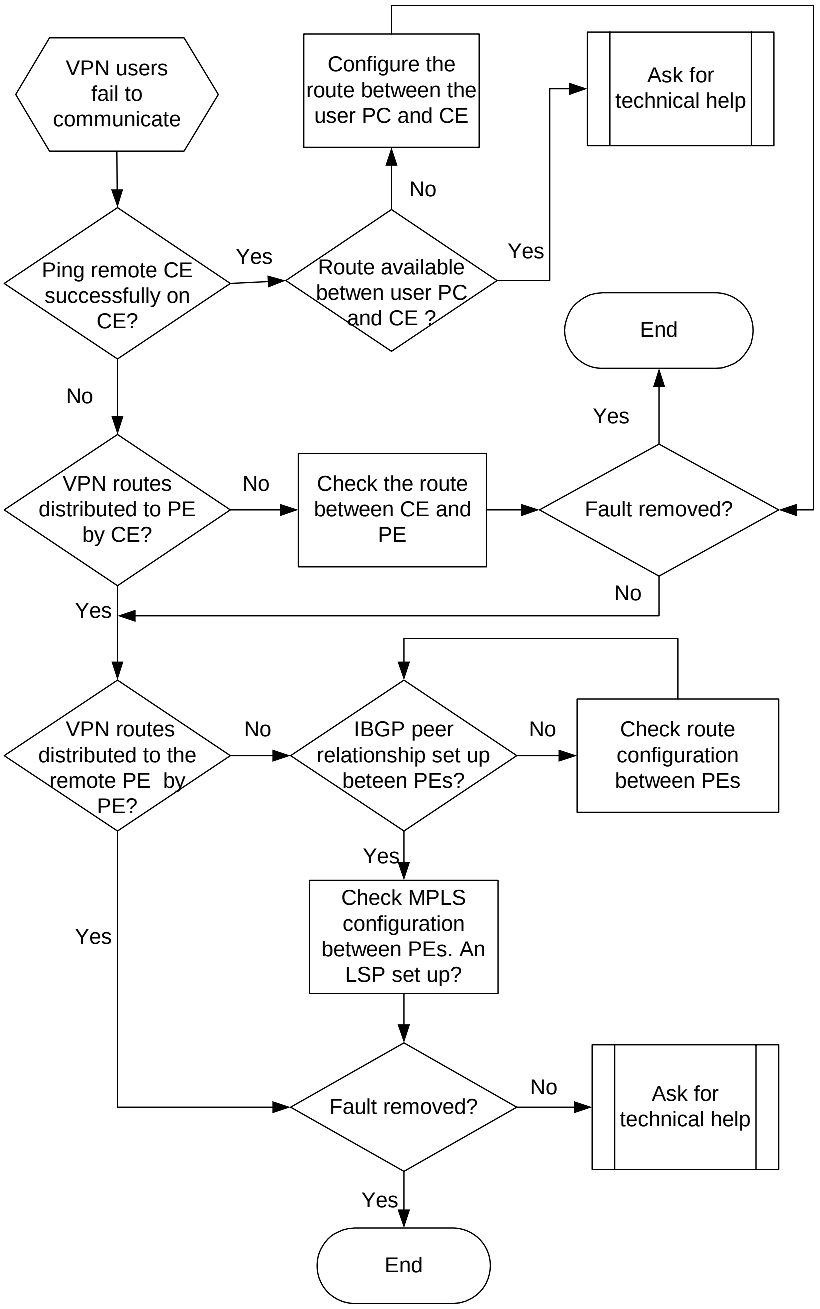
```
[PE1-bgp] ipv4-family vpn-instance vpna
[PE1-bgp-vpna] import-route direct
```

3.2.3 Troubleshooting flowchart

After configuration on respective routers shown in Figure 3-3, VPN users PC1 and PC2 cannot exchange information with each other.

Troubleshoot the network according to the flowchart shown in Figure 3-4.

Figure 3-4 MPLS VPN troubleshooting flowchart


VPN users fail to communicate
Configure the route between the user PC and CE
Ask for technical help
Ping remote CE successfully on CE?
Yes
Route available betwen user PC and CE ?
No
Yes
End
No
Yes
VPN routes distributed to PE by CE?
No
Check the route between CE and PE
Fault removed?
No
Yes
VPN routes distributed to the remote PE by PE?
No
IBGP peer relationship set up beteen PEs?
No
Check route configuration between PEs
Yes
Check MPLS configuration between PEs. An LSP set up?
Yes
Fault removed?
No
Ask for technical help
Yes
End

3.2.4 Troubleshooting procedure

The steps of troubleshooting are as follows:

Step 1 Check that reachable routes exist between CEs.

On the local CE, ping the remote CE.

- If the ping is successful, it indicates that reachable routes exist between CEs and rules out the route problem between CEs. The section between VPN user PCs and CE can be faulty. Check for reachable routes between them. If no reachable route is available, add the route.

If reachable routes exist between them, and the ping fails, contact Nortel technical support engineers for technical assistance.

- If the ping fails, use the **display ip routing-table** command on the local CE to view whether routes to the remote CE exist in the local routing table. Use the **display ip routing-table** command on the remote CE to view whether routes to the local CE exist. If the two CEs have no routes to each other, or only the local CE has routes to the remote CE but the remote CE has no routes to the local CE, it indicates a route problem between CEs. Go to Step 2.

NOTE

After you check that CE and its directly connected PE can ping each other successfully, use the **ping-vpn-instance** *vpn-instance-name* **-a** *source-ip-address dest-ip-address* command on this PE to check for reachable routes to the remote CE. *vpn-instance-name* is the name of the VPN to which CE belongs. *source-ip-address* is the IP address of the interface through which PE connects CE directly. *dest-ip-address* is the IP address of a specific interface on the remote CE.

Step 2 Check routes of various network segments between CEs.

Three network segments exist between CEs.

- From local CE to local PE
- From local PE to remote PE
- From remote PE to remote CE

For a route problem between the local CE and the local PE, and that between the remote PE and the remote CE, you can remove the fault according to the following step.

1. Check whether CE distributes the routing information to the directly connected PE.

   On PE, use the **display ip routing-table vpn-instance** *vpn-instance-name* command to view whether the VPN routing table holds the routing entries advertised from the directly connected CE.

NOTE

In this command, you must specify the parameter **vpn-instance** *vpn-instance-name* to display the routes within a specified VPN. If you do not specify the parameter, the command displays public network routes of PE.

If the VPN routing table on PE has no routes to CE, use the **display bgp vpnv4 all peer** command to check whether EBGP peers establish between PE and CE.

- If EBGP peers establish, check whether direct routes and inter-autonomous system (AS) routes import to the BGP routing table of CE. Check whether direct routes are imported in the VPN instance view of BGP IPv4 address family on PE.
- If no BGP peers are set up between PE and CE, check for a consistent AS number in BGP configuration on PE and CE. For details about troubleshooting, see *Nortel Secure Router 8000 Series Troubleshooting - IP Routing* (NN46240-706).

For a route problem between the local PE and the remote PE, perform the following step to isolate the fault.

2. Check whether private network routes on the local PE are distributed to the remote PE.

On the remote PE, use the **display ip routing-table vpn-instance** *vpn-instance-name* command to check for routes to the local CE.

- If routes to the local CE exist, use the **display ip routing-table vpn-instance** *vpn-instance-name* command on the local PE. If routes to the remote CE exist, it indicates that there is no route problem between PEs.
- If no routes to the local CE exist in the VPN routing table, use the **display bgp vpnv4 all peer** command to check whether BGP VPNv4 peers establish between PEs.

- If BGP VPNv4 peers establish between PEs, check whether VPN targets of the two PEs match. The export VPN target of the local PE must be consistent with the import VPN target of the remote PE. The import VPN target of local PE must be consistent with the export VPN target. If not, modify the configuration.
- If BGP VPNv4 peers do not establish between PEs, the possible cause can be failure to establish BGP peers between PEs. Use the **display bgp peer** command to view public network BGP peers of PE. For information about the public network route problem between PEs, see *Nortel Secure Router 8000 Series Troubleshooting* **-** *IP Routing* (NN46240-706).

NOTE

The VPNv4 routes between PEs are transferred by peers in the VPNv4 address family. The establishment of BGP VPNv4 peers depends on BGP peers in the public network.

CAUTION

Specify the loopback interface used for BGP connection when you configure IGBP neighbors. Use the **peer** *peer-ip-address* **connect-interface loopback** *interface-number* command to specify IBGP peers.

On PE, check VPN routes of the remote CE. If you specify the next hop, but not the loopback interface of the remote PE, the public network route cannot be associated with the LSP of the public network.

If BGP configuration is correct and all BGP peers establish correctly, but no routes to the remote CE are found by using the **display ip routing-table vpn-instance** command, the reason is that no LSP is established between PE and the next hop of the routes to the remote CE. This situation restricts the route from finding the associated LSP.

Use the **display ip routing-table vpn-instance** *vpn-name ip-address* [*mask* | *mask-length*] **verbose** command, and you can find that the value of the tunnel ID is 0x0. The following is an example:

```
<PE1> display ip routing-table vpn-instance vpna 10.2.1.202 32 verbose
Destination: 10.1.1.202/32
     Protocol: BGP            Process ID: 0
   Preference: 255                  Cost: 0
      NextHop: 3.3.3.3         Interface: NULL0
 RelayNextHop: 0.0.0.0         Neighbour: 3.3.3.3
        Label: 15360           Tunnel ID: 0x0
                            SecTunnel ID: 0x0
    BkNextHop: 0.0.0.0       BkInterface:
      BkLabel: NULL            Tunnel ID: 0x0
                            SecTunnel ID: 0x0
        State: Inactive Adv WaitQ     Age: 00h01m05s
          Tag: 0
```

Use the **display bgp vpnv4 all routing-table label** command on both the local PE and the remote PE to check whether the labels at both the ends match. The private network label assigned by the local PE is referred to as an incoming label for the local PE, and an outgoing label for the remote PE.

If they match, go to Step 3.

Step 3 Check that an LSP is established between PEs.

Network traffic on the MPLS VPN is transferred to the remote through LSPs on the public network. In actual configuration, the next hop of the private network route must be bound with the LSP.

- In case the LSPs are generated first, the binding can be queried against the tunnel management (TNLM) by the Routing Management (RM) according to the IP address of the next hop of the private network route.
- In the case that routes are learned first and then LSPs are generated, the TNLM notifies the RM of the destination IP address of the LSP. According to the IP address, the RM finds the associated private network route, and performs iteration.
- Therefore, check if an LSP establishes between PEs.
- Use the **display mpls lsp include** *ip-address mask* command on PE. In this command, *ip-address* is the IP address of the next hop of the private network route. If you find that the LSP that uses the next hop of the private network route as the destination is not set up, follow these steps.
- Verify that an LDP session establishes.

  Use the **display mpls ldp session** command to check whether an LDP session establishes.

  Common causes of failure to set up LDPs are as follows:

  - LSR ID configuration error: Remote PE cannot find the route to the LSR ID, leading to setup failure. Nortel recommends that you set the IP address of the loopback interface as the LSR ID. The IP address is advertised through the routing protocol and static route.
  - LSR ID configuration error and no **mpls ldp transport-address** configuration: If the **mpls ldp transport-address** command is not configured on the interface, PE will use the LSR ID to set up an LDP session with the remote PE. If the LSR ID is incorrect, the LDP session cannot establish successfully. To avoid this problem, run the **mpls ldp transport-address** command on the interface.
- Check that a TCP connection establishes for LDP sessions.

  Use the **display tcp status** command to view the TCP connection.

  If the routing information is correct, you can find that the TCP connection is already set up. The State in the output must be Established. If the TCP connection is not established, check for IP connectivity.
- Check that LDP parameters are consistent on both the ends of an LSP.

  LDP parameters must be consistent on both the ends of an LSP.

  If parameters are not consistent, for example, the label distribution mode is DOD on one end and DU on the other end, an LDP session fails to establish.
- Check that the policy to set up the LSP is configured.

  By default, a policy is adopted by which only the host address is triggered to set up LSP.

  To trigger all the routes to set up LSP, configure the **lsp-trigger all** command in MPLS.
- Check the status of interfaces enabled with MPLS LDP.

  Use the **display mpls interface** command and the **display mpls ldp interface** command to check whether the interfaces are Up or Active.

  If the status of the interface is Down or Inactive, use the **shutdown** command, and the **undo shutdown** command in the interface view. If the interface remains Down, check the physical link.

Check if the forwarding entry is correct on PE. Use the **display fib vpn-instance** *vpn-instance-name* command to view the forwarding information base (FIB) of the VPN on the Main Processing Unit (MPU).

For example:

```
<Nortel> display fib vpn-instance vpna
Destination/Mask   Nexthop         Flag TimeStamp     Interface       TunnelID
202.2.4.1/32       127.0.0.1         HU    t[172572]      InLoop0           0x6002000
202.2.4.0/24       202.2.4.1          U     t[172572]      GE4/0/0           0x6002000
```

NOTE
You can view the Tunnel ID by using the **display tunnel-info** command.

If the FIB entry exists only on the main control board but not the interface board, it indicates that IPC messages may be lost. In such scenarios, contact Nortel technical personnel.

----End

3.3 Troubleshooting cases

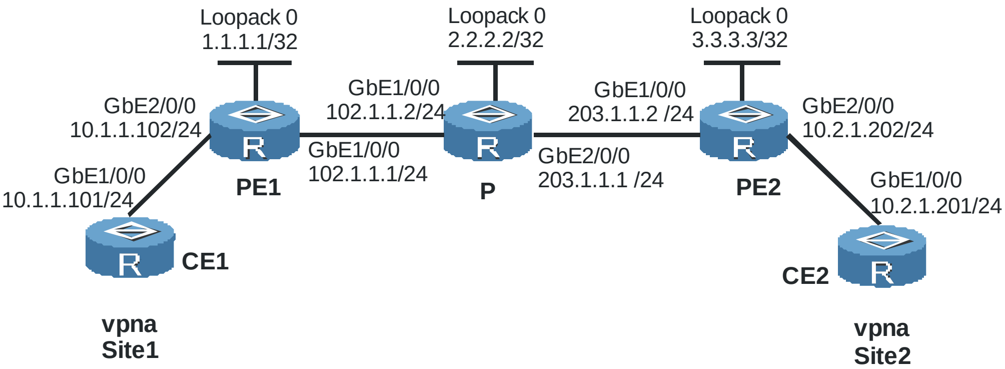
This section covers the following topics:

- PE fails to send private network routes to the remote CE
- CEs cannot communicate
- Failure to ping large packets of the private network
- PE cannot ping through the remote CE network segment
- Failure to establish the MP-EBGP peer in inter-AS VPN-OptionC

3.3.1 PE fails to send private network routes to the remote CE

Fault symptom

Figure 3-5 Networking diagram



In Figure 3-5, the following solution is adopted:

- EBGP runs between PE and CE.
- An IBGP adjacency establishes between PE1 and PE2 to transfer VPNv4 routing information that contains inner labels.

- An arbitrary IGP runs between PE1, P, and PE2 to transfer routing information of the public network.
- Both MPLS and MPLS LDP are enabled on PE1, P, and PE2 individually.

Fault symptoms: PE1 has the private network route sent from CE1 while PE2 and CE2 do not have this route.

Fault analysis

A public network tunnel is a necessity when private network traffic traverses the public network to the remote. Therefore, you must bind the next hop of the private network route with the LSP between PEs.

- In the case that LSPs are generated first, the binding between the routes and tunnels exists in TNLM. According to the IP address of the next hop of the private network route, RM can search TNLM for the binding.
- When routes are learned first and then LSP tunnels are generated, the TNLM notifies the RM related information such as the destination IP address of the LSP. According to the information, the RM finds the associated private network route and performs iteration.
- Use the **display ip routing-table vpn-instance** command on PE2. If no VPN routes appear, but the configuration is correct and BGP peers are set up correctly, the possible cause is that the LSP tunnel is not set up successfully.
- Use the **display ip routing-table vpn-instance** *vpn-instance-name ip-address* [*mask* | *mask-length*] **verbose** command on PE1 to view the tunnel ID of the LSP.

If the tunnel ID is 0x0, it indicates that the route to *ip-address* does not find the associated tunnel. The reason is often that the setup of LSP for the next hop of the route fails.

```
<PE1> display ip routing-table vpn-instance vpna 10.2.1.202 32 verbose
Destination: 10.2.1.202/32
     Protocol: BGP             Process ID: 0
   Preference: 255                   Cost: 0
      NextHop: 3.3.3.3          Interface: NULL0
 RelayNextHop: 0.0.0.0          Neighbour: 3.3.3.3
        Label: 15360            Tunnel ID: 0x0
                             SecTunnel ID: 0x0
    BkNextHop: 0.0.0.0        BkInterface:
      BkLabel: NULL             Tunnel ID: 0x0
                             SecTunnel ID: 0x0
        State: Inactive Adv WaitQ     Age: 00h01m05s
          Tag: 0
```

Check the LSP to the next hop (3.3.3.3):

```
<PE1> display mpls lsp include 3.3.3.3 32
```

If the display is blank, it indicates that no LSP to 3.3.3.3 exists. The LSP is not set up successfully.

Check whether MPLS LDP is enabled on the interface that connects PE1 and P, and on the interface that connects P and PE2:

```
[PE1] interface giggabitethernet 1/0/0
[PE1-Gigabitethernet1/0/0] display this
#
interface Gigabitethernet1/0/0
 link-protocol ppp
 ip address 192.168.1.2 255.255.255.0
 mpls
#
```

The preceding display shows that MPLS LDP is not enabled in the interface view.

Troubleshooting procedure

Step 1 Use the **display ip routing-table vpn-instance** command on the remote PE to view whether there are local VPN routes in the VPN routing table. If local VPN routes exist, it implies that the routes in the RM are active; otherwise, the routes are inactive.

Step 2 If the remote PE has no local VPN routes, use the **display ip routing-table vpn-instance** *vpn-instance-name ip-address* [*mask* | *mask-length*] **verbose** command on the remote PE to view the Tunnel ID, State, and the next hop of the route. If the local PE does not have the detailed information about the route, use the **display bgp vpnv4 all peer** [*ipv4-address*] **verbose** command to check whether the BGP VPNv4 peer is set up successfully.

Step 3 If the Tunnel ID is 0x0 and the State is Inactive Adv WaitQ, use the **display mpls lsp include** *nexthop-address* **32** command to check for the LSP to the next hop of the route.

Step 4 If no LSP exists, check whether MPLS LDP is enabled on the interface that connects PE1 and P, and on the interface that connects P and PE2.

Step 5 If MPLS LDP is not enabled on the interface, configure MPLS LDP in the interface view.

----End

Summary

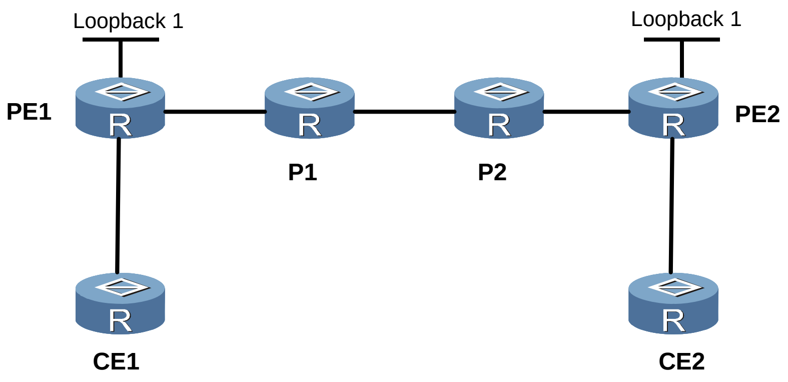
To transfer the traffic of a private network across the public network, you need a public network tunnel.

If the setup of a public network tunnel fails, the reason can be that MPLS LDP is not enabled on the interface, or that an LDP session is not established. This leads to the PE failure to send private network routes to CE.

3.3.2 CEs cannot communicate

Fault symptom

Figure 3-6 BGP/MPLS VPN networking diagram



The BGP/MPLS VPN service is configured in the network as shown in Figure 3-6. CE1 and CE2 belong to the same VPN. After the configuration, CE1 cannot successfully ping CE2.

Fault analysis

NOTE

Consider the configuration of PE2 as an example. The configuration of PE1 is similar to that of PE2, and is not covered in this chapter.

Use the **display bgp peer** command on PE2 to check the IBGP peer relationship between PE2 and PE1. The IBGP peer relationship is not set up successfully.

Query the distribution of labels, and find that P2 distributes a label of 3 to the previous hop P1.

In normal cases, PE2 distributes a label less than 16 to the previous hop P2, and P2 distributes a label larger than 16 to the previous hop P1. Then it can be determined that the error lies in incorrect judgment of hops.

A router judges whether it is the egress node of the LSP because a direct route exists to the outbound interface of the IBGP session. Check the routing table on P2. Find that a direct route to PE2 exists, the endpoint of IBGP.

Check the configuration and find that the loopback interface is not specified by using the **peer** *peer-ip-address* **connect-interface loopback** *interface-number* command as the outbound interface of the local IBGP peer session.

If the outbound interface is not specified for the local IBGP session, the default is the outbound interface of data streams. Because the outbound interface of data streams connects P2 directly; P2 considers itself as the egress node of the LSP. The P2 mistakenly distributes a label with a value less than 16 to P1, which causes the label at the stack bottom to pop up ahead of schedule and results in interworking failure.

Currently, the Secure Router 8000 Series, by default, distributes labels only for the route with a 32-bit mask. This type of configuration error can cause another phenomenon where the public network route or private network route has no corresponding LSPs.

Troubleshooting procedure

- Do as follows on the two PEs.

Step 1 Use the **interface loopback** *interface-number* command in the system view.

Step 2 Use the **ip address** *ip-address* **32** command to configure an IP address for the loopback interface.

Step 3 Use the **quit** command to return to the system view.

Step 4 Use the **bgp** *as-number* command to enter the BGP view.

Step 5 Use the **peer** *peer-address* **connect-interface loopback** *interface-number* command to specify the loopback interface as the outbound interface of the IBGP peer session.

Step 6 Save the configuration.

- On CE, ping the remote CE. If the ping succeeds, it indicates that the fault is isolated.

----End

Summary

When you configure PE peers, specify the local loopback interface as the outbound interface of the local IBGP session.

3.3.3 Failure to ping large packets of the private network

Fault symptom

If the Nortel Secure Router 8000 Series router networks with a device from another vendor to deploy Layer 3 MPLS VPN service by using the Ethernet interface, the packet larger than 1492 bytes cannot be transmitted between private network users. Users cannot access part of websites or download files through the File Transfer Protocol (FTP).

Use the **ping** command, and find that the IGMP payload larger than 1464 bytes cannot be pinged successfully.

Fault analysis

The default maximum transmission unit (MTU) of an Ethernet interface is 1500 bytes. When forwarding data, Layer 3 MPLS VPN adds a 4-byte or 8-byte MPLS packet header between the IP header and the Layer 2 frame header. A 4-byte label is added during the forwarding between the penultimate hop and the tail-end hop; an 8-byte label is added in other cases.

Because MPLS processing is unknown to the link layer, it still receives a maximum of 1500-byte data packet by default. The packet is longer than 1500 bytes after adding an MPLS packet header to a packet of 1492 to 1500 bytes. Consequently the link layer cannot receive the packet, affecting the forwarding.

Troubleshooting procedure

Step 1 Change the MTU of the device from the other vendor. The MTU must be at least 1508 bytes.

Step 2 By default, an Ethernet interface on the Nortel Secure Router 8000 Series router can send and receive jumbo frames. No change is needed on the Nortel Secure Router 8000 Series router.

----End

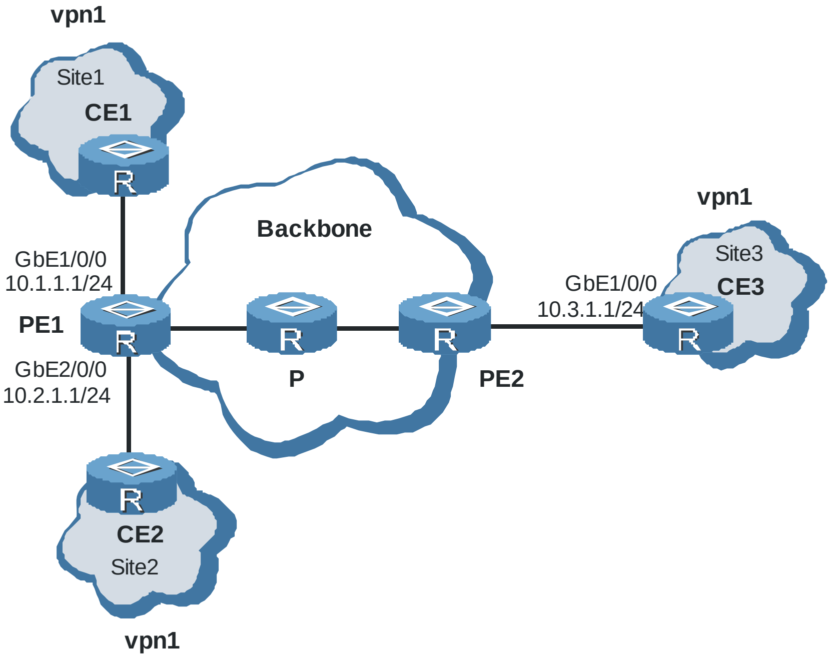
Summary

When jumbo packets cannot be received, check whether the MTU is too small.

3.3.4 PE cannot ping through the remote CE network segment

Fault symptom

Figure 3-7 PE cannot ping through the remote CE network segment



As shown in Figure 3-7, after binding multiple private network interfaces with the same VPN instance, use the **ping 10.3.1.1** command on CE1 and CE2 to ping the remote CE3 segment of PE1 successfully. The **ping -vpn-instance vpn1 10.3.1.1** command on PE1 cannot ping through the CE3 segment.

Fault analysis

After binding multiple private network interfaces on the ingress (PE) with the same VPN instance, if you ping or tracert the remote CE segment from PE, the source address of the Internet Control Message Protocol (ICMP) packet is a private network address that is Up on the local PE. If the remote CE does not import the address, no response packet returns.

Therefore, to use the **ping -vpn-instance** *vpn-instance-name dest-ip-address* command to ping the remote CE segment successfully, ensure the remote CE uses the Up private network addresses of the local PE.

Troubleshooting procedure

Step 1 Ensure the remote CE uses the Up private network addresses of the local PE. Using the **import-route direct** command in the BGP VPN instance view on the local PE can ensure that all the private network routes of the local PE can be advertised through MP-BGP. Replace the **ping -vpn-instance** *vpn-instance-name dest-ip-address* command with the **ping -vpn-instance** *vpn-instance-name* **–a** *source-ip-address dest-ip-address* command.

----End

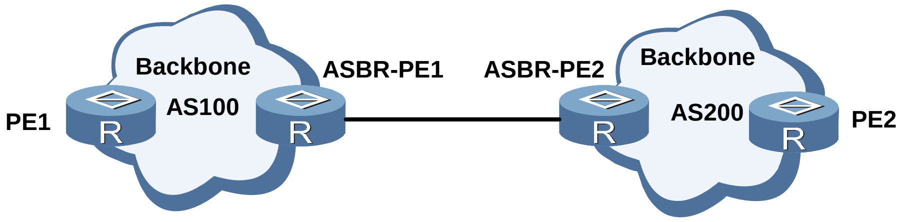
Summary

If you ping the remote CE network segment from PE, Nortel recommends that you specify the source address of the ping packet.

3.3.5 Failure to establish the MP-EBGP peer in inter-AS VPN-OptionC

Fault Symptom

Figure 3-8 Networking diagram of the inter-AS VPN-OptionC troubleshooting



As shown in Figure 3-8, when you configure the inter-AS VPN-OptionC, establishing the MP-EBGP peer relationship between PE1 and PE2 fails. The PE1 and PE2 cannot ping through the loopback address of each other.

After checking the routing table or the forwarding table, you find that multiple load-balancing paths exist between PE2 and ASBR-PE2.

Fault analysis

In the inter-AS VPN-OptionC, PE learns the route of the peer PE through the Autonomous System Boundary Router (ASBR) within the local AS.

After receiving the BGP public labeled route sent by the ASBR in the local AS, PE performs the following action:

- The BGP module fills out the label and tunnel ID (Token in the routing table and FIB).
- The RM fills out the egress and iterative next hop of the route and FIB.

The BGP periodically searches if the LDP LSP to the local AS exists. If so, a new Next Hop Label Forwarding Entry (NHLFE) is created and its Outgoing Token denotes the LDP LSP. The tunnel ID of the new NHLFE is stored in the Token field of the routing table and FIB.

The route is conveyed to the RM. According to the BGP next hop, the RM fixes on the iterative next hop and the egress. If there are multiple load-balancing paths between the PE and ASBR, BGP chooses only one path while the RM iterates multiple IGP paths. From the multiple Interior Gateway Protocol (IGP) paths, the RM selects one path to fill out the iterative next hop and egress.

Therefore, the BGP peer relationship cannot establish between PEs.

Troubleshooting procedure

Step 1 Use the **display fib** command on PE2 to check the next hop, egress, and token of the LSP tunnel from PE2 to PE1.

Step 2 Use the **display tunnel-info** *tunnel-id* command on PE2 to check the egress and next hop of the tunnel with an ID equal to Token, are consistent with that in the FIB.

Step 3 If the egress and next hop are not consistent, check whether load-balancing exists between the ASBR-PE1 and the ASBR-PE2. If yes, cancel the load balancing.

Step 4 If the egress and next hop are not consistent and no load balancing occurs between the ASBR-PE1 and the ASBR-PE2, the cause can be that the next hop of the IBGP peer corresponds to multiple equal-cost IGP routes. Nortel recommends that you delete some links to ensure IBGP has no equal-cost IGP routes.

----End

Summary

The BGP searching for the LDP LSP and the route iteration are two separate processes.

It is possible that the egress and the next hop of the iteration are not those of the found LDP LSP.

3.4 FAQs

Q: A BGP adjacency establishes between PEs, but private network packets cannot forward normally. What is the problem?

A: Possible causes are:

- The loopback interface is not used to establish the BGP adjacency.
- The loopback interface is used, but its address mask is not 32-bits, and its address is not unique in the network.
- An LSP is not set up properly between PEs.

Q: In the BGP/MPLS VPN networking of the inter-AS Option B, proper adjacencies establish between ASBRs, but private network packets cannot forward. What are the causes?

A: Possible causes are:

- The EBGP peer relationship between ASBRs is not set up by using the directly connected interface.

- The **undo policy vpn-target** command is not configured for BGP on ASBR.

Q: LDP configuration between routers is correct, and the route is correct but the establishment of LSP fails. What is the reason?

A: The reason can be that the next hop of the route mismatches with the next hop of the LSP.

To validate the LSP, the next hop of the LSP must exactly match with the next hop of the route.

Q: In Inter-AS VPN Option B, the ASBR does not forward the VPNv4 route forwarded by another ASBR. What is the reason?

A: The reason can be that the interface that connects with the ASBR is not enabled with MPLS. As a result, the label does not apply successfully and the LSP cannot establish, thereby causing failure to distribute VPNv4 routes.

Q: Why do I fail to find the route after running the display ip routing-table vpn-instance command?

A: This command does not display the route in an inactive state. Routes in an inactive state can occur if no tunnel exists. You can run the **display ip routing-table vpn-instance** *vpn-instance-name ip-address* [*mask* | *mask-length*] **verbose** command to view detailed information on routes.

Q: Why can the route reflector not forward private network routes after the VPNv4 adjacency establishes between two customers?

A: You must run the **undo policy vpn-target** command in VPNv4 address family on the route reflector. The route reflector can receive and forward the private network routes even when no VPN configuration exists.

Q: Both the LDP LSP and the GRE LSP exist. Why can the router not choose the GRE LSP automatically after the LDP LSP is down?

A: The problem can be that no tunnel policy configuration exists in the VPN view.

Q: The peer *peer-ip-address* next-hop-local command has been configured for the reflector. Why does the forwarded route not change the next hop?

A: In the Secure Router 8000 Series implementation, after the next hop changes, labels are reallocated for routes, but the reflector does not change the route label. After the **peer** *peer-ip-address* **next-hop-local** is configured, the next hop of the route cannot change even if the **peer** *peer-ip-address* **next-hop-local** is configured.

3.5 Diagnostic tools

3.5.1 display commands

Command	Description
display interface Ethernet	Displays detailed information about the Ethernet interface.
display interface	Displays detailed information about all interfaces.
display ip routing-table vpn-instance *vpn-instance-name*	Displays information about the routes in the active state in the routing table.
display ip routing-table vpn-instance *vpn-instance-name* **verbose**	Displays detailed information about a specified VPN route in the RM routing table, including inactive routes.
display bgp vpnv4 all routing-table	Displays information about all BGP routes, including the routes of the VPNv4 address family and those of the VPN-instance address family.
display bgp vpnv4 all routing-table label	Displays information about all labeled BGP routes, including the routes of the VPNv4 address family and those of VPN-instance address family.
display bgp vpnv4 all peer	Displays information about all BGP VPNv4 peers and VPN-instance peers.
display bgp vpnv4 vpn-instance *vpn-instance-name* **routing-table**	Displays information about the route of a specified instance of BGP.
display mpls lsp	Displays information about all LSPs, including the information on the LSP created through BGP, LDP, and other signaling protocols.
display fib vpn-instance *vpn-instance-name*	Displays information about the forwarding entry of a specified VPN instance in the FIB.
display bgp vpnv4 all routing-table *ip-address*	Displays detailed information about a specified route of BGP.

3.5.2 debugging commands

Command	Description
debugging ethernet	Debugs an Ethernet interface.
debugging bgp all	Enables all BGP debugging.
debugging bgp update	Debugs BGP update packets.
debugging bgp verbose	Enables detailed BGP debugging.
debugging rm ipv4 urt	Debugs RM IPv4 routes.

Command	Description
debugging mpls management	Debugs MPLS BGP/LDP messages.
debugging mpls packet	Debugs MPLS packets.
debugging bgp graceful-restart	Enables BGP Graceful Restart debugging.
debugging bgp event	Debugs BGP Finite State Machine (FSM) events.
debugging bgp *peer-ip-address* **all**	Enables all debugging of a specified BGP peer.

3.5.3 Alarms

Item	Description
Alarm message	Warning: VPN-Instance is in stale state
Meaning	The VPN-instance is in the stale state. It is not allowed to configure a VPN with this name.
Possible cause	Nortel recommends that you do not delete a VPN and reconfigure it immediately because it takes time to delete the routes of a VPN after you delete the VPN.
Solution	Wait for the VPN routes are deleted.

Item	Description
Alarm message	Warning: RD is not configured
Meaning	Configuration of the Import route target (IRT) and Export route target (ERT) commands in the VPN view fails.
Possible cause	The RD is not configured first.
Solution	Configure the rout distinguisher.

Item	Description
Alarm message	Error: RD is not unique
Meaning	You cannot specify this RD value.
Possible cause	Another VPN is configured to use this RD value.
Solution	Delete the VPN with the same RD value or specify another RD.

Item	Description
Alarm message	Error: VPN-Target list is full
Meaning	Targets are full and you cannot configure more.
Possible cause	You can configure up to 16 targets only.
Solution	Delete one or more existing VPN targets.

Item	Description
Alarm message	Warning - Maximum Route Limit xxx Reached - Allowing Route to be added
Meaning	In the VPN1 routing table, the number of routes reaches the limit. Routes can be added until the limit defined in the paf file is reached.
Possible cause	The value of *number* specified in the **routing-table limit** *number* **simply-alert** command in the VPN view is too small.
Solution	Increase the *number* in the **routing-table limit** *number* **simply-alert** command.

Item	Description
Alarm message	Warning - Threshold level xx Percent reached - Route addition denied
Meaning	In the VPN1 routing table, the number of routes reaches the limit. Routes can be added until the threshold defined by the **routing-table limit** command is reached.
Possible cause	The value of *alert-percent* set in the **routing-table limit** *number alert-percent* command in the VPN view is too small.
Solution	Increase the *alert-percent* in the **routing-table limit** *number alert-percent* command.

Item	Description
Alarm message	Label allocation : label is used out
Meaning	No more labels can be allocated.
Possible cause	The number of applied labels reaches the maximum threshold defined in the paf file.
Solution	Increase the number of allowed labels in the paf file.

Item	Description
Alarm message	BGP ILM Creation Failed
Meaning	No more LSPs can be created.
Possible cause	The number of created LSPs reaches the maximum limit defined in the paf file.
Solution	Increase the number of allowed LSPs defined in the paf file.

3.5.4 Logs

Item	Description
Log message	BGP_L3VPN: Allocate token failed
Meaning	Applying for tokens from LSPM fails.
Possible cause	The number of tokens reaches the limit of the license.
Solution	Purchase a new license.

Item	Description
Log message	BGP_L3VPN (Id = xx) : VPN has no ERT, withdraw default-route to peer x.x.x.x
Meaning	Service provider PE withdraws the sent routes.
Possible cause	ERT is not configured for the VPN.
Solution	Configure ERT.

Item	Description
Log message	BGP_L3VPN(Id = xx): RM cross route x.x.x.x failed.RMErrorNum = xx
Meaning	Creating cross routes in the routing table fails.
Possible cause	Cross routes fail in the RM policy filtering, or RM is abnormal.
Solution	Check the RM policy or contact a Nortel engineer for technical assistance.

Item	Description
Log message	BGP: Maximum IPv4 Routes License Value xxx is Exceeded
Meaning	The number of BGP routes reaches the threshold.

Item	Description
Possible cause	The number of routes reaches the limit defined in the permit file.
Solution	Purchase a new permit file.

Item	Description
Log message	BGP xxx: Receiving unsupported capability xxx. Identified in OPEN MSG from x.x.x.x
Meaning	Open packets with the unsupported capability are received.
Possible cause	Inconsistent capability is configured at the two peer routers.
Solution	Configure the peer with the same capability on the two peer routers.

Item	Description
Log message	VPN is stale, don’t send default -route to peer x.x.x.x
Meaning	Do not send the default route of the VPN.
Possible cause	The VPN is in the stale state; therefore, relevant routes do not need to be processed.
Solution	This state is normal and no treatment is needed.

Item	Description
Log message	RM VOS_TASK Memory Shortage Callback notified
Meaning	RM notifies BGP of failure to apply for memory.
Possible cause	Insufficient memory.
Solution	Wait for system processing or reduce the configuration and the amount of routes to reduce the utilization of memory.

Item	Description
Log message	BGP: Wrong ASPATH Message Type xxx
Meaning	Analyze the wrong AS-Path message type.
Possible cause	The AS-path attribute of the received route is incorrect.
Solution	Check whether the origin of the route is correct.

Contents

Figures

4 MPLS L2VPN troubleshooting

About this chapter

The following table describes the contents of this chapter.

Section	Describes
4.1 MPLS Layer 2 VPN overview	This section describes the knowledge you need before you troubleshoot a Multiprotocol Label Switching (MPLS) Layer 2 virtual private network (VPN).
4.2 Layer 2 VPN troubleshooting	This section provides notes about configuring MPLS Layer 2 VPN, the MPLS Layer 2VPN troubleshooting flowchart, and the troubleshooting procedure in a typical MPLS Layer 2 VPN Network.
4.3 Troubleshooting cases	This section presents several troubleshooting cases.
4.4 FAQs	This section lists frequently asked questions and their answers.
4.5 Diagnostic tools	This section describes common diagnostic tools: **display** commands and **debugging** commands.

4.1 MPLS Layer 2 VPN overview

This section covers the following topics:

- Introduction to MPLS Layer 2 VPN
- CCC MPLS Layer 2 VPN
- SVC MPLS Layer 2 VPN
- Martini MPLS Layer 2 VPN
- PWE3 MPLS Layer 2 VPN
- Kompella MPLS Layer 2 VPN
- MPLS Layer 2 VPN IP-interworking

4.1.1 Introduction to MPLS Layer 2 VPN

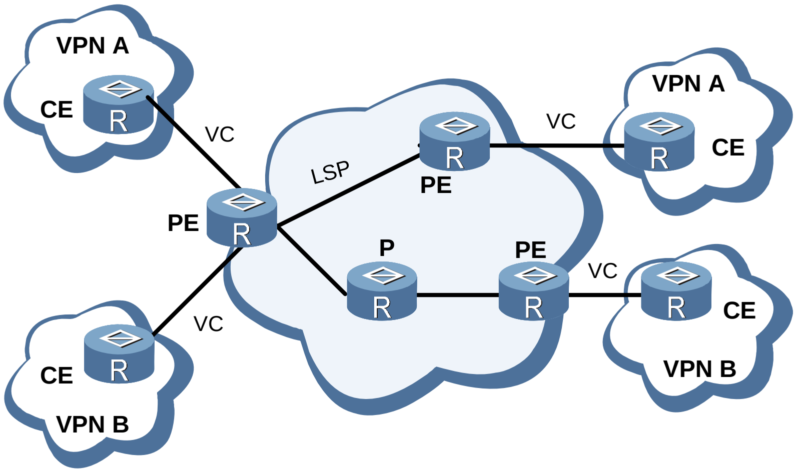
MPLS Layer 2 VPN

MPLS Layer 2 VPN allows operators to provide Layer 2 VPNs of different media over a unified MPLS network. The MPLS network can also provide traditional IP, MPLS Layer 3 VPN, traffic engineering, and Quality of Service (QoS) services.

From the users point of view, the MPLS network is a Layer 2 switching network that can establish a Layer 2 connection between nodes.

Use Asynchronous Transfer Mode (ATM) as an example. Every customer edge (CE) is equipped with an ATM virtual circuit (VC), and connects the remote CE through the MPLS network.

Figure 4-1 MPLS LAYER 2 VPN networking



Basic concepts of MPLS Layer 2 VPN

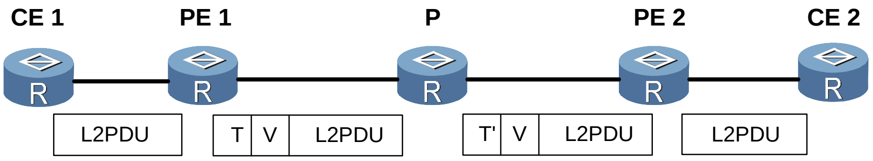
The CE, provider edger (PE), and provider router (P) defined in the MPLS Layer 2 VPN have the same meaning and mechanism as those in the BGP/MPLS Layer 3 VPN.

The MPLS Layer 2 VPN also uses a label stack to implement transparent transmission of packets across the MPLS network.

- The outer label, called the tunnel label, is used to transport packets from one PE to another PE.
- The inner label, called the VC label, is used to distinguish connections in different VPNs. According to the VC label, the receiving PE determines the CE where the packet is forwarded.

Figure 4-2 shows the change of label stack in the process of forwarding packets across the MPLS Layer 2 VPN.

Figure 4-2 MPLS Layer 2 VPN label stack processing



In Figure 4-2, L2PDU represents the link layer packet; T represents the tunnel label; V represents the VC label; and, T' represents a modified outer label.

Implementation of MPLS Layer 2 VPN

The Provider-Provisioned Virtual Private Network (PPVPN) workshop of the Internet Engineering Task Force (IETF) creates multiple MPLS Layer 2 VPN framework drafts. Martini and Kompella are the major drafts.

- draft-martini-l2circuit-trans-mpls: uses the Label Distribution Protocol (LDP) as the signaling protocol to transfer Layer 2 information and VC labels.
- draft-kompella-ppvpn-Layer 2 VPN: uses the Border Gateway Protocol (BGP) as the signaling protocol to transport Layer 2 information and VC labels.

You can also use static VC label configuration, such as Circuit Cross Connect (CCC) and Static Virtual Circuit (SVC) to implement MPLS Layer 2 VPN.

The process of implementation is described as follows.

4.1.2 CCC MPLS Layer 2 VPN

CCC implements MPLS Layer 2 VPN by means of static configuration.

Unlike common MPLS Layer 2 VPNs, CCC uses a one-level label to transport user data and it occupies a static LSP exclusively.

There are two types of CCC connection.

- Local connection: refers to the connection between two local CEs. The two CEs connect to the same PE. The PE functions as a Layer 2 switch that can carry out switching without a static LSP.
- Remote connection: refers to the connection between a local CE and a remote CE. The two CEs connect to different PEs, and a static LSP is required to transmit packets from one PE to another PE. Static LSPs and CCC connections can be associated by using a CLI command on the PE.

4.1.3 SVC MPLS Layer 2 VPN

SVC is another type of static MPLS Layer 2 VPN. The SVC transfers Layer 2 VPN information without using the signaling protocol but it requires manual configuration of VC label information.

When creating a static SVC Layer 2 VPN connection, you can use a tunnel policy to specify the tunnel type, which can be an LDP Label Switched Path (LSP), Constraint-Based Routing using LDP (CR-LDP) or Generic Routing Encapsulation (GRE) tunnel. Load balancing is also supported.

The SVC supports multihop inter-AS Layer 2 VPN but does not support local connection.

NOTE

CCC, SVC, and static LSP use the same label range of 16 to 1023.

4.1.4 Martini MPLS Layer 2 VPN

Martini mode is simple. It implements Layer 2 VPN by setting up a point-to-point link and transports Layer 2 information and VC labels using LDP.

In Martini mode, you can identify a VC between two CEs by using the VC type together with the VC ID.

- VC type: represents the encapsulation type of a VC, which can be ATM (atm-aal5-sdu), VLAN, or Point-to-Point Protocol (PPP).
- VC ID: is used to flag a VC. For VCs of the same type, the VC ID must be unique on the same PE.

PEs exchange VC labels using LDP and associate CEs using the VC ID. After a tunnel is set up successfully between PEs and label exchange, and bindings are complete, a VC is established.

For the remote connection, you must establish a remote LDP session to transport VC FECs and VC labels. This is because, the two PEs that exchange VC labels may not directly connect.

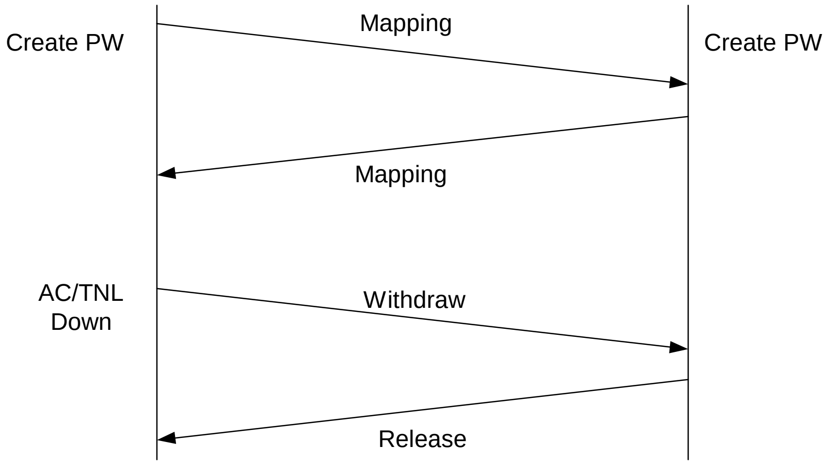
The Martini mode supports multihop inter-AS Layer 2 VPN but does not support local connection.

Martini MPLS Layer 2 VPN supports Graceful Restart (GR) . After router switchover, the VC label remains unchanged. During the switchover, the VC remains up.

After the switchover, the original label saved at the local end is deleted if found different from the one learned from the LDP peer. The VC that uses this label then becomes down.

Figure 4-3 shows the Martini signaling process.

Figure 4-3 Martini signaling process



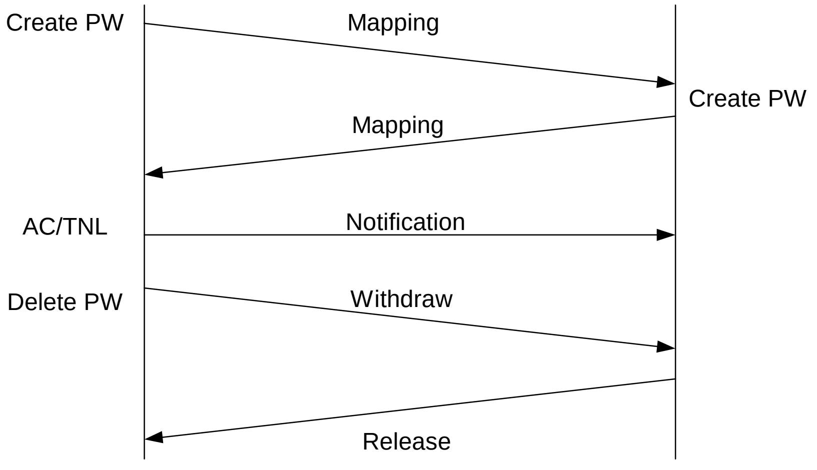
4.1.5 PWE3 MPLS Layer 2 VPN

Pseudo-Wire Emulation Edge-to-Edge (PWE3) is an extension of Martini mode.

The PWE3 sets up a PW on the control plane by using LDP. On the basis of the Martini mode, PWE3 adds a notification mechanism and reduces the interaction of control packets when the attachment circuit (AC) or the tunnel flaps. The PWE3 can also use Layer 2 TP version 3 as the signaling. The Reservation Protocol (RSVP) can be used as a signaling protocol to set up a PW with bandwidth guarantee, that is, RSVP-Traffic Engineering (RSVP-TE) PW. PWE3 mode is compatible with Martini mode.

Figure 4-4 shows the PWE3 signaling process.

Figure 4-4 PWE3 signaling process



4.1.6 Kompella MPLS Layer 2 VPN

Overview

Kompella mode implements Layer 2 VPN in an end-to-end fashion and uses BGP to transport Layer 2 information and VC labels.

Unlike Martini mode, Kompella MPLS Layer 2 VPN requires dividing the entire operator network into many VPNs, and globally numbering CEs within these VPNs instead of processing the connection between CEs directly.

Similar to BGP/MPLS VPN, Kompella mode also uses the VPN target to control the sending and receiving of VPN routes. This adds more flexibility to networking.

To set up a connection between two CEs, you must specify a separate CE ID for both the local CE and the remote CE on the PE.

The Kompella mode supports local connection and remote connection. The Kompella mode supports the following two types of inter-AS Layer 2 VPN.

- Multihop mode: adopts BGP label routes.
- Multiprotocol – Exterior BGP (MP-EBGP) mode: stores the label block on the ASBR.

Label block

In Kompella mode a label block is used to distribute labels. Labels can be allocated for multiple connections at a time.

You can specify a local CE range that shows the number of CEs to which a local CE can connect. The system allocates one label block to this local CE at a time, with the block size equal to the CE range. This mode allows users to distribute extra labels for VPNs. This causes a waste of labels in a short term but reduces the workload of future VPN expansion.

4.1.7 MPLS Layer 2 VPN IP-interworking

Two CEs of the same Layer 2 VPN can use different Layer 2 media to access the SP. To allow them to communicate, you must configure Layer 2 VPN IP-interworking.

Configuration notes vary with the Layer 2 medium through which the CE connects to the SP.

NOTE

The PE mentioned in the following section refers to a local PE unless otherwise stated.

Ethernet and VLAN

An interface or subinterface of an Ethernet type supports IP-interworking encapsulation. Note the following points:

- It is not required to assign an IP address for the Ethernet interface on PE. Even if an IP address is assigned, no routes generate.
- After the encapsulation, the Ethernet interface of PE processes only Address Resolution Protocol (ARP) packets and IP packets. Other types of packets are discarded.
- After receiving IP packets from CE, PE will not update dynamic MAC addresses.
- If you configure IP-interworking encapsulation on an ATM interface or subinterface, you cannot configure this encapsulation on the VE interface that is associated with the Permanent VC (PVC).

- The minimum VLAN IDs of the neighboring PE and CE must be the same; while that of the CEs on two ends of the tunnel can be different.

The processing of ARP packets:

- After IP-interworking encapsulation, the Ethernet interface will have ARP entries that are different from ordinary entries.
- On receiving an ARP request from CE, the IP interworking-encapsulated Layer 2 VPN incoming interface of PE will respond with its own MAC address regardless of the destination.
- An Ethernet interface or subinterface of PE can connect only one CE, it cannot connect multiple CEs by using a hub or LAN switch. Otherwise, PE can learn useless MAC addresses, leading to forwarding failure.

PPP

- PPP supports the Password Authentication Protocol (PAP) and Challenge-Handshake Authentication Protocol (CHAP) authentication. PPP supports local, Remote Authentication Dial-In User Service (RADIUS), and HWTACACS authentication.
- PPP supports STAC-LZS compression other than Internet Protocol Header Compression (IPHC) and Van Jacobsen (VJ) compression.
- PE can assign IP addresses for CEs; CE can also assign IP addresses for PEs. The mechanism of address allocation is similar to the common case.
- PPP supports transparent transmission of IP packets rather than MPLS, Intermediate System-to-Intermediate System (IS-IS), and Internetwork Packet Exchange (IPX) packets from a local CE to a remote CE. If any of these protocols is configured on the interface, NCP will still be negotiated but the protocol packet will not be forwarded.

NOTE

For PPP links, Nortel recommends that you select the way CE allocates IP addresses to PE. This can avoid address conflict on PE and facilitate network deployment.

Frame Relay

- Supports FRF.9 compression but does not support compression of the IP header in the Frame Relay (FR) frame.
- Supports the Local Management Interface (LMI) protocol.
- Supports the Inverse Address Resolution Protocol (INARP).
- Supports transparent transmission of IP packets from a local CE to a remote CE, but does not support that of MPLS packets, IS-IS packets, and IPX packets.

When you configure FR, note the following points:

- You must specify a VC number for an interface of data communications equipment (DCE) or network-to-network interface (NNI) type, whether it is a main interface or a subinterface.
- For an interface of data terminal equipment (DTE) type, if it is a main interface, the system can automatically determine the VC number based on the remote device; if it is a subinterface, you must manually specify a VC number for it.

4.2 Layer 2 VPN troubleshooting

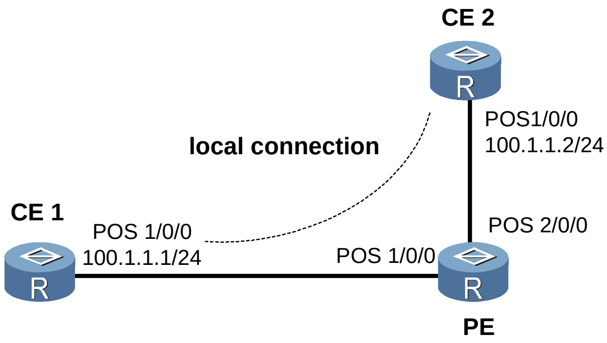
This section covers the following topics:

- Typical networking
- Configuration notes
- Troubleshooting flowchart
- Troubleshooting procedure

4.2.1 Typical networking

Local cross-connection networking

Figure 4-5 Local cross-connection networking

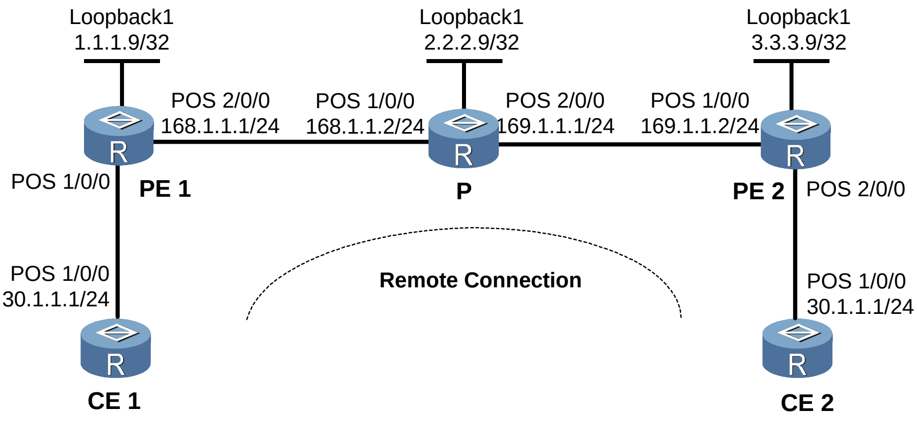


Only the CCC mode and the Kompella mode support local cross-connection. Both modes support IP-interworking in the case of local cross-connection.

The label does not change during data forwarding on PE.

Remote connection networking

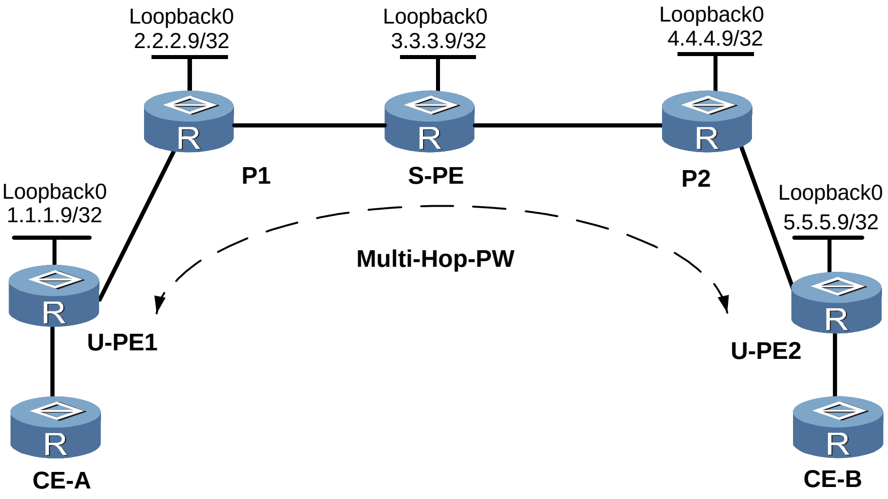
Figure 4-6 Remote connection networking



The networking shown in Figure 4-6 applies to all Layer 2 VPN remote connections.

Multihop connection networking

Figure 4-7 Multihop connection networking

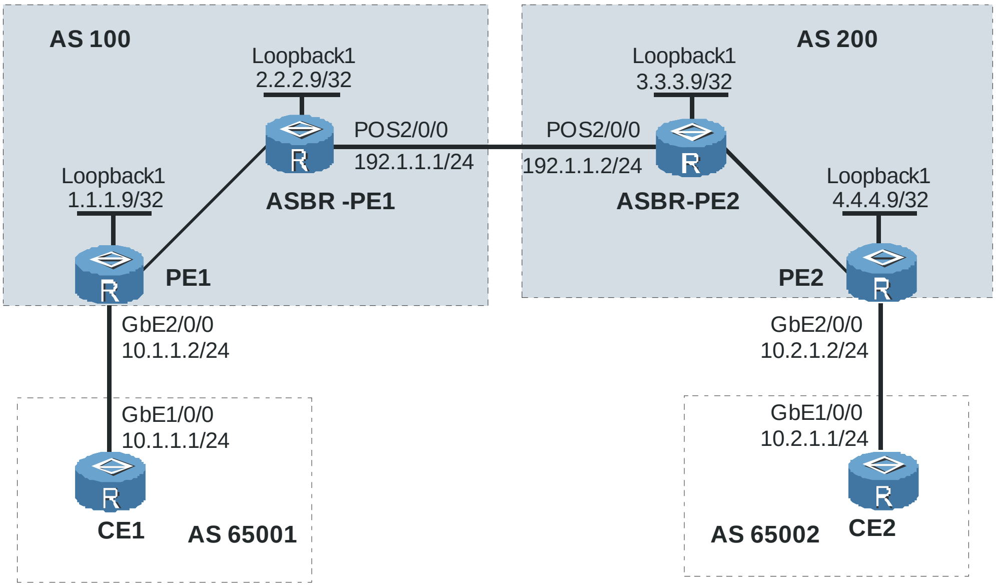


The networking shown in Figure 4-7 applies for multihop PWE3, including LDP-PW, and static-PW.

A PW is configured on the interface of U-PE. The PW switching is configured in the system view on S-PE.

Inter-AS networking

Figure 4-8 Inter-AS networking



Kompella supports three inter-AS implementations namely, virtual router and forwarder (VRF)-to-VRF, multihop, and MP-EBGP. Martini and SVC support the inter-AS both in the VRF-to-VRF mode and the Multihop mode.

4.2.2 Configuration notes

Item	Subitem	Notes
Configuring MPLS	LSR-ID	An LSR ID is similar to the Router ID. An LSR ID actually specifies an address. By default, LDP uses this address to establish an LDP session, so ensure the accessibility of the route to it. There are two methods to set an LSR ID. • Ensure that the LSR-ID is unique in the backbone network. The LSR ID is generally set to the address of the loopback interface. • If the **mpls ldp transport-address** command is configured on the interface that connects to the public network, LDP will use the address specified by this command to establish an LDP session.
	MPLS	You need to enable MPLS in the system view
Establishing the MPLS LDP session (dynamic VC connection)	MPLS LDP or remote MPLS LDP	The dynamic VC connection uses the LDP as the signaling. If PEs do not connect directly, the remote MPLS LDP session must be set up between PEs.

Item	Subitem	Notes
Configuring BGP (remote connection using BGP as the signaling)	AS	You must specify the same AS for all related PEs and Ps.
	Interface used for BGP connection	You must specify the loopback interface (with a 32-bit mask) as the egress interface of the session that is used to establish an IBGP connection between PEs.
	Enabling a specified peer	In the Layer 2 VPN address family view, you need to specify a peer or peer group between which the routing information is exchanged.
Enabling MPLS Layer 2 VPN	MPLS Layer 2 VPN	Whatever MPLS Layer 2 VPN mode you choose, you must enable MPLS Layer 2 VPN globally.
Configuring AC (Attached Circuit)	Encapsulation type, MTU and interface parameters of the specific link type	The Layer 2 VPN can be in the Up state only when the status of AC is Up. ● If the AC type is VLAN, the subinterface can be either the one based on the Ethernet or the VLANIF interface based on the port. ● If the AC type is ATM, configure the VC.
Configuring a connection	Creating a connection	● For the SVC mode, create the static Layer 2 VC in the interface view. ● For the Martini mode, create the Layer 2 VC in the interface view. ● For the CCC mode, create the CCC connection in the system view. ● For the Kompella mode, create the CE connection.
	Specifying an encapsulation type for the interface	For a Layer 2 VC connection the encapsulation type must be consistent on the interface at both VC ends.
	Configuring the VC ID	The VC IDs of the SVC on S-PE can be the same. However, the VC ID of the same encapsulation type on U-PE must be unique. Changing the encapsulation type on U-PE can lead to the collision of the VC ID. For the static PW, the default VC ID is 0. If the static PW is used in the switching, a non-zero VC ID must be configured.
	Specifying the MTU size for the interface	For an LDP VC, the MTU is one of the key parameters to be negotiated. The MTU size must be the same on both ends of a VC; otherwise, the VC will not go up. For U-PE, the MTU is specified in the interface view. For S-PE, the MTU is specified when switching VCs is configured.

Item	Subitem	Notes
	Configuring switching VC	For the multi-hop PW, you need to configure switching VCs.
	Configuring receiving and sending labels	For the static remote connection, the receiving and sending label need to be configured manually.

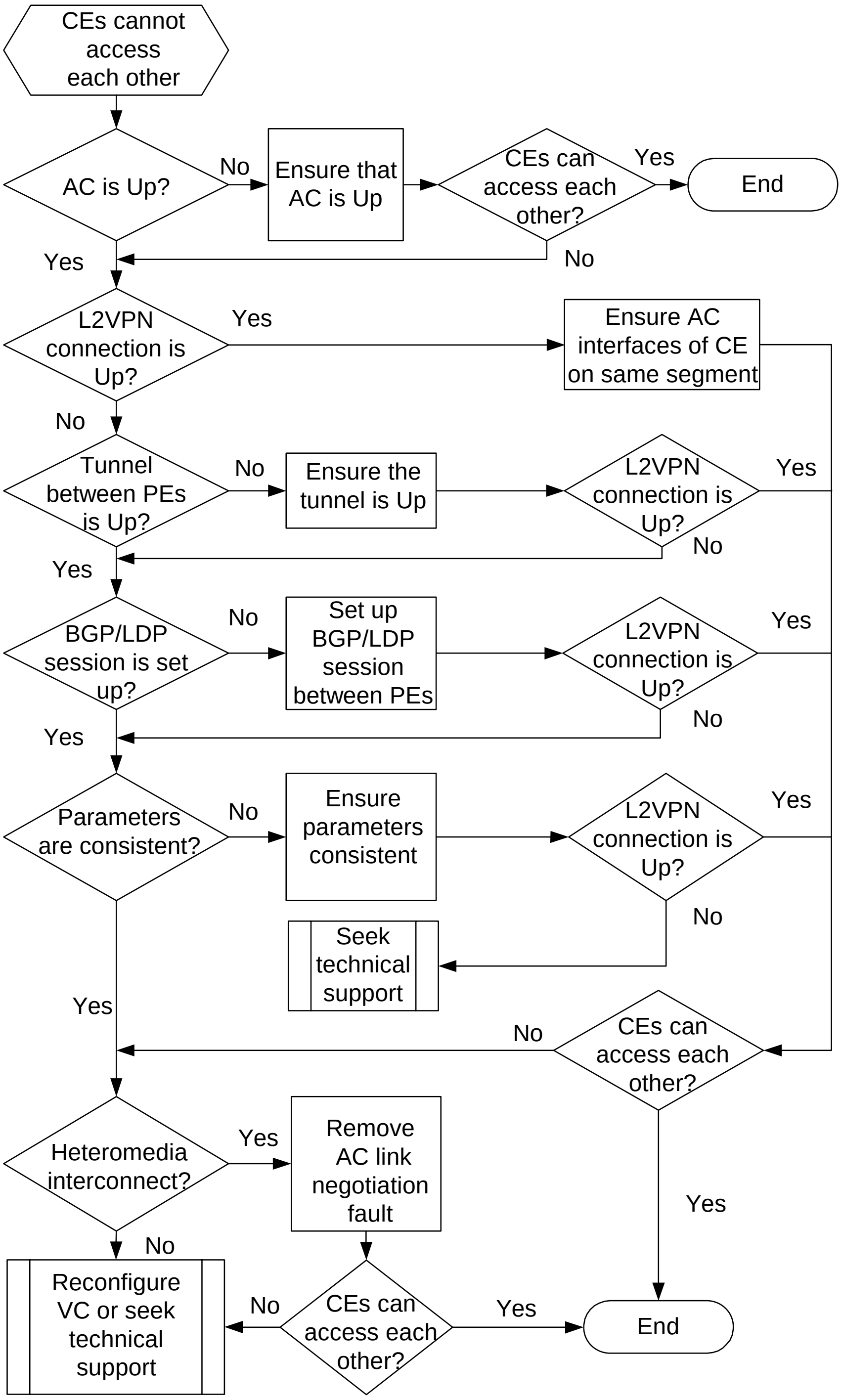
NOTE

The configuration changes with MPLS Layer 2 VPN implementation mode. For details about the configuration, see *Nortel Secure Router 8000 Series Configuration Guide - VPN* (NN46240-507).

4.2.3 Troubleshooting flowchart

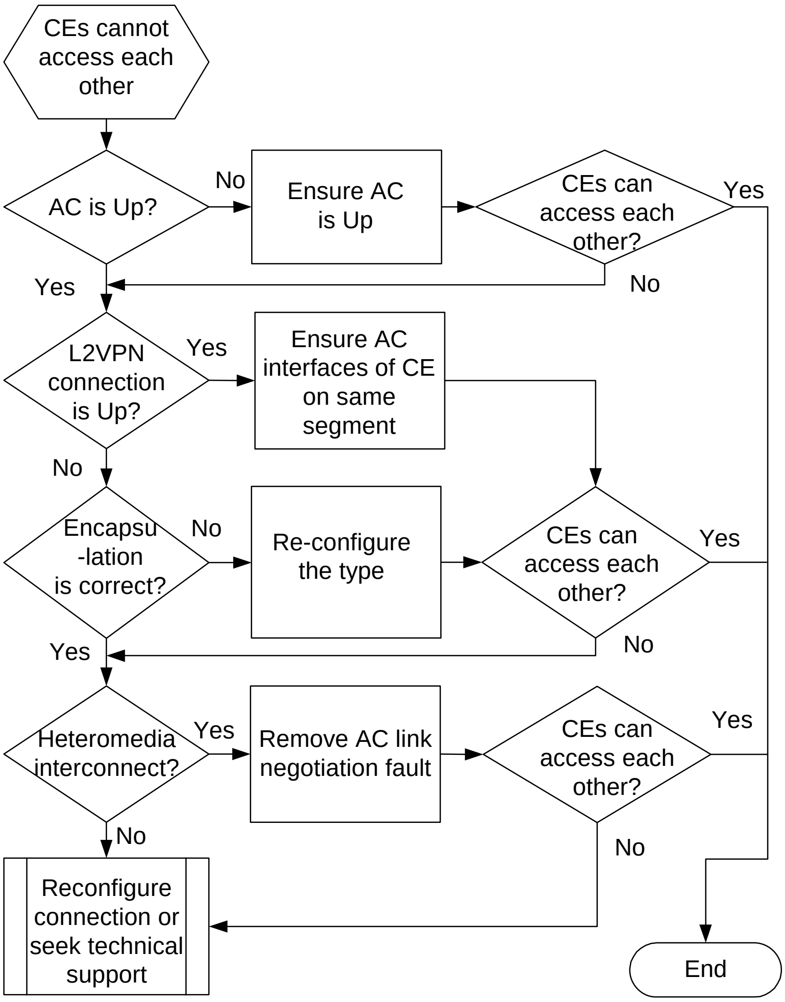
Remote connection

Figure 4-9 Troubleshooting flowchart of the MPLS Layer 2 VPN remote connection fault


CEs cannot access each other
AC is Up?
No
Ensure that AC is Up
CEs can access each other?
Yes
End
No
Yes
L2VPN connection is Up?
Yes
Ensure AC interfaces of CE on same segment
No
Tunnel between PEs is Up?
No
Ensure the tunnel is Up
L2VPN connection is Up?
Yes
No
Yes
BGP/LDP session is set up?
No
Set up BGP/LDP session between PEs
L2VPN connection is Up?
Yes
No
Yes
Parameters are consistent?
No
Ensure parameters consistent
L2VPN connection is Up?
Yes
No
Seek technical support
Yes
No
CEs can access each other?
Yes
Heteromedia interconnect?
Yes
Remove AC link negotiation fault
No
Reconfigure VC or seek technical support
No
CEs can access each other?
Yes
End

Local connection

Figure 4-10 Troubleshooting flowchart of the MPLS Layer 2 VPN local connection fault


CEs cannot access each other
AC is Up?
No
Ensure AC is Up
CEs can access each other?
Yes
No
Yes
L2VPN connection is Up?
Yes
Ensure AC interfaces of CE on same segment
No
Encapsu -lation is correct?
No
Re-configure the type
CEs can access each other?
Yes
No
Yes
Heteromedia interconnect?
Yes
Remove AC link negotiation fault
CEs can access each other?
Yes
No
No
Reconfigure connection or seek technical support
End

4.2.4 Troubleshooting procedure

The steps of troubleshooting are as follows:

Step 1 Check the AC status of the PE of both ends.

Before establishing the Layer 2 VPN connection, ensure the AC status is Up. If the status of AC is Down, remove the fault on the AC link and ensure the AC status on PE is Up.

NOTE

- When the AC type is VLAN, configure the subinterface.
- When the AC type is ATM, configure the VC.

Step 2 Check the status of the Layer 2 VPN connection.

On PE, use the following command in any view to check the AC status and the Layer 2 VPN connection status:

- In CCC mode, use the **display ccc** command or the **display layer 2 vpn ccc-interface vc-type** command.
- In SVC mode, use the **display mpls static-l2vc** command.
- In Martini mode, use the **display mpls l2vc** command.
- In Kompella mode, use the **display mpls layer 2 vpn connection** command.

If the status of the connection is Up, but the packet cannot forward normally, check that the AC interfaces on CE are on the same network segment.

For the static VC, check that the in-label and the out-label, and that of the remote end are consistent.

- **transmit-vpn-label** on the local end and **receive-vpn-label** on the remote end are consistent.
- **receive-vpn-label** on the local end and **transmit-vpn-label** on the remote end are consistent.

If the CEs still cannot communicate, use the **display fib** command and the **display ip routing-table** command to view whether the forwarding table and the routing table are consistent.

- If the tables are not consistent, the forwarding entry may not be delivered. You must delete the VC and reconfigure it.
- If the tables are consistent, contact Nortel technical personnel.

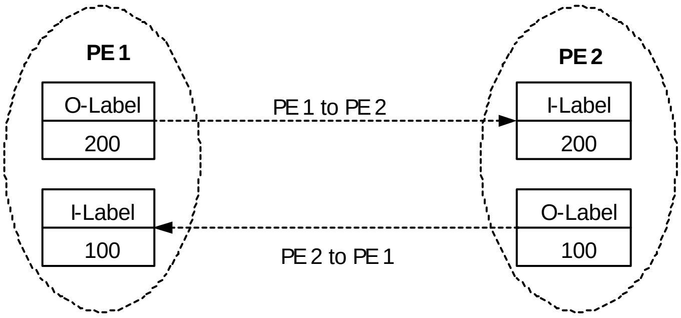
If the status of the Layer 2 VPN is Down, do as follows.

Step 3 Do as follows in the case of remote connection.

1. Check that the outer tunnel (public network tunnel) exists.

- L2VC connection: Run the **display mpls l2vc interface** command. If VC tunnel/token info does not appear in the output, check if the tunnel configuration is correct. If the text does appear, but TNL ID is 0x0, check that routes are reachable to both ends of a tunnel. If it is an SVC connection, check if the label at both ends match. For a same SVC connection, the egress label of one end must be the ingress label of another end as shown in Figure 4-11.

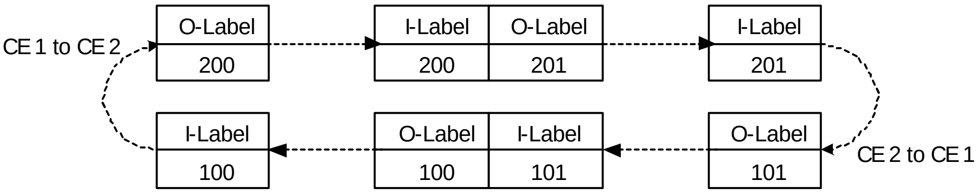
Figure 4-11 Sketch map of the SVC remote connection label



- Kompella mode: Run the **display mpls Layer 2 VPN connection interface** command. If tunnel type does not appear in the output, or id that follows is 0x0, check that the routes are reachable at both ends of a tunnel.

- Remote CCC connection: Run the **display ccc** command to check that the label at both ends match. For a same CCC connection, the egress label of one end must be the ingress label of another end as shown in Figure 4-12.

Figure 4-12 Sketch map of the CCC remote connection label



2. Check that the BGP connection or the MPLS LDP session establishes successfully.

- If LDP is used as the signaling protocol, use the **display mpls ldp session** command to check the establishment of a session. If PEs connect indirectly, the MPLS LDP remote session needs to be set up between PEs.
- If BGP is used as the signaling protocol, use the **display bgp vpnv4 vpn-instance** *vpn-instance-nam* **all peer** command to check that the BGP session establishes successfully.

For the diagnosis of MPLS LDP session faults, see 3 BGP/MPLS IP VPN troubleshooting.

For BGP troubleshooting, see *Nortel Secure Router 8000 Series Troubleshooting - IP Routing* (NN46240-706).

If the BGP connection or the MPLS LDP session establishes successfully, but still the Layer 2 VPN cannot be set up, perform the following checks.

3. Check that the negotiated parameters match.

Parameter mismatch can appear in various forms, as in the following examples:

- The maximum transmission unit (MTU) of one end is 1500 bytes, but that of the other end is 4470 bytes.
- One end supports CW while the other end does not.
- One end is encapsulated with PPP while the other end is encapsulated with Ethernet.

If the negotiated parameters mismatch, modify them to be consistent.

In the case of the heterogeneous-media interconnection, the encapsulation type of the connection must be IP-interworking.

If the status of VC is Down even after the configuration, do as follows.

Step 4 Do as follows in the case of the local connection.

Check that the encapsulation types are consistent on both local and remote ends if the local connection.

Step 5 Check whether the link negotiation between CE and PE succeeds when heterogeneous media interconnect.

If the negotiated parameters of the link between CE and PE mismatch, modify them to be consistent.

In the case of the Ethernet network, check that **local ce-mac** or **local ce-ip** is configured.

If the fault is still not rectified, check that the local PE is configured with the IP address of the remote CE.

If the fault persists, contact Nortel technical personnel.

----End

4.3 Troubleshooting cases

This section provides the following troubleshooting cases:

- VC type is not supported when setting up a PW on an ATM subinterface
- A static PW cannot be switched with other PWs
- Switch-L2VC is down after PW switching configuration
- PW attributes cannot be changed by using the reset pw command
- VC is up but the PPP session cannot establish
- VC under the interface is missing after the link protocol changes
- Both the session and the AC are up, but the VC cannot be up
- Ethernet interconnects with ATM, the VC is up, but the ping between CEs fails
- CEs cannot communicate by using the accessing mode of VLAN
- CEs cannot access each other though the static VC is up
- VC is down though AC is up
- Large-sized packets are lost between CEs on two ends of Layer 2 VPN
- Failure to establish the MPLS LDP session between PEs when RIP-1 is used in the Layer 2 VPN backbone

4.3.1 VC type is not supported when setting up a PW on an ATM subinterface

Fault symptom

Configuration of PWE3 is required. After a PW establishes on the ATM subinterface of U-PE, use the **display mpls l2vc** command to check it. In the output, VC Type is Unsupport. For example:

```
[Nortel] interface atm 2/1/0.100
[Nortel-Atm2/1/0.100] mpls l2vc 3.3.3.8 33
[Nortel-Atm2/1/0.100] display mpls l2vc interface atm 2/1/0.100
 *Client Interface : Atm2/1/0.100 is up
  Session State    : down
  AC State         : down
  VC State         : down
  VC ID            : 33
  VC Type          : Unsupport
  Destination      : 3.3.3.8
  Local Group ID   : 0
  Remote Group ID  : 0
  Local VC Label   : 119809
  Remote VC Label  : 0
  Local VC MTU     : 1500
  Remote VC MTU    : 0
  Local VCCV       : Disable
  Remote VCCV      : None
  Local Frag       : Disable
  Remote Frag      : None
  Local Ctrl Word  : Disable
  Remote Ctrl Word : None
  Tunnel Policy    : --
  Traffic Behavior : --
  PW Template Name : --
  VC tunnel/token info : 0 tunnels/tokens
  Create time      : 0 days, 0 hours, 0 minutes, 9 seconds
  UP time          : 0 days, 0 hours, 0 minutes, 0 seconds
  Last change time : 0 days, 0 hours, 0 minutes, 9 seconds
```

Fault analysis

By default, an ATM subinterface uses the Point-to-Multipoint Protocol (P2MP) as the link layer protocol. However, PWE3 does not support P2MP.

You must specify Point-to-Point (P2P) when you create an ATM subinterface.

After specifying P2P, you need to reconfigure the PW. The configuration is as follows:

```
[Nortel] interface atm 2/1/0.100 p2p
[Nortel-Atm2/1/0.100] mpls l2vc 3.3.3.8 33
```

Check the output and you can find that VC Type becomes atm aal5 sdu:

```
[Nortel-Atm2/1/0.100] display mpls l2vc interface atm 2/1/0.100
 *Client Interface : Atm2/1/0.100 is up
  Session State    : down
  AC State         : up
  VC State         : down
  VC ID            : 33
  VC Type          : atm aal5 sdu
  Destination      : 3.3.3.8
  Local Group ID   : 0
  Remote Group ID  : 0
  Local VC Label   : 119809
  Remote VC Label  : 0
  Local VC MTU     : 1500
  Remote VC MTU    : 0
  Local VCCV       : Disable
  Remote VCCV      : None
  Local Frag       : Disable
  Remote Frag      : None
  Local Ctrl Word  : Enable
  Remote Ctrl Word : None
  Tunnel Policy    : --
  Traffic Behavior : --
  PW Template Name : --
  VC tunnel/token info : 0 tunnels/tokens
  Create time      : 0 days, 0 hours, 0 minutes, 9 seconds
  UP time          : 0 days, 0 hours, 0 minutes, 0 seconds
  Last change time : 0 days, 0 hours, 0 minutes, 9 seconds
```

Troubleshooting procedure

Step 1 Specify P2P as the link layer protocol of an ATM subinterface.

Step 2 Reconfigure the PW.

----End

Summary

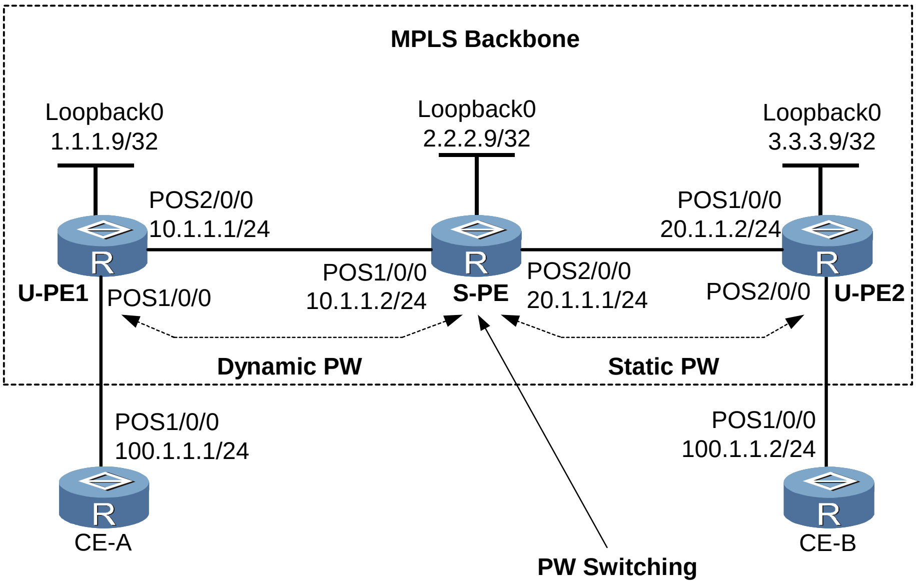
If you configure PWE3, you must specify P2P as the link layer protocol for the subinterface to create a PW on an ATM subinterface.

4.3.2 A static PW cannot be switched with other PWs

Fault symptom

After you configure static PW, you find that the static PW cannot be switched with other PWs as shown in Figure 4-13.

Figure 4-13 Networking diagram of the switching between the static PW and dynamic PW



For example:

# Configure a static PW on U-PE1:

```
[U-PE1-Pos1/0/0] mpls static-l2vc destination 3.3.3.3 transmit-vpn-label 100
receive-vpn-label 100
```

# Configure a static PW on U-PE2:

```
[U-PE2-Pos1/0/0] mpls static-l2vc destination 1.1.1.1 transmit-vpn-label 100
receive-vpn-label 100
```

# Configure static PW switching on S-PE:

```
[S-PE] mpls switch-l2vc 3.3.3.3 100 trans 100 recv 100 between 1.1.1.1 100 trans 100
recv 100 encapsulation ppp
```

Fault analysis

The VC ID is optional for the static PWE3. The static PW without a VC ID cannot be switched with the dynamic PW.

If you configure the mixed PW switching, specify a non-zero VC ID for the static PW. Otherwise, the multihop PW (MH-PW) cannot be located. Normally, the VC ID for the static PW is the same as that of the dynamic PW.

In this case, the possible cause is that the PW ID of the static PW is 0. You can use the following method to solve it.

# Configure U-PE1:

```
[U-PE1] pw-template pwt1
[U-PE1] peer-address 3.3.3.3
[U-PE1-Pos1/0/0] mpls static-l2vc pw-template pwt1 1 transmit-vpn-label 100
receive-vpn-label 100
```

# Configure U-PE2:

```
[U-PE1] pw-template pwt1
[U-PE1] peer-address 1.1.1.1
[U-PE1-Pos1/0/0] mpls static-l2vc pw-template pwt1 1 transmit-vpn-label 100
receive-vpn-label 100
```

# Configure static PW switching on S-PE:

```
[S-PE] mpls switch-l2vc 3.3.3.3 100 trans 100 recv 100 between 1.1.1.1 100 trans 100
recv 100 encapsulation ppp
```

Establishment of the static PW does not involve the signaling. As long as the label is correct, VC IDs can be different.

Troubleshooting procedure

Step 1 Create a PW template in the system view.

Step 2 Specify a peer for the PW in the PW template.

Step 3 Create a PW by using the PW template and specify a non-zero PW ID (also called VC ID) for it. Or specify a non-zero VC ID for the static PW.

----End

Summary

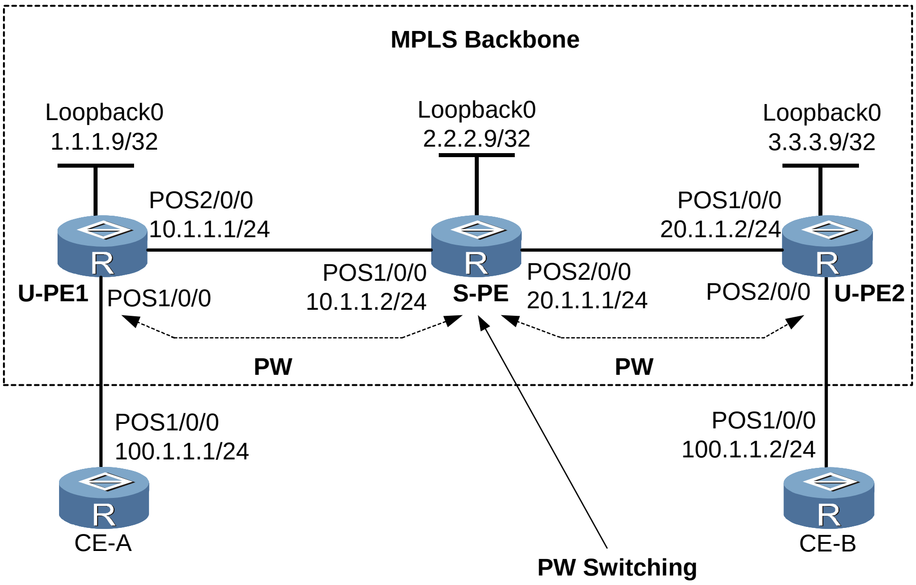
The PW ID for the static PW is optional.

Static PWs to be switched must be configured with a PW ID.

4.3.3 Switch-L2VC is down after PW switching configuration

Fault symptom

Figure 4-14 Networking diagram of Switch-L2VC troubleshooting



The configuration is as follows.

# Configure S-PE:

```
[S-PE] mpls switch-l2vc 1.1.1.9 45 between 2.2.2.9 34 encapsulation vlan
```

# Display the configuration and find that the status of the switch-L2VC is Down:

```
[S-PE] display mpls switch-l2vc
*Switch-l2vc type              : LDP<---->LDP
 Peer IP Address               : 2.2.2.9, 1.1.1.9
 VC ID                         : 45, 34
 VC Type                       : vlan
 VC State                      : down
 Local/Remote Label            : 119812/0, 119813/0
 Local/Remote Control Word     : Disable/None, Disable/None
 Local/Remote VCCV Capality    : Disable/None, Disable/None
 Local/Remote Frag Capability : Disable/None, Disable/None
 Switch-l2vc tunnel info       :
  0 tunnels for peer 2.2.2.9
  1 tunnels for peer 1.1.1.9
   NO.0  TNL Type : lsp   , TNL ID : 0x8b010000
 Create time                   : 0 days, 0 hours, 0 minutes, 9 seconds
 UP time                       : 0 days, 0 hours, 0 minutes, 0 seconds
 Last change time              : 0 days, 0 hours, 0 minutes, 9 seconds
```

Fault analysis

The Secure Router 8000 Series does not necessarily require a VC peer to use the remote MPLS LSR ID. When using the MPLS LDP, you must use the LSR-ID specified in the MPLS LDP view as the LSR-ID. Therefore, the VC peer can be the remote MPLS LSR ID or the 32-bit mask address of a loopback interface. Establish the session between the two ends by using the **remote peer** command.

An LSR cannot establish a session or LSP with itself. If a VC between an LSR and its remote is configured on S-PE where PW switching is performed, then, this VC cannot be Up. The remote address used for PW switching cannot be the address of the local router.

Troubleshooting procedure

Step 1 Check the peer IP address of the VC on S-PE.

Step 2 Modify the peer IP address used in the PW switching to the nonlocal S-PE router address.

----End

Summary

When you configure a multihop PW, note that a VC cannot establish between S-PE and U-PE.

4.3.4 PW attributes cannot be changed by using the reset pw command

Fault symptom

After PW configuration on PE, you change PW attributes.

Use the **reset pw template** command and the **reset pw** *vc-id* command. Find that PW attributes are unchanged.

# Check the configuration of the PW template on PE:

```
[PE] display pw-template pwt1
  PW Template Name : pwt1
  PeerIP           : 1.1.1.1
  Tnl Policy Name  : --
  PW Type          : Unknown
  CtrlWord         : Disable
  MTU              : 1500
  MaxAtmCells      : 1
  VCCV Capability  : Disable
  Fragmentation    : Disable
  Behavior Name    : --
  Total PW         : 1, Static PW : 1, LDP PW : 0
```

# Configure a PW by applying the PW template:

```
[PE-Atm2/1/0.100] mpls l2vc pw-template pwt1 2.2.2.2 100
```

# View the PW configuration:

```
[PE-Atm2/1/0.100] display mpls l2vc 100
 Total ldp vc : 1     0 up       1 down
 *Client Interface     : Atm2/1/0.100
  Session State        : down
  AC Status            : up
  VC State             : down
  VC ID                : 100
  VC Type              : atm aal5 sdu
  Destination          : 2.2.2.2
  Local VC Label       : 119811
  Remote VC Label      : 0
  Control Word         : Disable
  Local VC MTU         : 1500
  Remote VC MTU        : 0
  Tunnel Policy Name   : --
  Traffic Behavior Name: --
  PW Template Name     : pwt1
  Create time          : 0 days, 0 hours, 0 minutes, 6 seconds
  UP time              : 0 days, 0 hours, 0 minutes, 0 seconds
  Last change time     : 0 days, 0 hours, 0 minutes, 6 seconds
```

# Specify a new peer address for the PW in the PW template:

```
[PE-Atm2/1/0.100] pw-template pwt1
[PE-pw-template-pwt1] peer-address 3.3.3.3
 Info: The attribute of this PW template has been modified, please use PW restart command
to update PW's attribute
```

According to the prompt, do as follows:

```
[PE-pw-template-pwt1] return
```

# Reset the PW:

```
<PE> reset pw 100 atm-aal5-sdu
```

# Display the configuration and find that the peer IP address of the PW is unchanged:

```
<PE> display mpls l2vc 100
 Total ldp vc : 1     0 up       1 down

 *Client Interface     : Atm2/1/0.100
  Session State        : down
  AC Status            : up
  VC State             : down
  VC ID                : 1
  VC Type              : atm aal5 sdu
  Destination          : 2.2.2.2
  Local VC Label       : 119811
  Remote VC Label      : 0
  Control Word         : Disable
  Local VC MTU         : 1500
  Remote VC MTU        : 0
  Tunnel Policy Name   : --
  Traffic Behavior Name: --
  PW Template Name     : pwt1
  Create time          : 0 days, 0 hours, 0 minutes, 45 seconds
  UP time              : 0 days, 0 hours, 0 minutes, 0 seconds
  Last change time     : 0 days, 0 hours, 0 minutes, 45 seconds
```

# Reset the PW template:

```
<PE> reset pw pw-template pwt1
```

# Display the configuration and find that the peer IP address of the PW does not change:

```
<PE> display mpls l2vc 100
 Total ldp vc : 1     0 up       1 down
 *Client Interface     : Atm2/1/0.100
  Session State        : down
  AC Status            : up
  VC State             : down
  VC ID                : 1
  VC Type              : atm aal5 sdu
  Destination          : 2.2.2.2
  Local VC Label       : 119811
  Remote VC Label      : 0
  Control Word         : Disable
  Local VC MTU         : 1500
  Remote VC MTU        : 0
  Tunnel Policy Name   : --
  Traffic Behavior Name: --
  PW Template Name     : pwt1
  Create time          : 0 days, 0 hours, 1 minutes, 7 seconds
  UP time              : 0 days, 0 hours, 0 minutes, 0 seconds
  Last change time     : 0 days, 0 hours, 1 minutes, 7 seconds
```

Fault analysis

Some PW attributes can be configured by using the PW template or by using the CLI command. However, the latter method has the highest priority.

If PW attributes are specified in the CLI, then those specified in the PW template lose effect. The PW attributes do not change if the **reset pw template** and the **reset pw** *vc-id* commands are run.

In this case, you can use the PW template to set PW attributes that need changes. To set this, perform the following actions:

# Specify the peer IP address in the PW template:

```
[PE-Atm2/1/0.100] pw-template pwt1
[PE-pw-template-pwt1] peer-address 3.3.3.3
```

# Apply the template to the PW:

```
[PE-pw-template-pwt1] int atm 2/1/0.100
[PE-Atm2/1/0.100] mpls l2vc pw-template pwt1 100
```

# Display the configuration and find that the IP address of the PW peer is unchanged:

```
[PE-Atm2/1/0.100] display mpls l2vc 100
 Total ldp vc : 1     0 up       1 down

 *Client Interface     : Atm2/1/0.100
  Session State        : down
  AC Status            : up
  VC State             : down
  VC ID                : 100
  VC Type             : atm aal5 sdu
  Destination         : 2.2.2.2
  Local VC Label      : 119811
  Remote VC Label     : 0
  Control Word        : Disable
  Local VC MTU        : 1500
  Remote VC MTU       : 0
  Tunnel Policy Name   : --
  Traffic Behavior Name: --
  PW Template Name     : pwt1
  Create time         : 0 days, 0 hours, 0 minutes, 4 seconds
  UP time             : 0 days, 0 hours, 0 minutes, 0 seconds
  Last change time     : 0 days, 0 hours, 0 minutes, 4 seconds
[PE-Atm2/1/0.100] return
<PE> reset pw 100 atm-aal5-sdu
```

# Display the configuration and find that the IP address of the PW peer changes:

```
<PE> display mpls l2vc 100
 Total ldp vc : 1     0 up       1 down

 *Client Interface     : Atm2/1/0.100
  Session State        : down
  AC Status            : up
  VC State             : down
  VC ID                : 100
  VC Type              : atm aal5 sdu
  Destination          : 3.3.3.3
  Local VC Label       : 119811
  Remote VC Label      : 0
  Control Word         : Disable
  Local VC MTU         : 1500
  Remote VC MTU        : 0
  Tunnel Policy Name   : --
  Traffic Behavior Name: --
  PW Template Name     : pwt1
  Create time          : 0 days, 0 hours, 0 minutes, 53 seconds
  UP time              : 0 days, 0 hours, 0 minutes, 0 seconds
  Last change time     : 0 days, 0 hours, 0 minutes, 53 seconds
```

Troubleshooting procedure

Step 1 Create a PW template and set PW attributes (especially those that need change) on it.

Step 2 Apply the PW template to the PW.

Step 3 Run the **reset pw template** command or the **reset pw vc-id** command in the user view to modify PW attributes.

----End

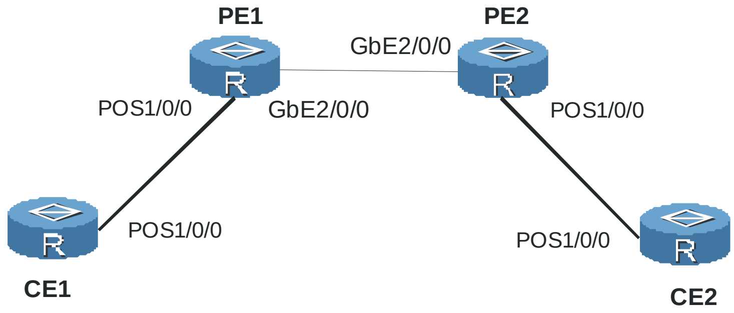
Summary

The **reset pw template** command or the **reset pw** *vc-id* command can only change the attributes that are set by using the PW template.

4.3.5 VC is up but the PPP session cannot establish

Fault symptom

Figure 4-15 Networking diagram



The CE and PE connect through a POS interface. The PE and PE connect through a GbE interface.

The VC is Up, but the PPP session cannot be Up. If a POS interface connects PEs, the PPP session between CE and PE goes Up.

Fault analysis

The VC on PE is Up because a tunnel exists between PEs and the CE-bound PE interface is Up administratively.

To enable a PPP session to be Up, PPP negotiation must succeed.

The PPP negotiation occurs between two CE interfaces. The PE connects to the public network through an Ethernet-type interface whose minimum packet is defined to be 64 bytes long. The PPP control packet, LCP packet, is very small and is less than 64 bytes even after two layers of labels are added. Consequently, the GbE interface on PE discards this negotiation packet. This causes the failure in transmitting the negotiation packet to the remote CE over the VC.

Troubleshooting procedure

Step 1 Connect PEs by using the POS interface. Alternatively, run the **mpls l2vc** *peer-ip-address* [*vc-id*] **control-word** command on the two PEs to configure a control word for Layer 2 VPN. Padding is automatically added to Layer 2 VPN packets.

----End

Summary

When the type of the link between CE and PE is different from that between PEs, check the minimum MTU value.

4.3.6 VC under the interface is missing after the link protocol changes

Fault symptom

The configuration is as follows.

# Configure MPLS Layer 2 VC on an interface on PE that connects the AC. Set the VC ID to 100:

```
[PE-Pos4/0/0] mpls l2vc 1.1.1.8 100
```

# View the configuration of the interface:

```
[PE-Pos4/0/0] display this
#
interface Pos4/0/0
 link-protocol fr
 mpls l2vc 1.1.1.8 100
#
return
```

# This interface has a VC with the VC ID of 100:

```
[PE-Pos4/0/0] display mpls l2vc interface pos 4/0/0
 *Client Interface : Pos4/0/0 is down
  Session State    : down
  AC State         : down
  VC State         : down
  VC ID            : 100
  VC Type          : fr
  Destination      : 1.1.1.8
  Local Group ID   : 0
  Remote Group ID  : 0
  Local VC Label   : 119808
  Remote VC Label  : 0
  Local VC MTU     : 4470
  Remote VC MTU    : 0
  Local VCCV       : Disable
  Remote VCCV      : None
  Local Frag       : Disable
  Remote Frag      : None
  Local Ctrl Word  : Enable
  Remote Ctrl Word : None
  Tunnel Policy    : --
  Traffic Behavior : --
  PW Template Name : --
  VC tunnel/token info : 0 tunnels/tokens
  Create time      : 0 days, 0 hours, 0 minutes, 19 seconds
  UP time          : 0 days, 0 hours, 0 minutes, 0 seconds
  Last change time : 0 days, 0 hours, 0 minutes, 19 seconds
```

# Another interface on PE also has a VC with the ID as 100, and the link layer protocol is High-Level Data Link Control (HDLC):

```
[PE-Pos4/1/0] display mpls l2vc interface pos 4/1/0
 *Client Interface : Pos4/1/0 is down
```

```
  Session State    : down
  AC State         : down
  VC State         : down
  VC ID            : 100
  VC Type          : hdlc
  Destination      : 2.2.2.8
  Local Group ID   : 0
  Remote Group ID  : 0
  Local VC Label   : 119809
  Remote VC Label  : 0
  Local VC MTU     : 4470
  Remote VC MTU    : 0
  Local VCCV       : Disable
  Remote VCCV      : None
  Local Frag       : Disable
  Remote Frag      : None
  Local Ctrl Word  : Disable
  Remote Ctrl Word : None
  Tunnel Policy    : --
  Traffic Behavior : --
  PW Template Name : --
  VC tunnel/token info : 0 tunnels/tokens
  Create time      : 0 days, 0 hours, 6 minutes, 14 seconds
 UP time          : 0 days, 0 hours, 0 minutes, 0 seconds
 Last change time : 0 days, 0 hours, 6 minutes, 14 seconds
```

# Change the link layer protocol of POS 4/0/0 to HDLC:

```
[PE-Pos4/0/0] link-protocol hdlc
```

# Recheck POS 4/0/0 and find that no VC exists:

```
[PE-Pos4/0/0] display mpls l2vc interface pos 4/0/0
```

# Check PE and find that only one VC is left. This VC is on POS 4/1/0 whose link layer protocol is HDLC:

```
[PE] display mpls l2vc
 Total ldp vc : 1     0 up       1 down

 *Client Interface     : Pos4/1/0
  Session State        : down
  AC Status            : down
  VC State             : down
  VC ID                : 100
  VC Type              : hdlc
  Destination          : 2.2.2.8
  Local VC Label       : 119809
  Remote VC Label      : 0
  Control Word         : Disable
  Local VC MTU         : 4470
  Remote VC MTU        : 0
  Tunnel Policy Name   : --
  Traffic Behavior Name: --
  PW Template Name     : --
  Create time          : 0 days, 0 hours, 8 minutes, 26 seconds
  UP time              : 0 days, 0 hours, 0 minutes, 0 seconds
 Last change time     : 0 days, 0 hours, 8 minutes, 26 seconds
```

Fault analysis

If an interface (POS 4/1/0 for example) on PE has an HDLC-type PW with the ID of 1, and you change the link layer protocol of another interface (POS 4/0/0 for example) to HDLC, the system deletes the PW under POS 4/0/0 automatically. The reason is that the two PWs have the same VC ID and the same VC type.

Troubleshooting procedure

Step 1 If you need to change the link layer protocol of a VC, ensure that no identical PW ID and VC type are configured on other interfaces of the same router.

----End

Summary

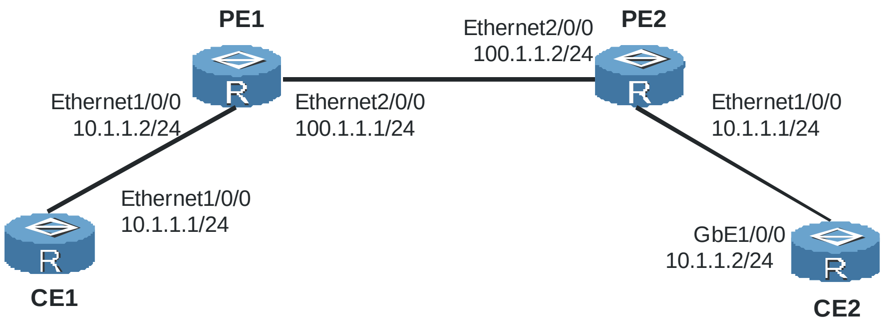
The combination of VC ID and VC type must be unique on the same router.

If a VC changes its link protocol type and this causes a conflict with the other VCs, the VC is automatically deleted.

4.3.7 Both the session and the AC are up, but the VC cannot be up

Fault symptom

Figure 4-16 Networking diagram



As shown in Figure 4-16, the VC is not Up after you configure the Martini MPLS Layer 2 VPN. Check the session and the AC, and find both of them are Up.

Fault analysis

Use the **display mpls l2vc** *vc-id* command on PE to check the MTU value for consistency. For example:

# Check the MTU value of the Ethernet interface on PE1:

```
[PE1-Ethernet1/0/0] display mpls l2vc 100
 Total ldp vc : 1     0 up       1 down
 *Client Interface     : Ethernet1/0/0
```

```
  Session State        : up
  AC Status            : up
  VC State             : down
  VC ID                : 100
  VC Type              : ethernet
  Destination          : 2.2.2.2
  Local VC Label       : 119808
  Remote VC Label      : 25600
  Control Word         : Disable
  Local VC MTU         : 80
  Remote VC MTU        : 120
  Tunnel Policy Name   : --
  Traffic Behavior Name: --
  PW Template Name     : --
  Create time          : 0 days, 0 hours, 0 minutes, 4 seconds
  UP time              : 0 days, 0 hours, 0 minutes, 0 seconds
  Last change time     : 0 days, 0 hours, 0 minutes, 4 seconds
```

# View the MTU value of the Ethernet interface on PE2:

```
[PE2-Ethernet1/0/0] display mpls l2vc 100
 Total ldp vc : 1     0 up       1 down
 *Client Interface     : Ethernet1/0/0
  Session State        : up
  AC Status            : up
  VC State             : down
  VC ID                : 100
  VC Type              : ethernet
  Destination          : 1.1.1.1
  Local VC Label       : 25600
  Remote VC Label      : 119808
  Control Word         : Disable
  Local VC MTU         : 120
  Remote VC MTU        : 80
  Tunnel Policy Name   : --
  Traffic Behavior Name: --
  PW Template Name     : --
  Create time          : 0 days, 0 hours, 0 minutes, 14 seconds
  UP time              : 0 days, 0 hours, 0 minutes, 0 seconds
  Last change time     : 0 days, 0 hours, 0 minutes, 14 seconds
```

The display shows that the MTU value of the local end is not consistent with that of the remote end, which leads to parameter negotiation failure.

Modify the interface MTU value on either PE to make the MTU value consistent at both ends.

For example, change the MTU value of the interface on PE2 to make it consistent with that on PE1:

```
[PE2-Ethernet1/0/0] mtu 80
[PE2-Ethernet1/0/0] shutdown
[PE2-Ethernet1/0/0] undo shutdown
```

After modification, the VC becomes Up:

```
[PE2-Ethernet1/0/0] display mpls l2vc 100
 Total ldp vc : 1     1 up       0 down
 *Client Interface     : Ethernet1/0/0
```

```
Session State        : up
AC Status            : up
VC State             : up
VC ID                : 100
VC Type              : ethernet
Destination          : 1.1.1.1
Local VC Label       : 25600
Remote VC Label      : 119808
Control Word         : Disable
Local VC MTU         : 80
Remote VC MTU        : 80
Tunnel Policy Name   : --
Traffic Behavior Name: --
PW Template Name     : --
Create time          : 0 days, 0 hours, 0 minutes, 14 seconds
UP time              : 0 days, 0 hours, 0 minutes, 0 seconds
Last change time     : 0 days, 0 hours, 0 minutes, 14 seconds
```

Troubleshooting procedure

Step 1 Check that the MTU value is consistent at both ends.

Step 2 If inconsistency occurs, modify the MTU value on either end to ensure consistency.

Step 3 Use the **shutdown** command and then the **undo shutdown** command on the modified interface.

----End

Summary

PWE3 has extended Martini interface parameters. Some of the parameters must be supported, and some of them do not. Some of the parameters must match while some of them need not match during the negotiation.

The following lists the Martini interface parameters.

Code	Length	Description
0x01	4	Interface MTU in octets
0x02	4	Maximum number of concatenated ATM cells
0x03	up to 82	Optional Interface Description string
0x04	4	CEM [8] payload bytes
0x05	4	CEM options

The following shows the PWE3 interface parameters.

Code	Length	Description
0x01	4	Interface MTU in octets

Code	Length	Description
0x02	4	Maximum number of concatenated ATM cells
0x03	Up to 82	Optional Interface Description string
0x04	4	CEP/TDM payload bytes
0x05	4	CEP options
0x06	4	Requested VLAN ID
0x07	6	CEP/TDM bit-rate
0x08	4	Frame-Relay DLCI Length
0x09	4	Fragmentation indicator
0x0A	4	FCS retention indicator
0x0B	4/8/12	TDM options
0x0C	4	Virtual Circuit Connectivity Verification (VCCV) parameter

Items from 0x06 to 0x0C are extended in PWE3.

Currently, the Secure Router 8000 Series supports the MTU, Maximum ATM cell number, Fragmentation and VCCV, but does not support the Request VLAN ID. You can set the same VLAN ID for the AC interface at both ends to rectify the problem of not supporting the Request VLAN ID.

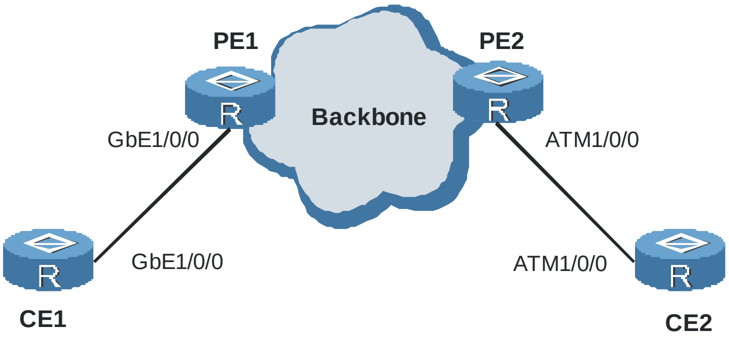
When configuring interface parameters, note the following:

- You must specify the same MTU for the Ethernet-type interface; otherwise, the PW cannot be Up.
- In ATM cell (0x0003 ATM transparent cell transport, 0x0009 ATM n-to-one VCC cell transport and 0x000A ATM n-to-one VPC cell transport) mode, the maximum ATM cell number must be sent to the peer in order to inform the peer how many cells it can handle at a time. When the remote end encapsulates packets, this number must not increase. Inconsistency of the cell number at both ends does not affect the status of a PW.
- Fragmentation and ATM cell handling mode are consistent at both ends. The configuration of fragmentation and ATM cell handling mode is optional. The local end only informs the remote end whether it can perform reassembly; whether the remote fragments packets depends on the packet size and its fragmentation capability. The fragmentation capability does not affect the status of a PW, and it is not necessary to be the same.
- VCCV processing is similar to ATM cell and fragmentation capability in terms of function. The VCCV configuration is optional. VCCV informs the remote of its VCCV capability. When performing VCCV, the peer chooses a path (CC) and a method (CV) according to the configuration at both ends. VCCV does not affect the status of a PW, and does not need to be consistent at both ends.
- The Request VLAN ID informs the peer of its capability. During forwarding, the remote is required to push a VLAN ID on its Layer 2 frame header. This configuration is optional. If you use the Request VLAN ID, the VLAN ID can be different at both ends.

4.3.8 Ethernet interconnects with ATM, the VC is up, but the ping between CEs fails

Scenario

Figure 4-17 Networking diagram



As shown in Figure 4-17, Ethernet interconnects ATM. After Layer 2 VPN IP-interworking is configured, the VC at both ends is Up, but the ping between CEs fails.

Fault analysis

Check whether the IP address of the two CEs is on the same network segment. The address of the two ends must be on the same network segment.

Use the **display local-ce mac** command on PE, and use the **display arp** command on CE to check the establishment of ARP entries of the Ethernet link.

If ARP entries are not set up successfully, configure the IP address and the MAC address for the Ethernet interface of CE on PE and also enable MAC broadcasting on PE. That is, run the **local-ce ip** command, the **local-ce mac** command and the **local-ce mac broadcast** command on PE.

For detailed configuration, see *Nortel Secure Router 8000 Series Configuration Guide - VPN* (NN46240-507).

NOTE

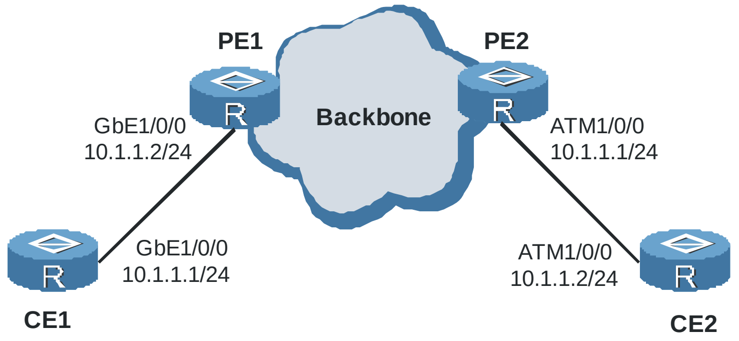
The IP address configured on PE is that of the corresponding interface on the remote CE.

For ARP entries of the ATM link, you can use one of the two methods:

- Use INARP to generate MAP dynamically. Figure 4-18 shows an example to configure IP addresses. The configuration is as follows:

```
[PE2] interface atm1/0/0
[PE2-Atm1/0/0] pvc 100/200
[PE2-atm-pvc-Atm1/0/0-100/200] map ip inarp broadcast
[PE2-atm-pvc-Atm1/0/0-100/200] ip address 10.1.1.1 255.255.255.0
[CE2] interface atm1/0/0
[CE2-Atm1/0/0] pvc 100/200
[CE2-atm-pvc-Atm1/0/0-100/200] map ip inarp broadcast
[CE2-atm-pvc-Atm1/0/0-100/200] ip address 10.1.1.2 255.255.255.0
```

Figure 4-18 IP address configuration diagram



- Use static MAP. Configure the **map ip** *peer-ce-address* **broadcast** command or the **map ip default broadcast** command in the PVC view of the ATM interface at both ends of the AC.

  For example:

```
[PE2] interface atm1/0/0
[PE2-Atm1/0/0] pvc 100/200
[PE2-atm-pvc-Atm1/0/0-100/200] map ip 10.1.1.2 broadcast
[PE2-atm-pvc-Atm1/0/0-100/200] ip address 10.1.1.1 255.255.255.0
[CE2] interface atm1/0/0
[CE2-Atm1/0/0] pvc 100/200
[CE2-atm-pvc-Atm1/0/0-100/200] map ip 10.1.1.1 broadcast
[CE2-atm-pvc-Atm1/0/0-100/200] ip address 10.1.1.2 255.255.255.0
```

Troubleshooting procedure

Step 1 Check that the IP address of CE at both ends is on the same network segment.

Step 2 Run the **display local-ce mac** command on PE and run the **display arp** command on CE to check whether ARP entries of the Ethernet link establish successfully.

Step 3 If ARP entries are not set up successfully, configure an IP address and MAC address for the AC interface of Ethernet type and enable MAC broadcasting on PE. For the ATM link, use INARP to generate MAP dynamically or use static MAP.

----End

Summary

In IP-interworking applications, if the VC is Up but the ping between CEs fails, the cause is often configuration error.

You must perform configuration according to the link type, so that ARP entries can generate correctly.

4.3.9 CEs cannot communicate by using the accessing mode of VLAN

Fault symptom

CEs adopt the accessing mode of VLAN. After the VLAN ID is changed, CEs on two ends cannot communicate.

Fault analysis

To modify the VLAN ID, you need to modify VC IDs of the AC interfaces along the packet-sending direction in turn. To make sure the modification takes effect, run the **shutdown** command and then the **undo shutdown** command on each VLAN interface.

Troubleshooting procedure

Step 1 Use the **vlan-type** command on the AC interfaces along CE to PE and PE to CE direction to modify the VLAN ID.

Step 2 Use the **shutdown** command on the AC interfaces to disable the interfaces.

Step 3 Use the **undo shutdown** command on the interfaces to enable them.

----End

Summary

When the VLAN access is adopted between CE and PE, the minimum VLAN ID of interfaces on both ends of the AC that the packet passes by must be consistent. Otherwise, the packet cannot be forwarded normally.

The minimum VLAN IDs of the CE interfaces on both ends of the tunnel can be different.

4.3.10 CEs cannot access each other though the static VC is up

Fault symptom

After the static VC is configured, the static VC is Up. CEs, however, cannot access each other.

For example:

```
[PE1] display mpls static-l2vc
 Total svc connections:  1,  1 up,  0 down

 *Client Interface     : Ethernet2/0/1 is up
  AC Status            : up
  VC State             : up
  VC ID                : 0
  VC Type              : ethernet
  Destination          : 2.2.2.2
  Transmit VC Label    : 200
  Receive VC Label     : 100
  Control Word         : Disable
  VCCV Capability      : Disable
  Tunnel Policy Name   : --
  Traffic Behavior     : --
  PW Template Name     : --
  Create time          : 0 days, 0 hours, 0 minutes, 17 seconds
  UP time              : 0 days, 0 hours, 0 minutes, 17 seconds
  Last change time     : 0 days, 0 hours, 0 minutes, 17 seconds
```

Fault analysis

Check the label of the static VC on the PE of the opposite end:

```
[PE2] display mpls static-l2vc
 Total svc connections:  1,  1 up,  0 down

 *Client Interface     : Ethernet1/0/1 is up
  AC Status            : up
  VC State             : up
  VC ID                : 0
  VC Type              : ethernet
  Destination          : 1.1.1.1
  Transmit VC Label    : 200
  Receive VC Label     : 100
  Control Word         : Disable
  VCCV Capability      : Disable
  Tunnel Policy Name   : --
  Traffic Behavior     : --
  PW Template Name     : --
  Create time          : 0 days, 0 hours, 0 minutes, 17 seconds
  UP time              : 0 days, 0 hours, 0 minutes, 17 seconds
  Last change time     : 0 days, 0 hours, 0 minutes, 17 seconds
```

You can see that the label configuration on the local PE is different from that of the peer.

CEs can communicate after the following configuration:

```
[PE1-Ethernet2/0/1] mpls static-l2vc destination 2.2.2.2 transmit-vpn-label 100
receive-vpn-label 200
```

Troubleshooting procedure

Step 1 Delete the static VC on one end and reconfigure it.

----End

Summary

When the label of the static VC is incorrect, the data cannot forward normally even though the VC is Up.

When you configure the static VC, note the following:

- The local **transmit-vpn-label** and the remote **receive-vpn-label** are consistent.
- The local **receive-vpn-label** and the remote **transmit-vpn-label** are consistent.

4.3.11 VC is down though AC is up

Fault symptom

After the configuration of Layer 2 VC, the AC is Up. However, the ping of the peer fails. After using the **display mpls l2vc** command, you will find the status of the VC is Down and all the remote VC label and the remote VC MTU are zeros, which are invalid.

```
[PE] display mpls l2vc
 Total ldp vc : 1     0 up       1 down

 *Client Interface     : Atm5/0/0
  Session State        : up
  AC Status            : up
  VC State             : down
  VC ID                : 100
  VC Type              : ppp
  Destination          : 3.3.3.3
  Local VC Label       : 119809
  Remote VC Label      : 0
  Control Word         : Disable
  Local VC MTU         : 1500
  Remote VC MTU        : 0
  Tunnel Policy Name   : --
  Traffic Behavior Name: --
  PW Template Name     : --
  Create time          : 0 days, 0 hours, 20 minutes, 16 seconds
  UP time              : 0 days, 0 hours, 0 minutes, 0 seconds
  Last change time     : 0 days, 0 hours, 4 minutes, 9 seconds
```

Fault analysis

Possible causes are:

- The encapsulation types on two ends are different.
- The peer is not configured with VC.

Troubleshooting procedure

Step 1 Check that the correct peer addresses are configured on PEs of two ends.

Step 2 Check that the VC IDs on two ends are consistent.

Step 3 Check that the encapsulation types on two ends are consistent.

Step 4 Check that the local VC MTU and the remote VC MTU are consistent.

Step 5 Check that the control word is enabled or disabled on both ends.

----End

Summary

VC uses LDP as the signaling. The negotiation of following parameters is required:

- VC type

- Control word
- MTU

Thus, the VC status can be Up only when those parameters are consistent on both ends.

4.3.12 Large-sized packets are lost between CEs on two ends of Layer 2 VPN

Fault symptom

After the Layer 2 VPN is set up between CEs, some large-sized packets are lost.

Fault analysis

The cause can be due to the fragmentation of the large-sized packets. The fragmentation can be caused by the MTU on the AC interfaces or the receiving interface is smaller than the MTU of the source interface.

Troubleshooting procedure

Step 1 Use the **display interface** command on the source interface to check the MTU.

Step 2 Use the **display interface** command on the PEs that the packet passes by to check whether AC interfaces exist with MTU values smaller than the MTU of the source interface.

Step 3 Use the **mtu** command in the AC interface view on CE or PE to increase the MTU value and ensure the packet sent by CE is not fragmented.

----End

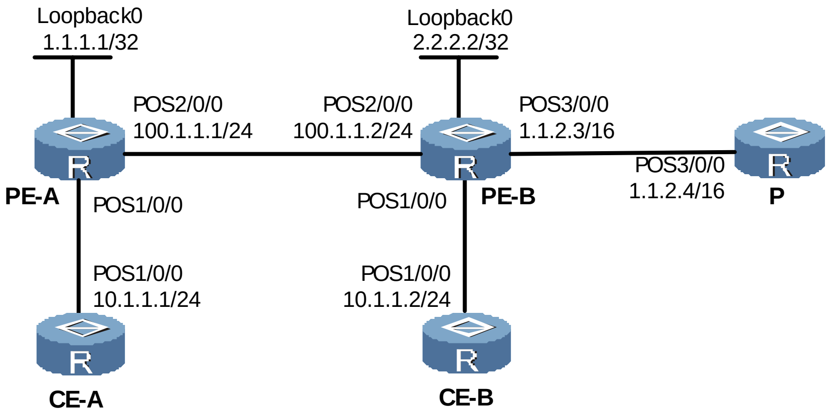
Summary

When CEs connect through the Layer 2 VPN, the sent packet passing through PEs cannot fragment. Otherwise, the packet cannot be received normally.

4.3.13 Failure to establish the MPLS LDP session between PEs when RIP-1 is used in the Layer 2 VPN backbone

Fault symptom

Figure 4-19 Networking diagram of the Layer 2 VPN backbone adopting RIP



After the Layer 2 VPN backbone network that runs RIP-1 advertises the local loopback0 address and the interface IP address, the MPLS LDP session between PEs cannot be set up.

The prompt on PE-A is as follows:

```
Del Session : EncdecEncode ldp notify msg failure.
```

Check the MPLS LDP session on PE-A. The display is as follows:

```
[PE-A] display mpls ldp session
         LDP Session(s) in Public Network
---------------------------------------------------------------------------
Peer-ID        Status     LAM  SsnRole  SsnAge     KA-Sent/Rcv
---------------------------------------------------------------------------
2.2.2.2:0      NonExistent     Passive          0/0
---------------------------------------------------------------------------
LAM : Label Advertisement Mode      SsnAge Unit : DDD:HH:MM
```

The prompt on PE-B is as follows:

```
Del Session : Tcp connection down
```

Check the MPLS LDP session on PE-B. The display is as follows:

```
 [PE-A] display mpls ldp session
         LDP Session(s) in Public Network
---------------------------------------------------------------------------
Peer-ID        Status     LAM  SsnRole  SsnAge     KA-Sent/Rcv
---------------------------------------------------------------------------
1.1.1.1:0       Initialized      Active        0/0
---------------------------------------------------------------------------
```

```
LAM : Label Advertisement Mode      SsnAge Unit : DDD:HH:MM
```

Fault analysis

Check the routing table on PE-B. The display is as follows:

```
[PE-B] display ip routing-table
Routing Tables: Public
         Destinations : 10       Routes : 10

Destination/Mask    Proto  Pre  Cost       NextHop         Interface

        1.0.0.0/8   RIP    100  1          100.1.1.1       Pos2/0/0
        1.1.0.0/16  Direct 0    0          1.1.2.3         Pos3/0/0
        1.1.2.3/32  Direct 0    0          127.0.0.1       InLoopBack0
        1.1.2.4/32  Direct 0    0          1.1.2.4         Pos3/0/0
        2.2.2.2/32  Direct 0    0          127.0.0.1       InLoopBack0
      100.1.1.0/24  Direct 0    0          100.1.1.2       Pos2/0/0
      100.1.1.1/32  Direct 0    0          100.1.1.1       Pos2/0/0
      100.1.1.2/32  Direct 0    0          127.0.0.1       InLoopBack0
      127.0.0.0/8   Direct 0    0          127.0.0.1       InLoopBack0
      127.0.0.1/32  Direct 0    0          127.0.0.1       InLoopBack0
```

RIP-1 can identify only the route of the natural segment such as Class A, B, and C.

In the routing table of PE-B, two routes to peer 1.1.1.1 exist:

- The IP address 1.0.0.0/8 learned by RIP-1.
- The IP address 1.1.0.0/16 that directly connects with PE-B.

According to the longest matching rule, the packet is sent to POS 3/0/0 whose IP address is 1.1.0.0/16. In the network segment connected with POS 3/0/0, the loopback address 1.1.1.1/32 does not exist. Therefore, the MPLS LDP session cannot be set up.

Troubleshooting procedure

Step 1 Replace RIP-1 with RIP-2 to advertise the 32-bit loopback address. This address serves as the MPLS LDP session address, on the PE.

----End

Summary

RIP-1 can identify only the route of the natural segment such as Class A, B and C. Use RIP-2 to advertise the 32-bit loopback address of PE.

4.4 FAQs

Q: How can I run Martini mode on the existent version?

A: The Secure Router 8000 Series defaults to run PWE3 and also supports compatibility with Martini mode. If the router is required to work only in Martini mode, use the **mpls l2vpn default martini** command in the system view.

You can use the **undo mpls Layer 2 VPN default martini** command to restore PWE3 mode.

If a VC has been configured, such a type of switching cannot be done.

Q: In what cases do I configure local-ce and local-mac in different media interworking?

A: You must configure the **local-ce** and **local-mac** when you configure IP-interworking encapsulation on an Layer 2 VPN Ethernet interface or subinterface on PE. After a Layer 2 VPN Ethernet interface is IP-interworking encapsulated, it learns MAC addresses in a new way. Accordingly, its ARP entries are different from ordinary ARP entries.

When PE receives an ARP request from CE through an IP-interworking encapsulated Layer 2 VPN ingress interface, PE responds with its own MAC address regardless of the destination. At this time, an Ethernet interface or subinterface of PE can connect only one CE, but cannot connect multiple CEs through a hub or LAN switch. When an Ethernet interface or subinterface of PE connects multiple CEs, PE can learn unhelpful MAC addresses, which can cause forwarding failure.

Q: What special configuration should be done on an FR interface? What is the configuration guideline when CE acts as DCE and PE functions as DTE?

A: When you configure FR, note that:

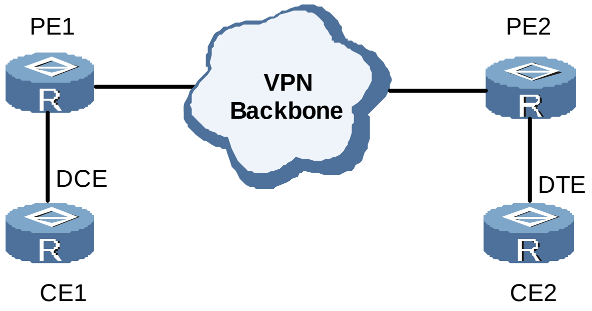
- You must configure a VC ID for a DCE or NNI interface regardless of whether it is a main interface or a subinterface.
- For a DTE interface, if it is a main interface, the system automatically determines its VC ID based on the remote device; if it is a subinterface, you must manually specify a VC ID for it.

When CE adopts FR to access PE, there is no special requirement on the interface that connects with CE on the PE.

In the two CEs setting up the connection, the interface that connects with PE on one CE is specified as DCE while that of another CE is specified as DTE.

Refer to Figure 4-20.

Figure 4-20 Networking scheme using DCE and DTE as the interface types



If you configure LSP, configure link mapping to permit the broadcast packets if PEs are connected through Non Broadcast Multiple Access (NBMA) network such as FR, ATM, and X.25.

Q: What is the function of the control word in Layer 2 VPN?

A: The control word on the PWE3 control plane is represented by a bit. The VC can be Up only when the control word at both ends is the same.

If the forwarding plane supports the control word, a 32-bit field is added to the data packet to show the packet order. Generally, disorder can occur in the case of load balancing.

When PEs connect through the Ethernet, and PE and CE connect in a PPP fashion, PPP negotiation fails because the control packet of PPP is too small, less than the minimum MTU supported by the Ethernet. In this case, the control word is used as padding to avoid this problem.

Q: Can I specify multihop VCs with the same peer and different encapsulation types when I configure switch-Layer 2 VC on SPE?

A: Yes, you can. A VC is determined by the combination of the VC ID and the VC type.

Q: Can I set the PW ID to 0 or ignore the configuration?

A: Yes, you can. You can set a PW ID for a static PW or choose not to set it. A static PW with a PW ID of 0 cannot switch with other PWs.

Q: How can I configure Layer 2 VPN load balancing?

A: Load balancing uses multiple tunnels to carry a PW. Data payload is divided among these tunnels and forwarded by them. The number of load balancing tunnels is determined by the permit file.

When you configure load balancing, you need to specify a tunnel selection policy, that is, specify a policy name when you configure VCs.

Q: What does the multihop mean in Layer 2 VPN? In what cases is multihop used? How can I configure multihop?

A: Layer 2 VPN multihop is a type of technology used to implement interworking between CEs, which connect multiple VCs.

When a VC must cross an AS, or no direct tunnel exists but multiple tunnel segments between two UPEs exist, configure multihop. With multihop, the network operation has lower requirement on the performance of the access device.

UPE cannot judge whether the remote is a UPE or SPE, so the configuration on UPE is the same as that in single-hop case. Regard the SPE as the remote. Configuration on SPE involves three scenarios:

- Dynamic to dynamic: Both sides are dynamic.
- Static to static: Both sides are static.
- Mixed: One side is dynamic and the other is static.

Q: Why can the same Layer 2 VC be configured with two types of encapsulation when MPLS switch-Layer 2 VC is configured on SPE?

A: In the following example, the same Layer 2 VC is configured with two types of encapsulation when MPLS switch-Layer 2 VC is configured on SPE:

```
[Nortel] mpls switch-l2vc 1.1.1.1 2345 between 2.2.2.2 1234 encapsulation
ip-interworking
[Nortel] mpls switch-l2vc 1.1.140.3 2345 between 1.1.140.2 1234 encapsulation hdlc
```

A combination of VC ID and VC type identifies a VC uniquely in PWE3. When the VC ID is the same, but the VC type differs, two VCs are determined.

Q: What are the conditions for a PW being up?

A: In a SVC, if a PW is to be Up the conditions are: the local AC is Up and the tunnel is Up. You can use the **display mpls static-l2vc interface** command to check the PW status.

In LDP, the conditions for a PW status of Up are:

- The local AC is Up.
- The tunnel is Up.
- The LDP session is Up.
- The MTUs, VC types, and control words are consistent on both ends.

You can use the **display mpls l2vc interface** command to check the PW status.

Q: What are the differences between tag or untagged configuration in the Ethernet interface view and tagged or raw configuration in the PWE3 view?

A: The tag or untagged mode of an Ethernet interface has no direct relation with the tagged or raw mode of a PWE3 tunnel.

- The tag or untagged mode of an Ethernet interface identifies a VLAN and a subinterface that receives packets sent from AC. By default, Ethernet packets are untagged and VLAN packets are tagged.
- The tagged or raw mode of PWE3 sets the PWE3 payload to carry a VLAN tag. A PWE3 packet coming out of a tunnel finds its egress based on the tagged or raw configuration.

The fact that the PWE3 packet carries the VLAN tag does not imply that the Ethernet interface bound with the PWE3 tunnel is configured with the VLAN tag.

Specifying the PWE3 with the Raw mode, you can realize the switching function of the VLAN tag. For example, the local AC interface is the Ethernet main interface while the remote is the Ethernet subinterface:

- The packet is received on the Ethernet main interface and the packet is untagged. The VLAN tag is not added to the packet because the mode of PWE3 is Raw. When the PWE3 tunnel sends the packet to the remote end, the VLAN tag is added to the packet because the egress is an Ethernet subinterface.
- After the remote Ethernet subinterface receives the packet with the VLAN tag, according to the Raw mode, the interface removes the VLAN tag and sends out the packet from the Ethernet main interface.

If both ends of a PW are a VLAN subinterface in tag mode, they must use the same VLAN tag. Otherwise, the packet is discarded.

In Q-in-Q mode, packets entering a tunnel carry multiple layers of tags. If the mode of PW is Raw, the outer tag of the packet is removed before the packet is forwarded to the remote tunnel end.

For a VLANIF interface, the VLAN packet does not carry a VLAN tag by default. If PWE3 is configured in tag mode, the forwarding engine adds a default VLAN tag to packets. The main Ethernet interface can emulate the default VLAN and make packets be in default VLAN mode.

Therefore, when you configure PWE3 on the interface of Ethernet type, you can configure the packet to be tagged or untagged manually instead of judging from the interface type.

Q: After CEs adopt the ATM to access PEs, all the CE interfaces and PE interfaces are up. Why can the CEs on two ends not ping through each other?

A: Check and ensure the PVC of the interface that connects with CE on the PE, and that of the interface that connects with PE on the CE are consistent.

4.5 Diagnostic tools

4.5.1 display commands

Command	Description
display mpls l2vc	Displays information about Layer 2 VC.
display tunnel-info	Displays information about tunnels.
display mpls lsp	Displays information about LSPs.
display mpls ldp	Displays information about LDP.
display mpls Layer 2 VPN connection	Displays information about the Layer 2 VPN using BGP as the signaling.
display mpls Layer 2 VPN	Displays the MPLS Layer 2 VPN information.

display mpls l2vc

# View information on the bound Layer 2 VC of a specified interface:

```
<Nortel> display mpls l2vc interface ethernet1/0/0
 *Client Interface : Ethernet1/0/0 is up
  Session State    : up
  AC State         : up
  VC State         : up
  VC ID            : 10
  VC Type          : ethernet
  Destination      : 2.2.2.2
  Local Group ID   : 0
  Remote Group ID  : 0
  Local VC Label   : 17408
  Remote VC Label  : 17408
  Local VC MTU     : 1500
  Remote VC MTU    : 1500
  Local VCCV       : Disable
  Remote VCCV      : Disable
  Local Frag       : Disable
  Remote Frag      : Disable
  Local Ctrl Word  : Disable
  Remote Ctrl Word : Disable
  Tunnel Policy    : --
  Traffic Behavior : --
  PW Template Name : --
  VC tunnel/token info : 1 tunnels/tokens
   NO.0  TNL Type : lsp   , TNL ID : 0x1002000
  Create time      : 0 days, 0 hours, 2 minutes, 13 seconds
  UP time          : 0 days, 0 hours, 0 minutes, 39 seconds
  Last change time : 0 days, 0 hours, 0 minutes, 39 seconds
```

display tunnel-info

# View information on all tunnels:

```
<Nortel> display tunnel-info all
 * -> Allocated VC Token
Tunnel ID           Type                 Destination          Token
----------------------------------------------------------------------
0x1002000           lsp                   2.2.2.2               0
0x51002001          local ifnet           --                    1
```

4.5.2 debugging commands

Command	Description
debugging mpls Layer 2 VPN	Debugs Layer 2 VPN.
debugging mpls packet	Debugs MPLS packets.

Contents

Figures

5 VPLS troubleshooting

About this chapter

The following table describes the contents of this chapter.

Section	Describes
5.1 VPLS overview	This section describes the knowledge you need before you troubleshoot VPLS.
5.2 VPLS troubleshooting	This section provides notes about configuring VPLS, the VPLS troubleshooting flowchart, and the troubleshooting procedure in a typical VPLS network.
5.3 Troubleshooting cases	This section presents several troubleshooting cases.
5.4 FAQs	This section lists frequently asked questions and their answers.
5.5 Diagnostic tools	This section describes common diagnostic tools: **display** commands and **debugging** commands.

5.1 VPLS overview

This section covers the following topics:

- Related concepts of VPLS
- Encapsulation type
- MTU

The development of Ethernet has made it a dominant LAN technology and it is increasingly applied as an access solution in the Metropolitan Area Network (MAN) and in the Wide Area Network (WAN).

Virtual Private LAN Service (VPLS) connects more than one Ethernet LAN segment through the Packet Switched Network (PSN), to enable them to operate as if in a LAN.

VPLS is also called Transparent LAN Service (TLS) or Virtual Private Switched Network service (VPSN). Unlike the common Layer 2 VPN point-to-point service, service providers use VPLS to offer Ethernet-based multi-point service over the MPLS backbone network.

5.1.1 Related concepts of VPLS

PW

A Pseudo Wire (PW) is a virtual connection that transmits frames between two provider edges (PE). In the VPLS packet, PW corresponds to the inner label.

The PE sets up and maintains a PW, at both ends.

The setup of a PW is a process of generating local and remote labels by using signaling. Currently, the Secure Router 8000 Series supports Label Distribution Protocol (LDP) signaling and Border Gateway Protocol (BGP) signaling.

The following conditions must be met before the PW status is Up:

- At least one AC is Up at the local end.
- At least one Virtual Switch Instance (VSI) is Up at the remote end, and the negotiation parameters are consistent at both ends of the PW.

Tunnel

A tunnel is a direct virtual path, that transparently transmits data.

The VPLS tunnel carries PWs. Multiple PWs can be delivered on a single tunnel. To set up a PW to the remote end, a tunnel to the remote end must be available first.

The tunnel is set up by the tunnel management module. VPLS queries the tunnel against the tunnel management module according to the remote destination address of a PW. If no tunnel to the remote destination address exists, the PW cannot be set up.

VPLS supports using the tunnel policy to choose a tunnel.

AC

The customer edge (CE) connects the PE through the Attachment Circuit (AC) in a Layer 2 VPN.

An AC can be either a physical link or a logical link. AC transfers frames between CE and PE. You can specify a remote PE as the AC side of the local VPLS (**upe** often used). The specified PE need not fully connect with other PEs or perform split horizon.

Similar to that in the distance vector (DV) routing protocol, the split horizon in VPLS can reduce the bandwidth consumption and prevent the loop.

VSI

VSI implements the bridging function.

In VPLS, a VSI on the PE represents a VPN. A PE can have multiple VPNs. Therefore, a PE can be configured with multiple VSIs. Each VSI provides separate VPLS service.

5.1.2 Encapsulation type

Packet encapsulation on the AC

Packet encapsulation on the AC is determined by the user access mode. Two user access modes are available:

- VLAN access: In this mode, the Ethernet frame sent upstream from the CE or sent downstream from the PE contains a VLAN tag in the frame header. This tag is a service delimiter used by the Internet Service Provider (ISP) to differentiate users. This type of tag is a P-tag.
- Ethernet access: In this mode, the Ethernet frame sent upstream by CE or sent downstream by PE does not contain a P-tag. If the frame contains a VLAN tag in its header, this tag is an internal VLAN tag and is of no significance for PE. This type of internal VLAN tag is a U-tag.

You can specify the access mode of the user on the device.

Packet Encapsulation on the PW

Two types of packet encapsulation exist on the PW.

- Raw mode: In this mode, the P-tag is not transmitted over the PW.
  If the upstream packets on CE contain the service delimiter, their service delimiter is removed before they are sent upstream; two layers of MPLS labels are added before they are forwarded. If the upstream packets on CE do not contain a service delimiter, they are sent upstream directly; two layers of MPLS labels are added before they are forwarded. For downstream packets on PE, the service delimiter is added as needed before they are forwarded to CE. It is not allowed to rewrite or remove an existent tag.
- Tagged mode: In this mode the frame sent to the PW must contain a P-tag.
  If the upstream packets on CE contain the service delimiter, they are sent upstream directly without the P-tag removed; two layers of MPLS labels are added before they are forwarded. If the upstream packets on CE do not contain the service delimiter, a null tag is added and then sent upstream; two layers of MPLS labels are added before they are forwarded.

For downstream packets on PE, their service delimiter is rewritten, removed, or retained as needed before they are forwarded to CE.

5.1.3 MTU

In VPLS, the maximum transmission unit (MTU) refers to the maximum transmission unit of the link layer. The encapsulation type and the MTU are both regarded as the Layer 2 information and are processed.

The MTU of respective VPLS must be consistent in a same VPN. If inconsistency occurs, the PW cannot be set up successfully.

5.2 VPLS troubleshooting

This section covers the following topics:

- Typical networking
- Configuration notes
- Troubleshooting flowchart
- Troubleshooting procedures

5.2.1 Typical networking

Basic topology

Figure 5-1 Basic VPLS networking

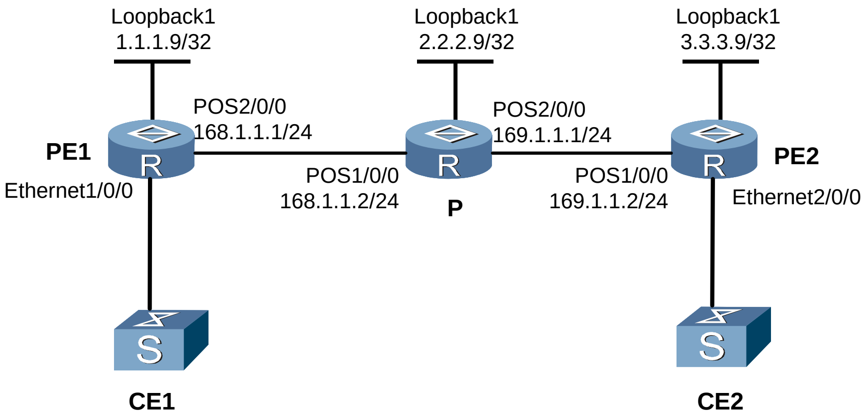


Figure 5-1 shows a basic VPLS topology and adopts the following solutions:

- CE1 and CE2 belong to the same VPN.
- The Interior BGP (IBGP) neighbor is set up between PE1 and PE2 to transmit VPN routing information carrying the inner label

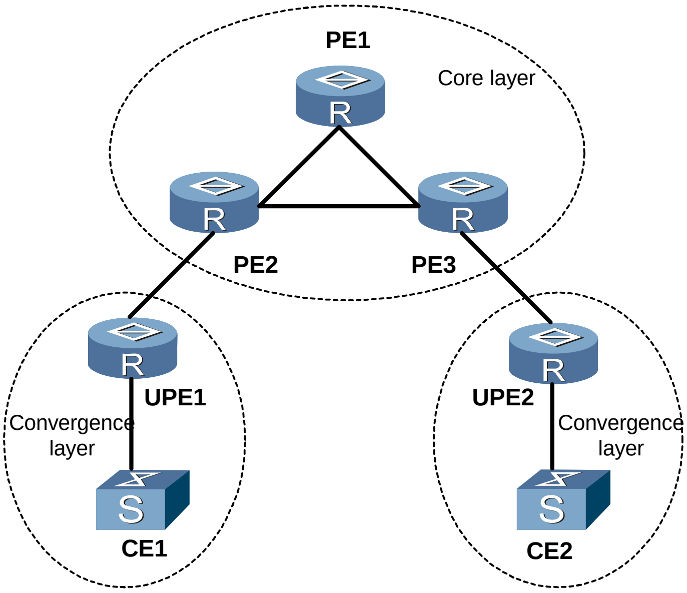
The PE1 and PE2 are user access devices on the public network, functioning like a Layer 2 device. For a packet sent from CE1, two layers (inner and outer) of MPLS labels are added before being forwarded. The packet is forwarded on the public network by using the outer label (that is, public network tunnel label). The corresponding VSI is found according to the inner label (that is, PW label) and the Layer 2 forwarding is performed and the packet is forwarded to CE2.

This networking simulates the three constitutional parts of a VPLS networking: PE, provider router (P), and CE.

This solution also meets the conditions of making a VPLS VSI Up: tunnel, AC access, and PW.

Hierarchical VPLS

Figure 5-2 Hierarchical VPLS Networking



The traditional LDP signaling requires that:

- PEs fully connect in a VPLS.
- Each PE is specified with a peer.

The configuration is quite arduous, and requires higher performance of individual PEs.

To rectify this problem, you can use hierarchical VPLS. The PEs in the network core still fully connect. A PE, as the user convergence device, only needs to be specified as a Underlayer PE (UPE) on its directly connected Superstratum PE (SPE).

5.2.2 Configuration notes

Item	Subitem	Notes
VSI	VSI creation	When you create a VSI, you need to specify a name for it. If you use BGP as the signaling protocol, choose the keyword **auto**; if you use LDP, choose the keyword **static**.
	VPLS encapsulation type and MTU of the VSI	By default, the encapsulation type is VLAN and the MTU is 1500 bytes. For the Virtual Leased Line (VLL) interworking, the encapsulation type is determined by the private network interface type of PE. ● For the Ethernet subinterface, the encapsulation type is VLAN. ● For the main interface of Ethernet, the encapsulation type is Ethernet. ● For the VLAN interface, the encapsulation type is VLAN. The private network interface type and the MTU must be consistent on the PE at both ends. When you configure the encapsulation type and the MTU: ● If you use BGP, you must configure them after router distinguisher (RD) configuration; otherwise, the system prompts that basic configuration must be performed first. ● If you use LDP, you must configure a VSI ID first.
	pwsignal (PW signaling protocol)	After you create a VSI, you must specify a signaling protocol, which can be LDP or BGP.
MAC address learning	Static MAC address entries	Each VSI has a MAC table. You can configure MAC entries in system view.
	Blackhole MAC address entries	
	MAC address learning capability	You need to configure MAC address learning in VSI view.

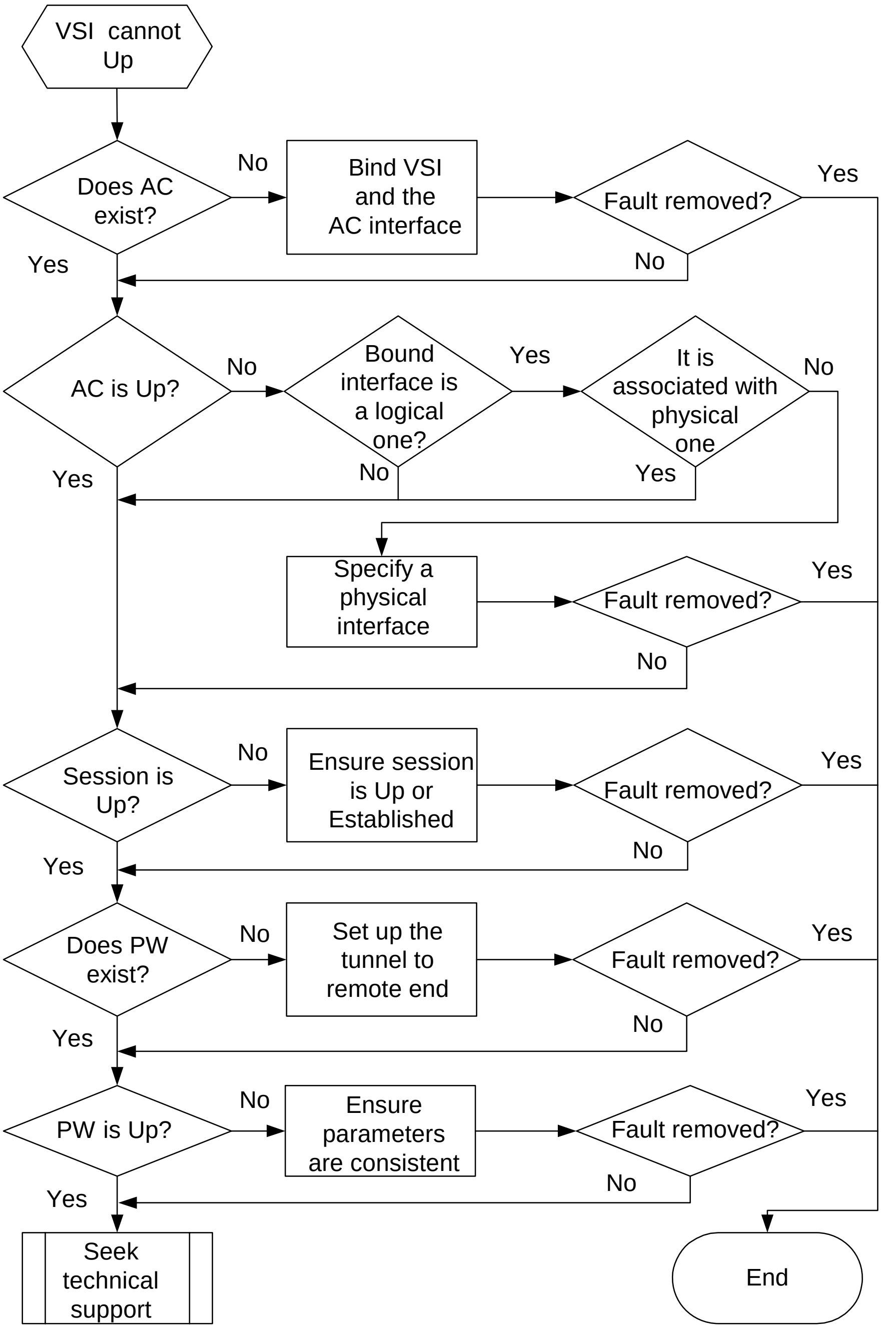
Item	Subitem	Notes
	MAC address learning mode	There are two VPLS MAC address learning modes: ● qualified: In this mode, the MAC address learning is based on the VLAN. Different VLANs in a same VSI instance can have different MAC address tables. ● unqualified: In this mode, the MAC address learning is based on the VSI. It is the default mode. MAC address learning mode does not affect interworking.
Handling of unknown frames received	Unknown-frame	You can specify the handling of unknown frames by using the **unknown-frame** { **unicast** | **multicast** } { **drop** | **local-handle** | **broadcast** } command in the VSI view.
VSI (in LDP signaling mode)	VSI peer	To establish a VPN in LDP signaling mode, you need to specify a peer by using the **peer** *peer-address* [**negotiation-vc-id** *vc-id*] [**tunnel-policy** *policy-name*] [**upe**] command. You must specify a VSI ID before you configure a peer. *peer-address* is often set to the loopback interface address of the peer. **negotiation-vc-id** refers to the VSI ID used for negotiation with the peer. This value is often used when the VSI ID is different at both ends but interworking is needed. *vc-id* cannot be the same as that of the other local VSIs and as that of the other local **negotiation-vc-id**. **tunnel-policy** specifies a tunnel policy used for communicating with the peer. This value should be an existent tunnel policy. **upe** indicates that the peer access mode is UPE.
	VSI-ID	You must specify a VSI ID in VSI LDP view. If **negotiation-vc-id** is not specified, this VSI ID is used to negotiate when you configure a peer. In this case, the VSI ID must be consistent with the remote VSI ID, and **negotiation-vc-id** must not be specified on the peer.

Item	Subitem	Notes
VSI (in BGP signaling mode)	VPN-Target	The VPN target is a label filtering policy used by VPLS in BGP signaling mode. Two VPN-target formats exist: *AS:nn* and *IP:nn*. *AS* represents the autonomous system number; *nn* is the user-defined figure; *IP* represents a local IP address. Ensure the association between the local VPN target attribute and the remote VPN target attribute: ● The local export-extcommunity attribute and the remote import-extcommunity attribute are consistent. ● The local import-extcommunity attribute and the remote export-extcommunity attribute are consistent. The traffic can flow in two-way only when the preceding two requirements are satisfied. The traffic can flow only in one-way if one of the two requirements is met. In general, the four values are configured consistent for convenience. You must specify an RD before you configure the VPN target.
	RD	RDs on a same router cannot be set to the same value.
	Site ID	Site ID is used to specify a VSI site, ranging from 0–65534. A site ID must be unique in a VPLS. The local site ID must not be larger than the sum of *range* and *default-offse*t of the peer. The local site ID must be larger than *default-offset* of the peer. *range* shows the number of sites in a VSI, with the maximum range of 1–65534. *default-offset* is 0 or 1.
Tunnel policy	tnl-policy	A tunnel policy is configured in the system view. VPLS specifies the policy to be used. Besides the VPLS tunnel policy you can specify a policy for a certain peer. By default, the LSP tunnel is chosen. You need to complete basic VPLS configuration before you configure a tunnel policy. In LDP mode, you need to configure a VSI ID first. In BGP mode, you need to specify an RD first.

Item	Subitem	Notes
AC	Binding of VSI and AC	Use the **l2 binding vsi** *vsi-name* command to bind the CE-bound interface with a VSI. Ensure that the AC interface is physically Up. (A logical interface is also required to be Up.) If the AC access mode is VLAN, you must configure a subinterface. If the mode is ATM, you need to configure a virtual circuit. When binding an Ethernet subinterface or an Ethernet trunk, you must configure a VLAN on the Ethernet subinterface.

5.2.3 Troubleshooting flowchart

Figure 5-3 VPLS troubleshooting flowchart



5.2.4 Troubleshooting procedures

The steps of troubleshooting are as follows:

Step 1 Check the status of the AC.

Run the **display vsi** *vsi-name* **verbose** command.

If the output does not include the Interface Name, it indicates that the VSI is not bound with the AC. You need to bind the CE-bound interface with the VSI.

For details, see 5.2.2 Configuration notes.

Step 2 Check the status of the session.

If the session is not set up, use the **display ip routing-table** command to check the route to the remote peer. If no route exists, configure a dynamic routing protocol or static route.

Step 3 Check the status of the PW or tunnel.

If the session is Up, check the status of the PW.

If no PW is available, the cause can be the absence of a tunnel to the peer. You can use the **display tunnel-info all** command to check the following:

- If the tunnel does not exist, configure the proper tunnel.
- If the tunnel exists, check if the peer of the VSI is specified and the peer is consistent with the peer that corresponds to the session.

Step 4 Check that parameters are consistent on both ends.

If the tunnel is normal, and the PW still cannot be set up, check that the encapsulation type, MTU, and VSI ID are consistent on both ends.

Ensure the local VPN target satisfies the following conditions:

- The local export-extcommunity and the peer import-extcommunity are consistent.
- The local import-extcommunity and the peer export-extcommunity are consistent.

The traffic can flow in the two-way mode only when the preceding two requirements are satisfied.

The traffic can flow only in the one-way mode if only one of the two requirements is met.

If the fault persists, use the **display current-configuration | begin vsi** *vsi-name* command to check the MAC address learning mode or contact the Nortel technical personnel.

NOTE

To make the configuration of the MAC address learning effective, run the **shutdown** command on the interface and then use the **undo shutdown** command.

----End

5.3 Troubleshooting cases

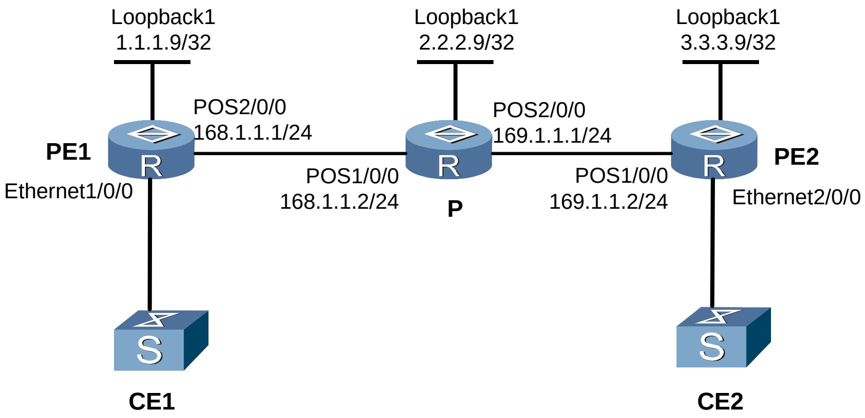
This section provides the following troubleshooting cases:

- A VSI cannot be up in LDP signaling mode
- Packets cannot forward successfully between two PEs though VSI is up
- A VSI cannot be up in BGP signaling mode

5.3.1 A VSI cannot be up in LDP signaling mode

Fault symptom

Figure 5-4 VPLS networking diagram



VPLS in LDP signaling mode is configured on both PE1 and PE2. After the configuration, the VSI cannot be Up.

Fault analysis

Step 1 Check the status of the VSI on PE1 and that on PE2.

Use the **display vsi verbose** command.

The display on PE1 is as follows:

```
VSI Name           : v1
    VSI Index                : 0
    PW Signaling             : ldp
    Member Discovery Style   : static
    PW MAC Learn Style       : unqualify
    Encapsulation Type       : vlan
    MTU                      : 1500
    VSI State                : down
    VSI ID                   : 1
   *Peer Router ID           : 3.3.3.9
    VC Label                 : 17409
    Session                  : up
    Tunnel ID                : 0x6002002,
    Interface Name           : Ethernet1/0/0
    State                    : up
```

The display on PE2 is as follows:

```
VSI Name                     : v1
      VSI Index                : 0
      PW Signaling             : ldp
      Member Discovery Style   : static
      PW MAC Learn Style       : unqualify
```

```
 Encapsulation Type      : vlan
 MTU                     : 1500
 VSI State               : down
 VSI ID                  : 1
*peer Router ID          : 2.2.2.9
 VC Label                : 17408
Session                  : up
Tunnel ID                : 0x6002001,
Interface Name           : Ethernet2/0/0
State                    : up
```

The AC at both ends is Up. The tunnel at both ends of a PW is existent, and the tunnel ID is not 0x0.

Step 2 Run the **display vsi remote ldp** command on PE2.

The display is as follows:

```
Vsi         Peer             VC      Group   Vsi         MTU      Vsi
ID          RouterID         Label   ID      Type        Value    Index
1           1.1.1.1          17409   0       vlan        1000     -
```

The preceding display shows that PE2 has a label to the remote.

Use the **display vsi remote ldp** command on PE1 and find that PE1 cannot receive the label of PE2.

It indicates that PE2 has problem.

Step 3 Check whether PE2 sends labels to PE1.

First, check that a remote peer is specified for PE2.

Find that the specified peer is not correct; it should be 1.1.1.9 rather than 2.2.2.9. Modify the peer.

----End

Troubleshooting procedure

Step 1 Run the **display vsi verbose** command on PE.

Step 2 Check the status of the VSI and that of the AC. Find that the VSI is Down but the AC is Up.

Step 3 Check the status of the PW. Find that the PW cannot be set up.

Step 4 Check whether the tunnel is existent. Find that the tunnel exists.

Step 5 Use the **display vsi remote ldp** command to check whether the remote label is received.

Step 6 If one end cannot receive the label from the remote end, check that the configuration of the remote peer is correct.

----End

Summary

If the signaling protocol is LDP and the VSI cannot be Up, the errors related to the peer are as follows:

- The IP address of the specified peer is incorrect.
- The address of the peer is not the peer LSR-ID. The LDP session cannot establish.
- The LSR-ID of the peer is redefined. Then the LDP session cannot be set up.

To enable the VSI status to be Up, at least two ACs must be Up, or at least one AC Up and one PW Up.

To locate this type of problem, begin by checking the status of the AC and that of the PW.

To enable an AC to be Up, you must bind the AC with an interface, and the current state of the interface must be Up.

The problem often occurs on the PW. To let a PW go Up, ensure that the MTU, encapsulation type, VSI ID, and remote peer configuration are correct. The key is that the local and remote ends can receive labels from each other.

You can use the **display vsi remote** { **ldp** | **bgp** } command to check them. You can judge which router has a configuration error based on whether it receives the label.

5.3.2 Packets cannot forward successfully between two PEs though VSI is up

Fault symptom

After the configuration of the VPLS, check the status of the VSI on PE. You will find the VSI is Up but the packets cannot forward successfully between two PEs.

Fault analysis

Step 1 Check whether the PW exists.

Use the **display vsi verbose** command to check whether the PW exists.

If the PW does not exist, it indicates the PW information is not delivered to the interface board.

If the PW exists, check whether the delivering status of the PW is OK.

- If not, it means the forwarding information is not delivered to the interface board, which leads to the failure of the forwarding.
- If the status is OK, check the operating status of the interface board.

Step 2 Check the MAC limit.

If the PW exists, packets cannot forward between PEs. Use the **display current-configuration | begin vsi** *vsi-name* command to check the MAC limit. If the MAC address entries exceed the MAC limit, reconfigure the MAC limit.

Step 3 Check whether the BGP peer is being re-established.

If the MAC address entries do not exceed the MAC limit, use the **display bgp peer** *peer-address* command to check whether the BGP peer is set up. When the BGP peer is being re-established, the VSI state remains Up for a very short period.

Step 4 Check the encapsulation modes of PEs on both ends.

If the BGP peer is set up, use the **display current-configuration | begin vsi** *vsi-name* command to check the encapsulation modes of PEs on both ends. If the modes are different, reconfigure them to be consistent.

----End

If the fault persists, contact the Nortel technical personnel.

Troubleshooting procedure

Step 1 Use the **display vsi** command to check that the status of the PW is Up.

Step 2 Use the **display vpls connection** command to check that the PW exists.

Step 3 Use the **display vpls fib** command to check that the delivering status of the PW is OK.

Step 4 If the status is OK, check that the operating status of the interface board is normal.

----End

Summary

In this case, the causes are as follows:

- The PW information is not delivered to the interface board.
- The MAC address entries exceed the MAC limit.
- When the BGP peer is being re-established, the VSI state remains Up for a very short period.
- The encapsulation modes on PEs of both ends are different.

5.3.3 A VSI cannot be up in BGP signaling mode

Fault symptom

See Figure 5-4.

IBGP runs between PE1 and PE2. A VSI is configured on them. After the configuration, you find that both the VSI on PE1 and that on PE2 cannot be Up.

Fault analysis

Step 1 Check the status of the VSI on PE1 and that on PE2.

Run the **display vsi verbose** command.

The display of PE1 is as follows:

```
***VSI Name               : bgp1
   VSI Index              : 0
   PW Signaling           : bgp
   Member Discovery Style : auto
   PW MAC Learn Style     : unqualify
   Encapsulation Type     : vlan
   MTU                    : 1500
   VSI State              : down
```

```
    BGP RD                : 1:1
    SiteID/Range/Offset   : 1/10/0
    Import vpn target     : 2:2,
    Export vpn target     : 2:2,
    Local Label Block     : 19456/10/0,
    Interface Name        : Ethernet6/0/1
    State                 : up
```

The display of PE2 is as follows:

```
***VSI Name               : bgp1
    VSI Index             : 0
    PW Signaling          : bgp
    Member Discovery Style : auto
    PW MAC Learn Style    : unqualify
    Encapsulation Type    : vlan
    MTU                   : 1500
    VSI State             : down
    BGP RD                : 1:2
    SiteID/Range/Offset   : 2/10/0
    Import vpn target     : 2:2,
    Export vpn target     : 2:2,
    Local Label Block     : 19456/10/0,
    Interface Name        : Ethernet6/0/1
    State                 : up
```

Step 2 Check whether the remote label has been received.

Use the **display vsi remote bgp** command on PE1 and on PE2. No information appears, which indicates that the remote label is not received.

It can be judged that BGP configuration has an error.

----End

Troubleshooting procedure

Step 1 Check the status of the AC. Find that the AC is Up at both ends.

Step 2 Run the **display vsi remote bgp** command. No output appears, which indicates that the label is not received.

Step 3 Check whether the VPN target matches.

Step 4 If the VPN target matches, ensure that the tunnel exists.

Step 5 If the tunnel exists, use the **display bgp peer all** command to check the setup of BGP adjacency.

Step 6 If the BGP adjacency is set up, use the **display bgp vpls all** command to check whether the remote label block is received.

Step 7 If the remote label block is not received, check BGP configuration. Find that the VPLS address family is not configured. Configure the VPLS address family to solve the problem.

----End

Summary

The differences between VPLS configuration in BGP signaling mode and that in LDP signaling mode are: the BGP mode requires that the VPLS address family be configured and the remote peer be enabled in the address family.

When you use BGP signaling, check that the BGP VPLS peer is specified and the remote label block is received. Whether a VSI can be Up is also affected by the status of the AC and that of PW as well as the encapsulation type and the MTU.

5.4 FAQs

Q: Why can the VSI not be up after a tunnel and an AC are established in VPLS configuration?

A: When you configure VPLS, note that:

- The VSI ID is consistent at both ends in LDP mode.
- The AC interface is bound with the VSI and the AC is in Up state.
- A tunnel to the remote end is available.
- The MTU and the encapsulation type are consistent at both ends.
- The status of the VSI peer is normal.
- In BGP mode, the VPN target matches at both ends.
- The ID of the local site falls in the range of the remote label block.
- Enable the remote peer in the BGP VPLS address family view.

Q: Why can the VPLS not be configured successfully on the VLAN interface?

A: Possible causes are:

- Other services are configured on the VLAN interface, such as MPLS/BGP VPN, multicast, or Virtual Leased Line (VLL).
- The status of the VLAN is Down.
- The Ethernet subinterface connects PE and P. (The Ethernet subinterface cannot be used to connect PE and P.)
- The site IDs of the VSI instances conflict with each other. For the same VPLS, site IDs of different sites must be different.
- No corresponding VSI instance is bound with PE.

Q: What are the requirements for the PW to be up in the configuration of VPLS?

A: The requirements are as follows:

- The parameters such as the encapsulation mode and MTU must be consistent on both ends.
- The status of AC is Up.
- The status of the tunnel is Up.
- The LDP session or the BGP remote peer exists between PEs.

Q: Different types of AC interfaces are bound at both ends. Does this affect the status of a VSI?

A: No, it will not. At present, the Secure Router 8000 Series supports only two types of AC interfaces:

- Ethernet
- VLAN

Q: Different types of AC interfaces are bound at both ends. Does this affect the interworking?

A: No, it will not.

Q: Different MAC address learning modes are configured at both ends. Does this affect the status of the VSI?

A: No, it will not. The status of the VSI is affected only when the MTU and the encapsulation type are not consistent at both ends. The MAC address learning mode, however, affects the packet forwarding.

Q: Should the status of a VIS be Up only after an AC is bound on the PE at both ends?

A: No, this condition is not necessary.

When you configure Hierarchical VPLS (HVPLS), you need to add the keyword **upe** to specify a peer. Then, the peer can be regarded as an AC. When a peer is specified as a UPE, as long as the corresponding VSI of the peer is Up, the PW can be Up even if the corresponding interface of the SPE is not bound with the VSI.

Q: Is it possible that only the same VSI on a peer PE is Up but it is Down on the other peer PEs?

A: Yes, this situation is possible. If two or more peer PEs of a VSI are specified as UPEs, and if the same VSI on one of the UPEs is Up, the VSI on other peer PEs can be Down.

Q: Should PEs fully connect in LDP mode?

A: As SPE, PEs must fully connect. As UPE, PEs do not necessarily fully connect.

Q: Should a VSI be UP only when the VSI IDs are consistent at both ends?

A: No, not always. When you configure a peer, you can use the **negotiation-vc-id** command to configure the negotiation VSI ID. If both ends use it, interworking can also be implemented.

Q: Does negotiation-vc-id have a connection with UPE?

A: No, it does not. **negotiation** is used only as a parameter.

Q: The LSP token is inconsistent with the token of the current tunnel in the VPLS MID table. Why does this happen?

A: The LSP token refers to the token value of the PW in the multicast mnformation description (MID) table, and cannot be compared with the tunnel value.

Q: What is the relationship between the site, range, and offset in BGP mode?

A: Site refers to the label block sent to a certain peer. The remote label of the local peer must fall in this label block. For example, the label block received from the remote is 1000/10/0. If the value of the local site is 5, the remote label of the local is 1005 for the remote.

Range is the sum of VPN sites connected by a VPLS.

Offset defines whether the label block base is counted as a label. Continue to use the previous example. If the label block is 1000/10/1, the remote label is calculated on the base of 1000. Therefore, the remote label of the local is 1001.

Q: What is the prerequisite for VPLS configuration?

A: Enable MPLS Layer 2 VPN before you configure VPLS.

Q: The display vsi remote bgp command can display the remote label. The display bgp vpls all command can also display the remote label. The display bgp vpls al command displays more information. What is the difference between these two commands?

A: The **display vsi remote bgp** command displays the labels that you select. The display contains both the local label information and the remote label information.

The **display bgp vpls all** command displays all the labels received by BGP from the remote. The display contains only the remote label information.

Therefore, the latter displays more information. After receiving labels from the remote, BGP chooses the best label and sends it to the VPLS module.

Q: When do I need to configure the mpls ldp remote peer command?

A: Generally, it is not necessary to configure the LDP remote peer. When PEs connect indirectly, you must configure the **mpls ldp remote peer** command.

In the case of interoperating with the device from another vendor, configure the LDP remote peer to accept the difference in the implementation mechanism.

5.5 Diagnostic tools

5.5.1 display commands

Command	Description
display vsi *vsi-name* **verbose**	Displays current VSI configuration. If you do not specify a vsi-name, information on all VSIs appears.
display vsi remote [**ldp** | **bgp**]	Displays the labels received by the remote. You can choose LDP or BGP.
display vpls fib verbose	Displays the detailed information about the VPLS_FIB.
display vpls mid interface vsi *vsi-name*	Displays information about the VPLS_MID. When you use the **display vpls mid token vsi vsi-name** command, the token value of the PW in the MID table appears.
display vpls connection	Displays information about VPLS connections.
display tunnel-info all	Displays information about this tunnel. Tunnel information includes information about the PW.
display bgp vpls all	Displays the remote label block of BGP VPLS.
display mpls l2vc	Displays the status of this VLL.
display vpls statistics	Displays VPLS statistics.
display mpls ldp session	Displays information about LDP sessions.
display mpls lsp	Displays information about MPLS LDP.

5.5.2 debugging command

Command	Description
debugging mpls l2vpn event	Debugs VPLS events.
debugging mpls l2vpn timer	Debugs the VPLS timer.
debugging mpls l2vpn vpls_fib	Debugs information on the VPLS_FIB.
debugging mpls l2vpn vpls_mid	Debugs information on the VPLS_MID
debugging mpls l2vpn advertisement	Debugs Layer 2 VPN BGP or LDP message advertisement.
debugging mpls packet	Debugs the MPLS packet forwarding.

NOTE

VPLS belongs to the Layer 2 VPN. Therefore, the **debugging** commands of the Layer 2 VPN also apply to VPLS.

Nortel Secure Router 8000 Series

Troubleshooting - VPN

Printed in Canada, India, and the United States of America

Release: 5.3
Publication: NN46240-710
Document Revision: 01.01
Document status: Standard
Document release date: 30 March 2009

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

www.nortel.com

LEGAL NOTICE

While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

ATTENTION
For information about the safety precautions, read "Safety messages" in this guide.

For information about the software license, read "Software license" in this guide.