3Com Router 3000 Ethernet Family Configuration Guide

3C13636

www.3Com.com

Part Number: 10014939 Rev. AA

February 2006

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as “Commercial Computer Software” as defined in DFARS 252.227-7014 (June 1995) or as a “commercial item” as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com’s standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com, the 3Com logo, are registered trademarks of 3Com Corporation.

Intel and Pentium are registered trademarks of Intel Corporation. Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. UNIX is a registered trademark in the United States and other countries, licensed exclusively through X/Open Company, Ltd.

All other company and product names may be trademarks of the respective companies with which they are associated.

3Com Corporation
350 Campus Drive
Marlborough, MA
01752-3064

Introduction

Table of Contents

Chapter 1 v2.4x Overview

1.1 Introduction

Versatile Routing Platform (v2.4x) is the versatile operating system platform of 3Com Technologies for data communications products. Focusing on IP services, it constructs a componential architecture, and provides abundant functionality as well as the application-based tailorability and scalability.

Taking the TCP/IP stack as the core, v2.4x integrates the data communications technologies in routing, QoS, VPN, security, and VoIP into the operating system, and offers remarkable data forwarding capability.

v2.4x is a network operating system of which 3Com Technologies owns the exclusive intellectual property rights (IPR). It provides a uniform set of interfaces (network, user and management) for various hardware platforms and therefore offers a variety of flexible application solutions with hundreds of features. Moreover, as a platform of sustainable development, it can protect network investments.

1.2 Architecture of v2.4x

Using the TCP/IP model as a reference, the architecture of v2.4x implements protocols at layers encompassing data link, network, and application, as shown in the following figure:

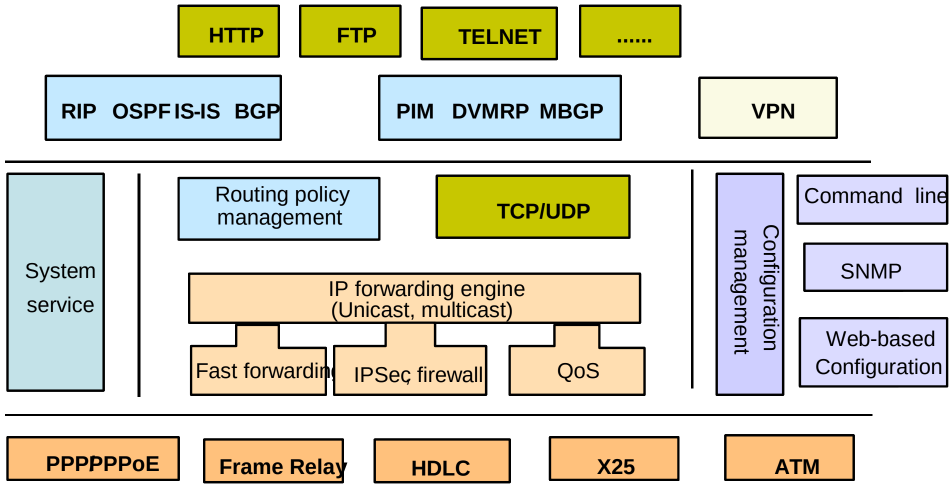


Figure 1-1 v2.4x architecture

1.3 V2.4x Functionality and Use with Products

Note:

V2.4x is the network system platform for 3Com 5000/6000 Routers.

This manual describes the functionality available with V2.4x in detail. The features and commands restricted to the 3Com 6000 routers are declared as “Router 6000 only.”

In the examples throughout this manual, most network interfaces are represented by interface-type slot-number/card-number/interface-number, Serial 0/0/0 for example. This numbering convention applies to the 3Com 6000 Routers. For other routers, network interfaces are represented by interface-type slot-number/interface-number, Serial 0/0 for example.

The following table lists all the essential functionality provided by the router network system platform V2.4x:

Table 1-1 V2.4x functionality

Attribute	Description	
Network interconnectivity	LAN protocols	Ethernet_II Ethernet_SNAP VLAN Transparent bridge
	Link layer protocols	PPP, MP SLIP ISDN PPPoE IPoA PPPoA PPPoEoA HDLC Frame Relay LAPB X.25 ATM
	VPN	L2TP VPN GRE VPN IPSec VPN MPLS VPN (L2/L3) DVPN

Attribute	Description	
Network protocols	IP services	ARP, ARP proxy Static domain name resolution IP unnumbered DHCP Relay DHCP Server DHCP Client IGMP
	Non-IP services	DLSw IPX
	IP routing	Static routing management Dynamic routing protocols: ● RIP-1/RIP-2 ● OSPF ● BGP ● IS-IS Routing policy Policy routing Multicast routing protocols: ● PIM-DM ● PIM-SM ● MBGP ● MSDP
MPLS	Basic MPLS features MPLS VPN MPLS QoS	

Attribute	Description	
Network security	Authentication, authorization, accounting (AAA) services	RADIUS HWTACACS CHAP authentication PAP authentication
	Firewalls	Packet filter ● Interface-based ACL ● Time-based ACL Firewall ● Packet filtering firewall ASPF (stateful firewall)
	Data security	Terminal access security IPSec IKE
	NAT	Allows LAN users to access external networks by using the IP addresses in the address pool Supports associations of ACL and address pool Supports associations of ACL and interface Allows the hosts on external networks to access the internal server Allows configuring valid time ranges for address translation Supports multiple ALGs NAT multi-instance
Network reliability	Backup center VRRP	
QoS	Traffic policing	Traffic policing
	Congestion management	FIFO, PQ, CQ, WFQ, CBQ/LLQ, RTP
	Congestion avoidance	WRED
	Traffic shaping	TS
	Interface rate limit	LR
	FR QoS	
	MPLS QoS	

Attribute	Description	
System management	File management	File system management FTP Server and Client for uploading and downloading the configuration file or application TFTP Client for uploading and downloading files Default configuration file for auto-config
	User management	Users fall into the following categories: ● Terminal users: log onto the router from a console, Aux, or asynchronous port ● Telnet users: telnet to the router ● SSH users: log onto the router through SSH connections ● FTP users: FTP to the router for file transfer ● PPP users: set up PPP connections through dial-up or PPPoA for example, with the router for network access ● PAD users: set up PAD connections with the router for network access Terminal and Telnet users are classified into four levels: visit, monitor, system, and manage User-interface with multiple authentication and authorization methods at login
	Terminal access services	Telnet TTY Remote terminal connection (RTC)
	Network management	Standard SNMPV3, compatible with SNMP V2C, SNMP V1 Support for RMON Support for NTP time synchronization Network test tools such as **tracert**, **ping**, **hwping** commands for diagnosing the health of the network quickly Detailed debugging information useful for network troubleshooting
	Equipment management	Hot swap of interface cards/fans/power supplies (Router 6000 only) Query for statistics on memory and CPU

Attribute	Description	
	CLI	Multiple terminal services for entering the CLI: ● console port for local configuration ● AUX port for remote or local configuration ● Telnet or SSH for local or remote configuration ● Telnet for logging in directly and managing other routers ● PAD terminal service ● Dumb terminal service ● Rlogin terminal service Hierarchical configuration command protection, safeguarding the router against intrusion Prompt and help information in both English and Chinese
	Log management	
Dial-up network	DCC configuration Modem management configuration	
Voice	Basic functions of IP voice	Voice activity detection (VAD), comfort noise, jitter buffer and volume tuning PBX functions, such as do-not-disturb, call forwarding on busy, unconditional call forwarding, alarm-call, and multiline hunt group FXS, FXO and E&M analog interfaces Fast connection and tunneling Voice MPR Calling identification delivery (CID) Voice communication on loopback interfaces Manual/automatic busy-tone detection Routing policies of PSTN backup to IP and PSTN backup to GK Static, dynamic and combined VoIP routing policies Voice QoS Fast and normal voice data receiving/transmitting Networking with the A8010 Refiner
	Protocol and signaling	R2, Q.931, Q.SIG, digital E&M, H.323, SIP
	Voice codec	G.711, G.723, G.726, G.729
	Fax	ITU-T T.30, T.4, and T.38 recommendations Adjustment of multiple fax parameters Fax over IP

Attribute	Description	
	E1/T1 voice	E1 port for R2, DSS1, Q.SIG, and digital E&M signaling T1 port for DSS1 and Q.SIG subscriber signaling simultaneous voice data transmission over PRI interfaces
	Voice RADIUS	Local-first authentication Card number/password flow and calling number flow One-stage and two-stage dialing
	GK Client	Interacts RAS messages with GK Server as GK Client, and dynamically resolves called number to the peer gateway address Standby GK Server
	IPHC	PPP-based RTP and TCP header compressions PPP-based STAC-LZS compression PPP-based link fragmentation and interleave

🕮 **Note:**

Currently, hot swap of interface cards/fans/power supplies is restricted to the 3Com Router 6000.

Chapter 2 User Configuration Interface

2.1 Setting up Configuration Environments

The system supports both local and remote configuration. The following subsections tell you how to set up the configuration environments.

2.1.1 Setup through the Console Port

Step 1: To set up a local configuration environment, connect the serial port on a PC (or terminal) to the console port on the router using a standard RS-232 cable, as shown in Figure 2-1.

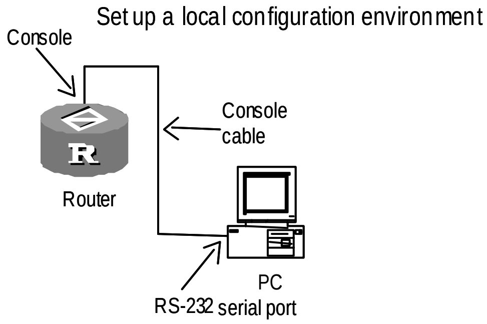


Figure 2-1 Set up a local configuration environment through the console port

Step 2: Run the terminal emulation program (Win9X HyperTerminal for example) on the PC, and set the terminal communication parameters as follows:

Bits per second: 9600

Data bits: 8

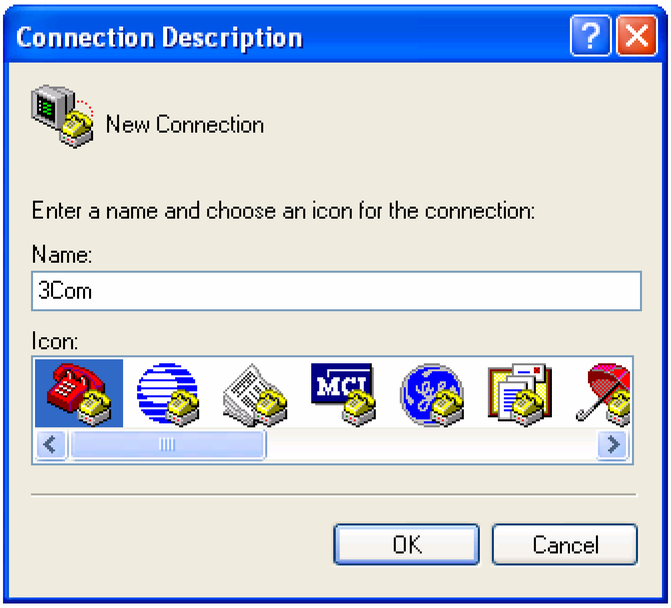
Stop bits: 1

Parity: None

Flow control: None

TermType: VT100

See Figure 2-2 through Figure 2-4.



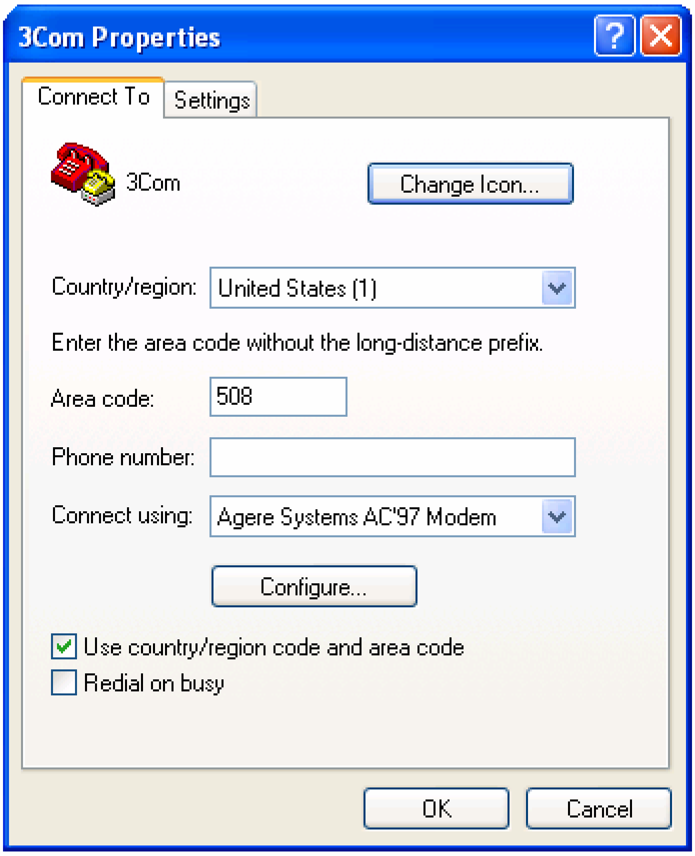
New Connection

Enter a name and choose an icon for the connection:

Name: 3Com

Icon:

Figure 2-2 New connection



3Com

Country/region: United States (1)

Enter the area code without the long-distance prefix.

Area code: 508

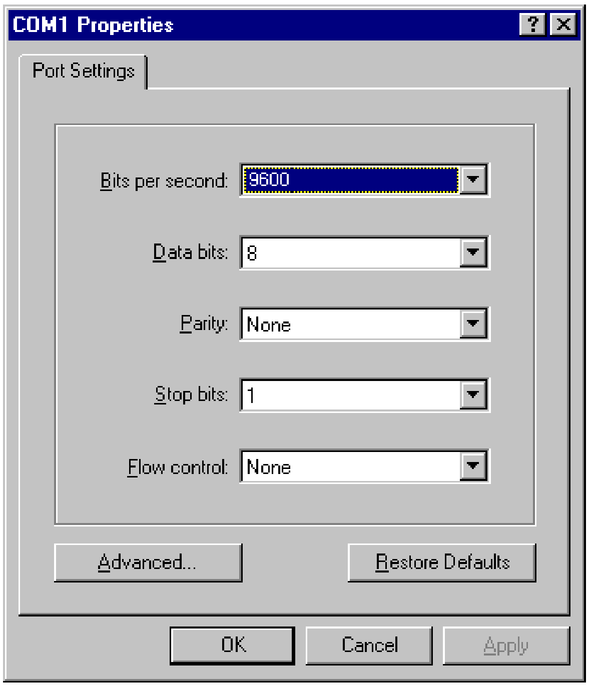
Phone number:

Connect using: Agere Systems AC'97 Modem

☑ Use country/region code and area code

□ Redial on busy

Figure 2-3 Set the connection port



Bits per second: 9600

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

Figure 2-4 Set the port communication parameters

Step 3: The router runs Power-On Self-Test (POST), and upon its completion prompts you to press <Enter> until the command line prompt (such as <3Com>) appears.

Step 4: Enter commands to configure the router or view its running state. Whenever you need help, enter "?" For more information about the commands, see later chapters.

2.1.2 Setup through Telnet

You may telnet to the router through a LAN or WAN, provided that:

1) This is not the first power-on of the router.
2) You have correctly configured the IP addresses of the interfaces on the router.
3) You have appropriately configured authentication at login and access control rules.
4) At least a reachable route exists between the console terminal and the router.

Follow these steps to set up a configuration environment:

Step 1: Connect the Ethernet port on the PC to the Ethernet port on the router through the LAN for a local environment as shown in Figure 2-5 or through the WAN for a remote environment as shown in Figure 2-6.

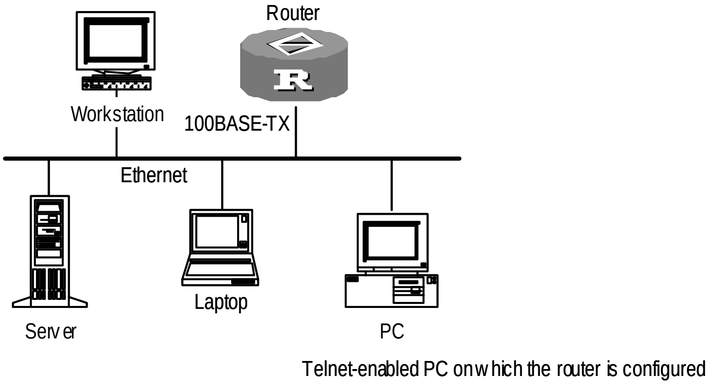


Figure 2-5 Set up a local configuration environment through the LAN

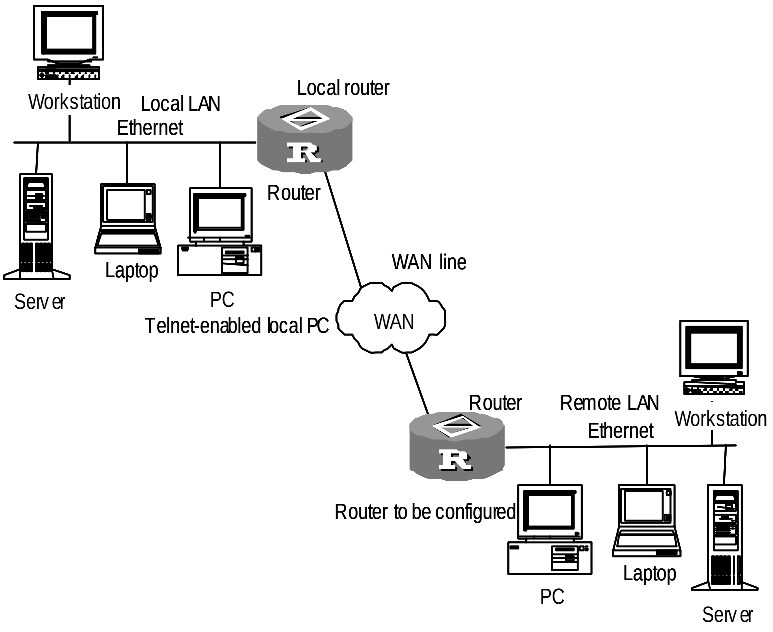
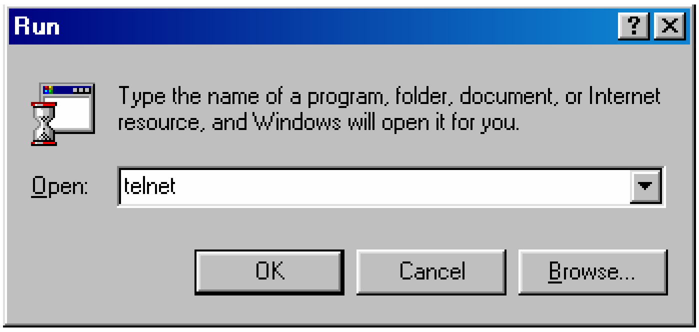


Figure 2-6 Set up a configuration environment through the WAN

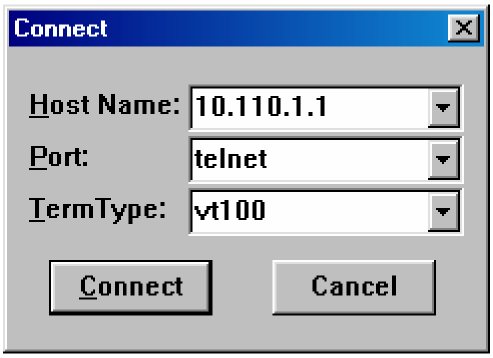
Step 2: Run the Telnet program on the PC and set its terminal type to VT100, as shown in Figure 2-7 and Figure 2-8.



Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: telnet

Figure 2-7 Run the Telnet program


Connect

Host Name: 10.110.1.1

Port: telnet

TermType: vt100

Figure 2-8 Set up a Telnet connection with the Router

Note:

Host Name in Figure 2-8 refers to the host name or IP address of the remote router.

Step 3: Enter the IP address of the router’s Ethernet port on the local PC (or the IP address of the router’s WAN port on the remote PC) to connect with the Router. If the authentication succeeds, the system will display the command line prompt (<3Com> for example). If you see the message "All user interfaces are used, please try later!" try again later.

Step 4: Enter commands to configure the router or view its running state. Whenever you need help, enter "?” For more information about the commands, see later chapters.

Note:

When you telnet to the router to configure it, take caution in modifying its IP address, as such modification may result in disconnection of the Telnet link. If you must make a modification, enter the new IP address of the router and then try for a new connection.

2.1.3 Setup through the AUX Port

To set up a configuration environment by connecting the AUX port on the router through modem dial, you need to attach a modem to the serial port on the PC and a modem to the AUX port on the router, as shown in Figure 2-9.

Step 1: Attach a modem to the AUX port.

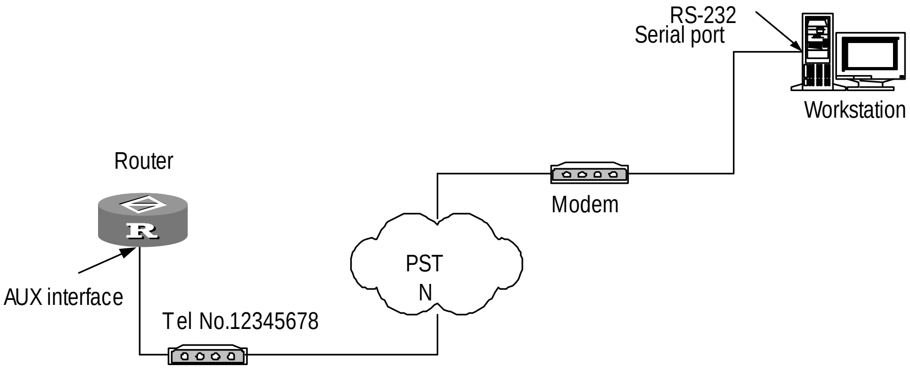


Figure 2-9 Set up a remote configuration environment

Step 2: Dial to connect the router remotely by using a terminal emulation program (such as Windows9X HyperTerminal). In the HyperTerminal, select the RS-232 serial port of the PC for connection, and set the terminal communication parameters similar to those used for setting up connection through the console port:

Bits per second: 9600

Data bits: 8

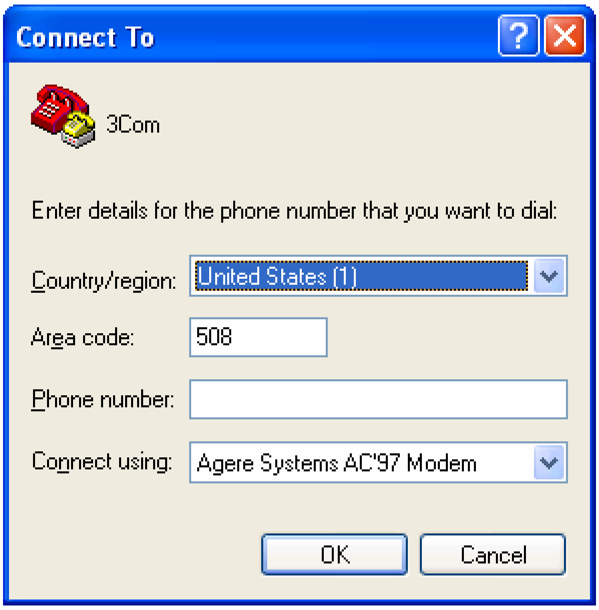
Stop bits: 1

Parity: None

Flow control: None or hardware control

TermType: VT100

See Figure 2-10 and Figure 2-11.



3Com

Enter details for the phone number that you want to dial:

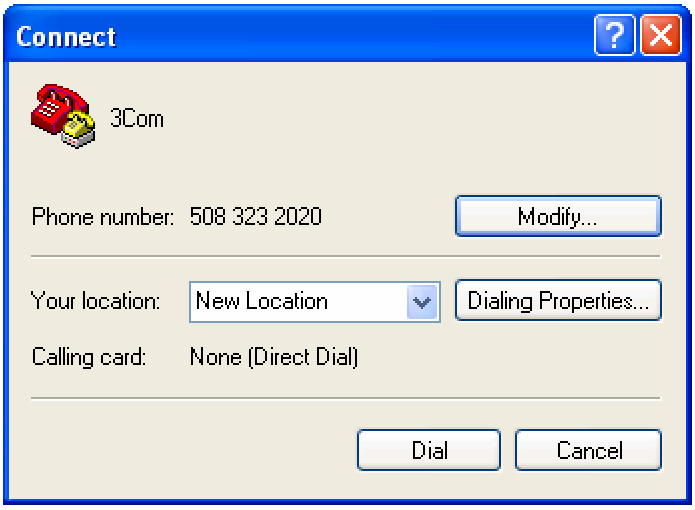
Country/region: United States (1)

Area code: 508

Phone number:

Connect using: Agere Systems AC'97 Modem

Figure 2-10 Set the number to be dialed



Connect

3Com

Phone number: 508 323 2020

Your location: New Location

Calling card: None (Direct Dial)

Figure 2-11 Dial on the remote PC

Step 3: Enter the correct username and password. When you see the command line prompt (<3Com> for example) in the HyperTerminal configure or manage the router.

2.1.4 Setup through SSH

Secure Shell (SSH) provides high information security and powerful authentication to protect your router from attacks, such as, IP address spoofing or plain text password interception. These attacks are likely to happen when users log onto the router from an insecure remote network. The router can be connected to multiple SSH clients for setting up connections with routers or UNIX hosts that run SSH Server. The environment configuration procedures are similar to those of Telnet.

Step 1: To set up a local configuration environment connect the Ethernet port of the PC to that on the router through the LAN, or construct network layer interconnection through a Hub or Ethernet switch. To set up a remote configuration environment connect the PC and the router over the WAN.

Step 2: Configure SSH parameters on the router. For more information, refer to the section “Terminal Services” in the “System Management” part in *V2.4x Configuration Guide*.

Step 3: Run SSH client program on the PC and set the parameters including the IP address of the remote router, SSH version, and RSA key file. Next establish a connection to the router for configuration.

2.2 CLI

The system provides rich configuration commands and the CLI through which users can configure and manage their routers. The CLI supports:

- Local and remote configuration through the AUX port.
- Local configuration through the console port.
- Local and remote configuration through Telnet and SSH.
- Modem dialup to remotely log onto and configure the router from its asynchronous serial port.
- Flexible terminal access approaches, such as dumb terminal and redirect Telnet.
- User interface view for managing the particular configurations of different terminal users.
- Hierarchical command protection where users can only execute the commands at their own level or lower levels.
- Local, password, and AAA authentication modes to safeguard the router against intrusion.
- Easy access to on-line help by entering "?"
- Quick network test tools such as **tracert** and **ping**.
- Abundant debugging information for fault diagnosis.
- Telneting to other routers for management.
- FTP and TFTP services for easy file uploading and downloading.
- Saving and executing commands that have been executed.
- Multiple intelligent command parsing methods (provided by command line descriptor) such as fuzzy match and context association for convenience of input.

2.2.1 Command Line Views

For hierarchical protection, system commands are divided into four levels:

- Visit: involves commands for network diagnosis (such as **ping** and **tracert**), commands for accessing an external device (such as Telnet client, SSH client, RLOGIN). Saving the configuration file is not allowed at this level.
- Monitor: includes the **display** and **debugging** commands for system maintenance, and service fault diagnosis. Saving the configuration file is not allowed at this level.
- System: provides service configuration commands, including routing and commands at each level of the network for providing services.
- Manage: influences the basic operation of the system and the system support modules for service support. Commands at this level involve file system, FTP, TFTP, configuration file switch, power control, standby board control, user management, level setting, as well as parameter setting within a system (the last case involves those non-protocol or non RFC provisioned commands).

Login users are also classified into four levels that correspond to the four command levels. After users at different levels log in, they can only use commands at their own level or lower levels.

To fence off intrusion of illegitimate users, legitimate users are required to provide the correct super password, if one has been configured using the **super password** command, when they switch from a lower level to a higher level. For privacy, the entered password is not displayed on the screen. Users have three chances to provide the correct password. Only after the correct password is entered can they switch to the higher level. Otherwise, the original user level remains unchanged.

The command views are implemented according to configuration requirements which are related to one other. For example, after logging onto the router you enter user view where you can only view state and statistic information. In user view, key in **system-view** to enter system view where you can key in different configuration commands to enter their views.

Command lines are associated with the views described in the following table.

Table 2-1 Command views

Category	Views
User view	—
System view	—
Routing protocol view	**ospf** (OSPF view), **rip** (RIP view), **bgp** (BGP view), **isis** (IS-IS view), and so on.
Interface view	**ethernet** (FE), **gigabitethernet** (GE), **serial** (serial interface), **ce1** (cE1 interface), **ce3** (E3 interface), **ct1** (cT1 interface), **atm** (ATM interface), **pos** (POS interface), **virtual-template** (virtual template), **virtual-ethernet** (virtual Ethernet interface), **loopback** (loopback interface), **null** (null interface), **tunnel** (tunnel interface).
User interface view	—
L2TP group view	—
Routing map view	—

Table 2-2 shows the functionality of each command view and the commands for entering them.

Table 2-2 Command view functionality

Command view	Function	Prompt	command to enter	Command to exit
User view	Display basic information about operation and statistics	<3Com>	Enter right after connecting to the router	**quit** disconnects from the router
System view	Configure system parameters	[3Com]	Key in **system-view** in user view	**quit** returns to user view
User interface view	Manage the asynchronous and logical interfaces on the router	[3Com-ui0]	Key in **user-interface 0** in system view	**quit** returns to system view
OSPF view	Configure OSPF parameters	[3Com-ospf]	Key in **ospf** in system view	**quit** returns to system view
RIP view	Configure RIP parameters	[3Com-rip]	Key in **rip** in system view	**quit** returns to system view
BGP view	Configure BGP parameters	[3Com-bgp]	Key in **bgp 1** in system view	**quit** returns to system view
IS-IS view	Configure IS-IS parameters	[3Com-isis]	Key in **isis** in system view	**quit** returns to system view
Synchronous/ asynchronous serial interface view	Configure synchronous/ asynchronous serial interface parameters	[3Com-Serial1/0/0] [3Com-Serial1/0/2:1]	Key in **Interface serial 1/0/0** (or **1/0/2:1**) in system view	**quit** returns to system view
Asynchronous serial interface view	Configure asynchronous serial interface parameters	[3Com-async 1/0/0]	Key in **Interface async 1/0/0** in system view	**quit** returns to system view
Ethernet interface view	Configure Ethernet interface parameters	[3Com-Ethernet1/0/0]	Key in **Interface ethernet 1/0/0** in system view	**quit** returns to system view

Command view	Function	Prompt	command to enter	Command to exit
Subinterface view	Configure subinterface parameters	[3Com-serial1/0/0.1]	Key in **interface serial 1/0/0.1** in system view	**quit** returns to system view
ATM interface view	Configure ATM interface parameters	[3Com-Atm2/0/0]	Key in **interface atm 2/0/0** in system view	**quit** returns to the user view
ADSL interface view	Configure ADSL interface parameters	[3Com-adsl2/0/0]	Key in **interface adsl2/0/0** in system view	**quit** returns to system view
AUX interface view	Configure AUX interface parameters	[3Com-aux0]	Key in **interface aux 0** in system view	**quit** returns to system view
E1/CE1 interface view	Configure the timeslot binding mode on E1/CE1 interface and physical layer parameters	[3Com-E1 1/0/0]	Key in **controller e1 1/0/0** in system view	**quit** returns to system view
CT1 interface view	Configure the timeslot binding mode on CT1 interface and physical layer parameters	[3Com-T1 1/0/0]	Key in **controller t1 1/0/0** in system view	**quit** returns to system view
Virtual Ethernet interface view	Configure virtual Ethernet interface parameters	[3Com-virtual-Ethernet1/0/0]	Enter **Interface virtual-ethernet 1/0/0** in system view	**quit** returns to system view
Virtual template view	Configure the virtual-template parameters	[3Com-virtual-template0]	Key in **interface virtual-template 0** in system view	**quit** returns to system view
Loopback interface view	Configure loopback interface parameters	[3Com-Loopback2]	Key in **interface loopback 2** in system view	**quit** returns to system view

Command view	Function	Prompt	command to enter	Command to exit
NULL interface view	Configure null interface parameters	[3Com-NULL0]	Key in **interface null 0** in system view	**quit** returns to system view
L2TP group view	Configure the L2TP group	[3Com-l2tp1]	Key in **l2tp-group 1** in system view	**quit** returns to system view
Route-policy view	Configure the BGP route-policy	[3Com-route-policy]	Key in **route-policy test node permit node 10** in system view	**quit** returns to system view
PVC view	Configure PVC parameters	[3Com-pvc-Atm1/0/0-1/32]	Key in **pvc 1/32** in ATM interface view	**quit** returns to ATM interface view

Note:

The command line prompts take router name as prefix (which defaults to 3Com), view name as suffix, a pair of parentheses to denote the current view, a pair of point brackets (<>) to denote user view, and a pair of square brackets (“[]”) to denote system view or any other configuration views.

2.2.2 Online Help with Command Lines

The following are the types of online help available with the CLI:

- Full help
- Fuzzy help

To obtain the desired help information, you can:

1) Enter “?” in any view to access all the commands in this view and brief description about them as well.

```
<3Com> ?
```

2) Enter a command and a “?” separated by a space. If "?" is at the position of a keyword, all the keywords are given with a brief description.

```
<3Com> display ?
```

3) Enter a command and a “?” separated by a space. If "?" is at the position of a parameter, the description about these parameters is given.

```
[3Com] interface ethernet ?
  <3-3>  Slot number
```

```
[3Com] interface ethernet 3?
   /
[3Com] interface ethernet 3/?
  <0-0>
[3Com] interface ethernet 3/0?
   /
[3Com] interface ethernet 3/0/?
  <0-0>
[3Com] interface ethernet 3/0/0 ?
  <cr>
```

<cr> indicates that there is no parameter at this position. The command is then repeated in the next command line and executed if <Enter> is input.

4) Enter a character string followed by a "?". All the commands starting with this string are displayed.

```
<3Com> d?
debugging   delete   dir   display
```

5) Enter a command followed by a character string and "?". All the keywords starting with this string are listed.

```
<3Com> display h?
history-command hotkey
```

6) Press <tab> after entering the first several letters of a keyword to display the complete keyword, provided that these letters can uniquely identify the keyword in this command.

2.2.3 Command Line Error Information

The commands are executed only if they have no syntax error. Otherwise, error information is reported. Table 2-3 lists some common errors.

Table 2-3 Common command line errors

Error information	Cause
Unrecognized command	The command was not found.
	The keyword was not found.
	Parameter type error
	The parameter value is beyond the allowed range.
Incomplete command	Incomplete command
Too many parameters	Too many parameters
Ambiguous command	Ambiguous parameters

2.2.4 History Command

The CLI can automatically save the commands that have been entered. You can invoke and repeatedly execute them as needed. By default, the CLI can save up to ten commands for each user. Table 2-4 lists the operation that you can perform.

Table 2-4 Access history commands

Operation	Key	Result
View the history commands.	**display history-command**	Displays the commands that you have entered
Access the last history command.	Up-arrow key or <Ctrl+P>	Displays the earlier history command, if there is any. Otherwise, the system rings alarm.
Access the next history command	Down-arrow key or <Ctrl+N>	Displays the next history command, if there is any. Otherwise, the system clears the commands and rings alarm.

Note:

You may use arrow keys to access history commands in Windows 3.X Terminal or Telnet. However, the up-arrow key is invalid in Windows 9X HyperTerminal, because it is defined in a different way. You can use <Ctrl+P> instead.

2.2.5 Edit Features

The CLI provides the basic command edit functions and supports multi-line editing. The maximum length of each command is 256 characters. Table 2-5 lists these functions.

Table 2-5 Edit functions

Key	Function
Common Keys	If the editing buffer is not full, insert the character at the position of the cursor and move the cursor to the right. Otherwise, the alarm rings.
Backspace key	Delete the character to the left of the cursor and move the cursor back one character. If the cursor gets to the beginning of the command line, the alarm rings.
Left-arrow key or <Ctrl+B>	The cursor moves one character space to the left, and the alarm rings when the cursor gets to the beginning of the command line.
Right-arrow key or <Ctrl+F>	The cursor moves one character space to the right, and the alarm rings when the cursor gets to end of the command line.

Key	Function
Tab key	Pressing <Tab> after entering part of a keyword enables the fuzzy help function. If finding a unique match, the system will substitute the complete keyword for the incomplete one and display it in the next line. If there are several matches or no match at all, the system will not modify the incomplete keyword and display it again in the next line.

2.2.6 Display Features

I. Language selection

Your router offers both English and Chinese help information. You can toggle between them.

Perform the following configuration in user view.

Table 2-6 Toggle between languages

Operation	Command
Toggle to English.	**language-mode english**
Toggle to Chinese.	**language-mode chinese**

II. Display pause

When the information displayed exceeds one screen, you can pause using one of the methods shown in Table 2-7 .

Table 2-7 Display functions

Action	Function
Enter <Ctrl+C> when information display pauses	Stops the display and the command execution.
Enter <Space> when information display pauses	Continues to display information of the next screen page
Enter <Enter> when information display pauses	Continues to display information of the next line.

III. Information output

Many **display** commands are available for showing system status information. When outputting information, you can add "|" in the command to filter information. Three options are available:

- **begin** *text*: to display information starting from the line with "text"

- **exclude** *text*: to display information of the lines with no "text"
- **include** *text*: to display information of the lines with "text"

For example, if you enter the **display current-configuration | include ip** command, the configuration information for the line with "ip" are displayed.

2.2.7 Regular Expressions

I. Introduction to regular expressions

Regular expressions are a powerful and flexible tool for pattern matching and substitution. They are not restricted to a language or system and have been widely accepted.

When using a regular expression you need to construct a matching pattern according to certain rules, and then compare the matching pattern with the target object. The simplest regular expressions exclude all metacharacters. For example, you can specify a regular expression “hello” to match only the character string “hello”.

For flexible matching mode construction regular expressions are allowed to contain some special characters, called metacharacters, to define how other characters appear in the target object. The following table describes the metacharacters.

Table 2-8 Metacharacters

Metacharacter	Meaning
\	Escape Character
.	Matches any single character except for “\n”, including spaces.
*	The character to the left of the asterisk in the expression should match zero or more times.
+	There should be at least one match of the character to the left of the plus sign in the expression.
|	Allows either expression on the side of the pipe character (vertical bar) to match the target object.
^	The characters following the ^ sign must appear at the beginning of the target object.
$	The characters before the dollar sign must appear at the end of the target object.
[xyz]	Any of the characters in the square brackets may match the target character.
[^xyz]	Any characters other than those in the square brackets may match the target character.
[a-z]	Any of the characters within the specified range may match the target character.
[^a-z]	Any of the characters beyond the specified range may match the target character.

Metacharacter	Meaning
{n}	The “n” in the brace brackets is a non-negative integer, indicating that there are consecutive n matches.
{n,}	The “n” in the brace brackets is a non-negative integer, indicating that there are inconsecutive n matches.
{n,m}	The “m” and “n” in the brace brackets are non-negative integers, with n<=m. It indicates that the consecutive matches are in the range n to m. Note that no space is allowed on either side of the comma.

For example:

^ip: to match the target object starting with the character string “ip”

ip$: to match the target object ending with the character string “ip”

II. Benefits of regular expressions

You can use regular expressions to filter out uninterested information when a large amount of information is present.

1) Specify filtering mode in the command

In filtering output, you can choose from three kinds of filtering modes. In a command that supports regular expressions, they are presented as { **begin | exclude | include** } *regular-expression*:

- **begin**: to output all lines starting with the line that matches the specified regular expression.
- **exclude**: to output all lines except for those matching the specified regular expression.
- **include**: to output only the lines that match the specified regular expression.

2) Specify filtering mode between screens

If enormous information is present and output in multiple screens, you can filter information after the prompt, ”---- More ----” between screens which appears by entering a regular expression in one of the following forms:

- */regular-expression*: to output all lines starting with the line that matches the specified regular expression.
- *-regular-expression*: to output all lines except for those matching the specified regular expression.
- *+regular-expression*: to output only the lines that match the specified regular expression.

For example, you can use the following command to view the current configuration information:

```
<3Com> display current-configuration
#
 sysname 3Com
#
controller E3 0/1/0
 e1 1 channel-set 1 timeslot-list 1-31
#
controller T3 1/1/0
#
interface Ethernet0/2/0
 description Don't change the configuration please
 ip address 10.110.98.137 255.255.255.0
#
interface Ethernet1/0/0
#
interface Ethernet1/2/0
#
interface Serial0/1/0/1:1
 link-protocol ppp
 ip address 100.110.1.1 255.255.255.0
#
interface Pos0/0/0
#
interface NULL0
```

When the prompt “---- More ----” appears, you can enter a regular expression to filter information to be displayed. To output only the lines that contain the character string “interface”, for example:

```
  ---- More ----
+interface                             Manually entered by the user

filtering...
interface LoopBack0
user-interface con 0
user-interface vty 0 14
<3Com>
```

2.3 Hot Keys

2.3.1 Classifying Hot Keys

The hot keys in the system fall into two types user-configurable and system.

The user-configurable shortcut keys include CTRL_G, CTRL_L, CTRL_O, CTRL_T and CTRL_U. You can associate these shortcut keys with any commands for automatic execution.

The system shortcut keys have fixed functions and do not allow free customization, as shown in the following table:

Table 2-9 System hot keys

Keys or commands	Function
CTRL_A	Moves the cursor to the beginning of current line.
CTRL_B	Moves the cursor one character space leftward.
CTRL_C	Terminates the running function.
CTRL_D	Deletes the character at the cursor.
CTRL_E	Moves the cursor to the end of current line.
CTRL_F	Moves the cursor one character rightward.
CTRL_H	Deletes the character to the left of the cursor.
CTRL_K	Terminates the outbound connections.
CTRL_N	Displays the next command in the history command buffer.
CTRL_P	Displays the previous command in the history command buffer.
CTRL_R	Refreshes the information of current line
CTRL_W	Deletes the word to the left of the cursor
CTRL_X	Deletes all the characters to the left of the cursor
CTRL_Y	Delete all the characters to the right of the cursor
CTRL_Z	Returns to user view
CTRL_]	Terminates the inbound or re-directional connections
ESC_B	Moves the cursor one word leftward
ESC_D	Deletes the word to the right of the cursor
ESC_F	Moves the cursor one word rightward
ESC_<	Sets the cursor's location to the beginning of the clipboard
ESC_>	Sets the cursor's location to the end of the clipboard

2.3.2 Usage of the Hot Keys

- You can press a combined hot key wherever you are allowed to enter a command. The system will then display the corresponding command as if you had entered the complete command.
- If you have input part of a command without pressing <Enter>, you can delete the input characters and enter a complete command simply by pressing the hot key for this new command.
- Similar to executing a command, after a hot key is executed its corresponding command prototype is retained in the history command buffer and log for retrieve and problem addressing.

Note:

The function of a hot key may be restricted by its definition on the user terminal. If the same hot key is associated with different functions on the IP PBX and the user terminal, it is to be captured by the terminal program when executed and as such, cannot execute the associated command line on the router.

Perform the following configuration in system view.

Table 2-10 Define hot keys

Operation	Command
Define a hot key.	**hotkey** [**CTRL_G** | **CTRL_L** | **CTRL_O** | **CTRL_T** | **CTRL_U**] *command_text*
Restore the default values in the system.	**undo hotkey** [**CTRL_G** | **CTRL_L** | **CTRL_O** | **CTRL_T** | **CTRL_U**]

By default, the system assigns defaults to the hot keys of CTRL_G, CTRL_L and CTRL_O as follows:

CTRL_G: **display current-configuration**

CTRL_L: **display ip routing-table**

CTRL_O: **undo debugging all**

The default values of the other two hot keys are void by default.

Perform the following configuration in any view.

Table 2-11 Display the hot keys and their functions

Operation	Command
Display the hot keys and their functions.	**display hotkey**

2.3.3 Examples of Hot Keys in Use

# Assign the hot key CTRL_U to the **display ip routing-table** command and execute it.

```
[3Com] hotkey ctrl_u display ip routing-table
[3Com] Press <Ctrl_u>
[3Com] display ip routing-table
Routing Table: public net
Destination/Mask   Proto   Pre Cost        Nexthop         Interface
      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
```

2.3.4 Configuring Command Alias

The command alias function allows you to replace some common commands available with v2.4x with the command forms you prefer. The following are the command alias use conventions:

1) The system retains and displays alias-included commands that you entered in its prototype when you execute commands to save configurations or to view command history or current configurations.
2) You can input a command by inputting its conflict-free portion. When the command alias function is enabled, the likelihood exists that this incomplete portion is a fuzzy match of both a command alias and a command, however. In this case, the system considers the portion as the alias and outputs its associated command. To have the system output the intended command, you need to input the command completely. In the event that the character string you input is a fuzzy match of multiple aliases, the system prompts that the alias is ambiguous and asks you to input the complete keyword.
3) If you press <Tab> after inputting a unique alias, the system displays its associated keyword.
4) Full replacement of command lines is not supported. You can only map an alias with the first keyword in a command. The system can only replace this alias with the first keyword in the command and the second keyword in its **undo** form.

I. Enabling command alias

Perform the following configurations in system view.

Table 2-12 Enable command alias

Operation	Command
Enable command alias	**command-alias enable**
Disable command alias	**undo command-alias enable**

By default, the command alias function is disabled.

II. Mapping an alias with a command

Perform the following configuration in system view.

Table 2-13 Map an alias with a command keyword

Operation	Command
Map an alias with a command keyword.	**command-alias mapping** *cmdkey alias*
Cancel the map.	**undo command-alias mapping** *alias*

By default, no command alias is configured.

III. Displaying and Debugging

Perform the following configuration in any view.

Table 2-14 Display and debug

Operation	Command
Display the current alias settings.	**display command-alias**

Chapter 3 v2.4x Basic Configurations

3.1.1 Entering/Exiting System View

When logging onto the router from the console port, you enter user view and see the prompt <3Com> on the screen. To enter or exit system view, use the following commands.

Table 3-1 Enter/exit system view

Operation	Command
Enter system view from user view.	**system-view**
Return to user view from system view.	**Quit**
Return to user view from any other view.	**Return**

With the **quit** command, you can return to the previous view or exit the system from user view. The hot key <Ctrl+Z> is equivalent to the **return** command.

3.1.2 Configuring the Router Name

The command prompt contains a router name that can be configured as needed.

Perform the following command in system view.

Table 3-2 Configure the router name

Operation	Command
Configure the router name	**sysname** *sysname*

3.1.3 Configuring the System Clock

Perform the following configuration in system view.

Table 3-3 Configure system clock

Operation	Command
Set the standard time.	**clock datetime** *time date*
Set the time zone.	**clock timezone** *time-zone-name* { **add** | **minus** } *time*
Cancel the time zone setting.	**undo clock timezone**

Operation	Command
Import a daylight saving time scheme.	**clock summer-time** *summer-time-zone-name* { **one-off | repeating** } *start-time start-date end-time end-date add-time*
Cancel the daylight saving time scheme.	**undo clock summer-time**

3.1.4 Configuring a Banner

A banner shows information displayed at login, login authentication, or configuration.

Perform the following configuration in system view.

Table 3-4 Configure a banner

Operation	Command
Configure the banner to be displayed at login.	**header incoming** *text*
Configure the banner to be displayed at login authentication.	**header login** *text*
Configure the banner to be displayed when a user enters user view.	**header shell** *text*
Cancel the banner setting.	**undo header** { **incoming** | **login** | **shell** }

3.1.5 User Level Switching

I. Configuring password for user level switching

You may set user level switching passwords. After that, a user that logs onto the router with a lower user level is required to provide the password before operating on higher level commands.

Perform the following configuration in system view.

Table 3-5 Configure a user level switching password

Operation	Command
Configure a user level switching password.	**super password** [**level** *user-level*] { **simple** | **cipher** } *password*
Delete the configured password	**undo super password** [**level** *user-level*]

II. Switching user levels

You must provide the correct password before you can become a higher level user.

Perform the following configuration in user view.

Table 3-6 Switch the user level

Operation	Command
Switch the user level.	**super** [*level*]

For more information on user level configuration, refer to the section discussing user management in the part “System Management” of this manual.

3.1.6 Locking User Interfaces

When you want to leave for a while you may lock the user interface to prevent it from being accessed by illegitimate users. When locking the interface you need to configure and confirm a password which is required in unlocking the interface.

Perform the following configuration in user view.

Table 3-7 Lock the user interface

Operation	Command
Lock the user interface.	**lock**

3.1.7 Configuring Command Levels

All the commands are administratively assigned to different views and categorized into four levels: visit, monitor, system, and manage, identified respectively by 0 through 3.

Perform the following configuration in system view.

Table 3-8 Configure command privilege level

Operation	Command
Assign a level to the commands in the specified view.	**command-privilege level** *level* **view** *view command-key*
Restore the default.	**undo command-privilege view** *view command-key*

The following table describes the default level of the commands.

Table 3-9 Default command levels

Level	Privilege	Command
0	Visit	**ping**, **tracert**, **telnet**
1	Monitor	**display**, **debugging**
2	System	All configuration commands except for those at manage level
3	Manage	FTP, TFTP, Xmodem, and file system operation commands

🕮 **Note:**

All commands have default views and privilege levels. Generally no configuration is required.

3.1.8 Displaying System Information

In terms of function, you may collect these types of system status information with the **display** command:

- Configuration information
- Operating information
- Statistics

The following table just lists the system-related **display** commands. Refer to other chapters for those associated with protocols and interfaces.

Perform the following configuration in any view.

Table 3-10 Display system status information

Operation	Command
Display information on system version.	**display version** [*slot-id*]
Display software version details.	**vrbd**
Display information on the system clock.	**display clock**
Display information on terminal users.	**display users** [**all**]
Display the initial configurations.	**display saved-configuration**
Display the current configurations.	**display current-configuration**
Display debugging status.	**display debugging** [**interface** *interface-type interface-number*] [*module-name*]
Display diagnostic information.	**display diagnostic-information**

Operation	Command
Display clipboard information.	**display clipboard**
Display the current status of the memory in the system.	**display memory**
Display statistics about CPU usage.	**display cpu-usage** [**configuration** | *number* [*offset*] [**verbose**] [**from-device**]]
Set the CPU usage statistic interval.	**cpu-usage cycle** { **5sec | 1min | 5min | 72min** } [**slave | slot** *slot-num*]
Display the history of the CPU usage statistics in graphics.	**display cpu-usage history** [**task** *task-id*] [**slave | slot** *slot-num*]

When troubleshooting or servicing the system, you can use the **display diagnostic-information** command to collect operating information about active modules in the system.

The **display diagnostic-information** command can at a stroke collect the information displayed at the terminal after executing the commands such as **display clock**, **display version**, **vrbd**, **display device**, **display current-configuration**, **display saved-configuration**, **display interface**, **display controller**, **display ip interface**, **display ip statistics**, **display exception**, **display logbuffer**, and **display history all**.

System Management

Table of Contents

Chapter 1 System Management Overview

After reading the first part “Getting Started” in this manual, you may read this part to learn how to further manage and service your router.

This part is organized as follows:

- System Maintenance Management
- HWPing Configurations
- File Management
- User Interface Configuration
- User Management
- NTP Configuration
- SNMP Configuration
- **Error! Reference source not found.**
- RMON Configuration
- Terminal Services

I. System maintenance management

This chapter introduces the powerful tools and the information center feature available with V 2.41 for network test and troubleshooting.

II. File management

This chapter provides information about the file system functions available with V 2.41. You can manage the files on the hard disk and Flash memory, such as host software, configuration files and log files.

It also covers the supported file transfer protocols: FTP and TFTP.

III. User interface management

This chapter introduces four types of user interfaces supported by V 2.41: console interface, AUX interface, asynchronous serial interface (TTY), and virtual terminal line (VTY). V 2.41 provides you user interface view to manage them, controlling access to the router from these interfaces.

IV. User management

This chapter presents the user management policies available with V 2.41 for convenient and effective user and service management to gain increased network security.

V. NTP configuration

This chapter presents NTP and its configurations. The NTP service available with V 2.41 allows the system to guarantee timekeeping synchronization of the devices on the network along with other NTP-supported devices, ensuring reliability of interoperation.

VI. SNMP configuration

This chapter presents SNMP and its configurations. Together with the network management system, SNMP can efficiently administer the running devices on the network.

VII. BIMS

BIMS comprises the BIMS center side and the device side. The following is how it works to centralize device management:

1) The device sends the BIMS center a request at startup or/and sends requests at regular or irregular intervals. This depends on how you set your policy.
2) The BIMS center interacts with the device according to the policy issued by the administrator. During interaction, the administrator can manage the device, for example, upgrade software, modify configuration, or view configuration/state information.

VIII. RMON

Remote monitoring (RMON) is a kind of management information base (MIB) defined by Internet Engineering Task Force (IETF); it is the most important enhancement to MIB-II. RMON MIBs comprise sets of statistics data, analyzing data, and diagnostic data. Unlike a standard MIB which only provides the raw data about the managed objects for a port, RMON MIBs provide the statistics and resultant data about the entire network segment. RMON thus allows you to monitor traffic over a network segment and even the entire network.

IX. Terminal services

This chapter covers the terminal services available with V 2.41, such as terminal services of console port, AUX port, Telnet, SSH, PAD and dumb terminal. You can manage devices both locally and remotely, without having to connect a physical terminal for each device.

X. POS terminal access

POS terminals are widely deployed at points of sale such as shopping malls and gas stations for card acceptance. They are predominant in areas such as commerce, finance, and taxation.

Depending on network environment, three POS terminal access approaches are available: dial-up, asynchronous leased line, and POSPAD packet network. They will be discussed later in this part.

Chapter 2 System Maintenance Management

System maintenance management includes the following functions:

- Use of the system maintenance and debugging tools
- Maintenance and management of the information center

2.1 auto-config

2.1.1 Introduction

With the auto-config feature, you can have your router, straight out of box, automatically detect and configure all its interfaces upon its first use and start Telnet, FTP, or Web service. Then the connected router or console terminal that has been pre-configured at the network center automatically connects to the router to configure it or to transfer the configuration file. Alternatively, this connection can be initiated administratively.

Auto-config is well suited to the low-end and mid-range routers on the edge of enterprise networks. To build up a network for configuring your router automatically and remotely, connect the router to the router at the network center depending on the specific interface that you use:

- For an E1, T1, E3, and T3 interface, use the fiber-optic line of PDH/SDH network.
- For a serial (in synchronous mode), asynchronous, E1-F, or E1-F interface, use the synchronous/asynchronous leased line of digital data network (DDN).
- For a 10/100 Mbps Ethernet interface, use the 10/100 Mbps Ethernet.
- For an analog modem (AM) interface, use the analog telephone line of PSTN network.

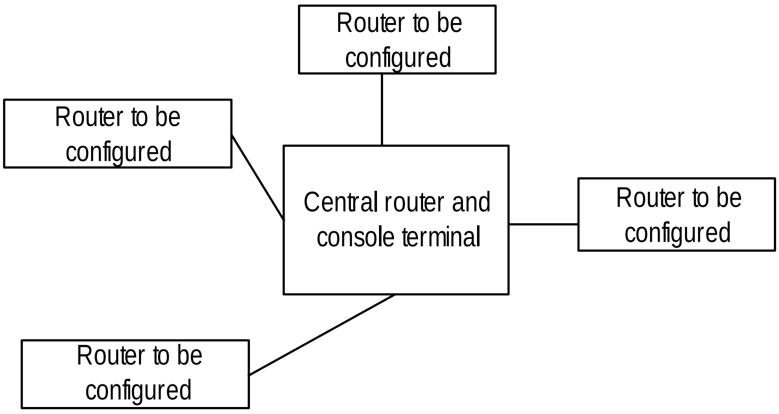


Figure 2-1 Network design for auto-config configuration

The router decides whether to enable the auto-config feature by checking the configuration files. The specific procedure includes:

1) If the router detects the configuration file, it runs the file instead of enabling the auto-config feature.
2) If no configuration file is available, the router runs v 2.41cfg.def, the default configuration file, which it has detected, instead of enabling the auto-config function.
3) When the router fails to detect the above configuration files, it runs the **auto-config** command automatically (by default, auto-config is enabled) and perform the following batch operation:

- For the Serial interface, enable PPP on them to make all the Serial interfaces work in the PPP Negotiate mode. Specify the default user name and password and enable telnet, ftp and web services.
- For the Controller (E1/E3/T3) interface, generate corresponding Serial interfaces and perform the same configuration as Serial interface by the **using** { **e1** | **t3** | **e3** } command. For the Controller (T1) interface, bind all the timeslots to one serial interface and perform the same configuration as the Serial interface by the **channel-set** command.
- For the Ethernet interface, enable the DHCP client and wait the peer to assign address, specify the default user name and password, and enable telnet and ftp service.
- For the AM interface, configure flow mode and modem encoding format and make it support terminal service.

Note:

For the details about enabling the configuration file, refer the section “Configuration File Management”.

2.1.2 Manually Configuring auto-config on the Router

I. Enabling auto-config

Perform the following configuration in system view.

Table 2-1 Enable/disable **auto-config**

Operation	Command
Enable the auto-config feature	**auto-config enable**
Disable the auto-config feature	**undo auto-config**

By default, the auto-config feature is enabled.

II. Implementing the auto-config operation

⚠ **Caution:**

The **auto-config** operation runs a series of commands in batch and changes the current configuration, but the **undo** command is not available. So it is usually used in booting a router for the first time and caution should be taken in using it on already configured networks.

Although the auto-config function is available in the default configuration file "v 2.41cfg.def", you cannot save the configuration result of the **auto-config** command.

Perform the following configuration in system view.

Table 2-2 Implement the **auto-config** operation

Operation	Command
Implement the **auto-config** operation	**auto-config**

The **auto-config** operation runs these commands in batch:

1) Enabling FTP and configuring the VTY (Telnet) and TTY (through AM interface) users to adopt the local authentication

```
ftp server enable
user-interface vty 0 4
authentication-mode scheme
user-interface tty user-interface-number
```

```
modem call-in
speed 57600
authentication-mode scheme
```

2) Configuring the locally authenticated default user name and password, enabling Telnet and FTP services for the default user

```
local-user admin password cipher admin
level 3
service-type ftp telnet
service-type terminal
```

By default, the user name and password are both "admin".

3) Detecting all the Controller interfaces, setting the working status of the E1/T1/E3/T3 interfaces to non-channelized, and generating the corresponding Serial interfaces. For the T1 interface, use the **channel-set** command to bind all the timeslots to one Serial interface.

```
controller e1 interface-number
using e1
controller e3 interface-number
using e3
controller t3 interface-number
using t3
controller t1 interface-number
channel-set 0 timeslot-list 1-24
```

4) Detecting all the Serial interfaces including the logical interfaces generated by Controller interfaces, choosing PPP link layer encapsulating protocol and configuring to get IP address through PPP negotiation, setting the interfaces into UP status

```
Interface serial interface-number
link-protocol ppp
ip address ppp-negotiate
undo shutdown
```

5) Detecting all the Ethernet interfaces, enabling the dhcp client function, setting the interfaces into UP status

```
Interface ethernet interface-number
ip address dhcp-alloc
undo shutdown
```

6) Detecting all the AM interfaces, configuring the working mode to flow mode and the encoding format to Modem (set the CountryCode to UK if there is an E1/E3 module and otherwise to US), and setting the interface into UP status.

```
Interface analogmodem interface-number
async mode flow
country-code { united-kingdom | united-states }
country-code { united-kingdom | united-states }
```

```
undo shutdown
```

2.1.3 Configuring the Central Router

The central router or console terminal needs to be configured by the network administrator, who determines which interfaces should be configured based on network connection. The following describes the interfaces and their configuration.

I. Serial interface (Serial/Async/E1-F/T1-F) configuration

Note:

The Serial/Async/E1-F/T1-F interfaces have similar configurations: all chose PPP encapsulating protocol assign an IP address to the peer. The difference is that the Serial/E1-F/T1-F interface works in the synchronous mode (by default) and is configured in Serial view while Async interface works in the asynchronous mode and is configured in Async interface view.

1) Configuring the IP address pool

Perform the following configuration in system view.

Table 2-3 Configure the IP address pool

Operation	Command
Define the IP address pool assigning addresses to PPP users	**ip pool** *pool-number*

2) Enabling PPP on the Serial interface

Perform the following configuration in Serial view.

Table 2-4 Enable PPP on the Serial interface

Operation	Command
Enable PPP on the Serial interface	**link-protocol ppp**

3) Assigning an IP address to the peer end on the Serial interface

Perform the following configuration in Serial view.

Table 2-5 Assign an IP address to the peer end

Operation	Command
Assign an IP address to the peer end	**remote address** { *ip-address* | **pool** [*pool-number*] }

II. E1/T1/E3/T3 interface configuration

Perform the following configuration in Controller e1/t1/e3/t3 view.

Table 2-6 Set working status for E1/T1/E3/T3 interface

Operation	Command
Set E1 interface into non-channelized mode	**using e1**
Bind all the timeslots of T1 interface to serial interface	**channel-set 0 timeslot-list 1-24**
Set E3 interface into non-channelized mode	**using e3**
Set T3 interface into non-channelized mode	**using t3**

In addition, make the same configuration on those generated Serial interfaces.

III. Ethernet interface configuration

Enable DHCP Server to assign an IP address to the Ethernet interface corresponding to the router to be configured.

Table 2-7 Establish the DHCP address pool and configuring the range of the dynamic IP address

Operation	Command
Establish the DHCP address pool or enter the DHCP address pool view (system view)	**dhcp server ip-pool** *pool-name*
Configure the range of the dynamic IP address (DHCP address pool view)	**network** *ip-address* [**mask** *netmask*]

IV. Originating a Telnet/FTP connection

First confirm the interface IP address of the router to be configured, and then originate a Telnet/FTP connection to log into it for configuration or loading configuration files.

By default, the user name and password for Telnet/FTP login are both “admin”.

V. Connecting by dialing through AM interface

First connect the AM interface on the router to be configured with the remote console terminal in the central equipment room through PSTN. Then the administrator can set up a connection at the remote teminal by dialing in flow mode using terminal emulation program. In this program, the settings are:

Interface for actual connection: RS-232 serial interface

Termianl communication paramter:

Baudrate: 9600 bps

Data bit: 8

Stop bit: 1

Parity check: None

Flow control: None/hardware

Terminal emulatio: VT100/auto-detection.

By default, the user name and password for dialing login are both “admin”.

Note:

Here only key key configurations are listed. As for others , you can adopt the default configuration.

2.1.4 Switching between Console and AUX

On low-end router, the functionality of Console and AUX ports is support by the same physical interface, namely CONSOLE. In user interface view, the physical interface CONSOLE can be configured to operate in either Console or AUX mode.

Note:

Make sure to setup telnet server on the router before changing to AUX mode.

To setup physical interface CONSOLE to AUX mode:

Step 1: Enter system view

Step 2: In ***user-interface console 0*** view, enter ***console switch-to aux***

To set up a configuration environment by connecting the AUX port on the router through modem dial, you need to attach a modem to the serial port on the PC and a modem to the AUX port on the router, as shown in Figure 2-2.

Step 1: Attach a modem to the AUX port.

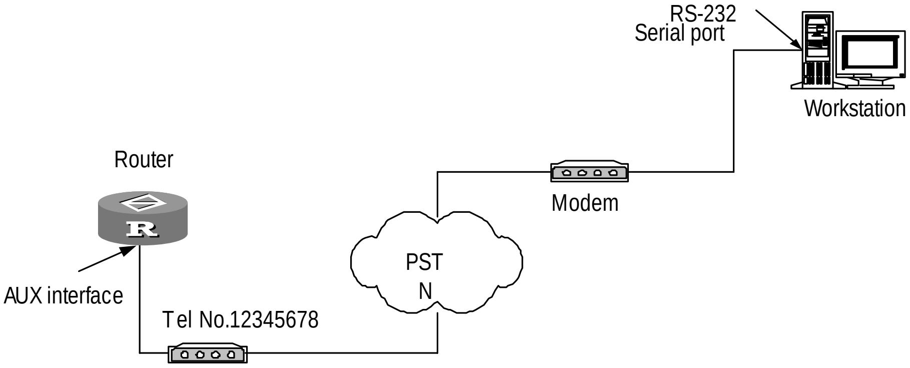


Figure 2-2 Set up a remote configuration environment

Step 2: Dial to connect the router remotely by using a terminal emulation program (such as Windows9X HyperTerminal). In the HyperTerminal, select the RS-232 serial port of the PC for connection, and set the terminal communication parameters similar to those used for setting up connection through the console port:

Bits per second: 9600

Data bits: 8

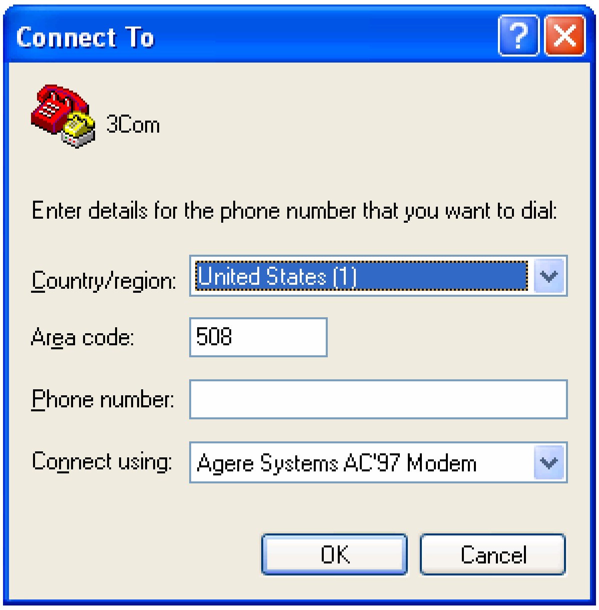
Stop bits: 1

Parity: None

Flow control: None or hardware control

TermType: VT100

See Figure 2-3 and Figure 2-4.


Connect To

3Com

Enter details for the phone number that you want to dial:

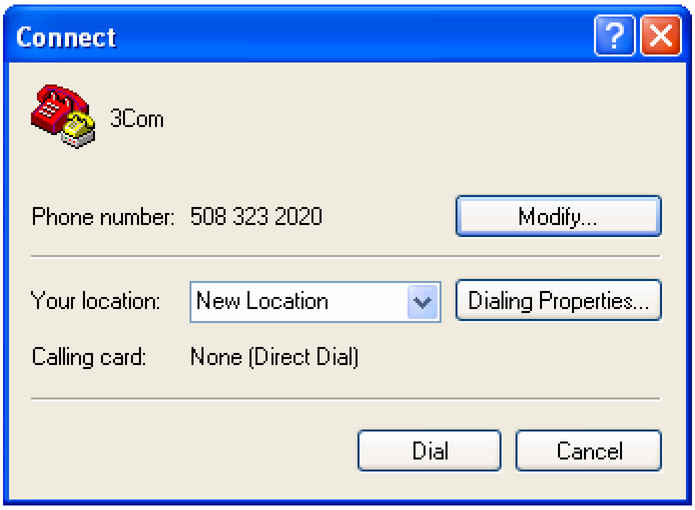
Country/region: United States (1)

Area code: 508

Phone number:

Connect using: Agere Systems AC'97 Modem

Figure 2-3 Set the number to be dialed



Phone number: 508 323 2020

Your location: New Location

Calling card: None (Direct Dial)

Figure 2-4 Dial on the remote PC

Step 3: Enter the correct username and password. When you see the command line prompt (<3Com> for example) in the HyperTerminal configure or manage the router.

2.1.5 Displaying and Debugging auto-config

Perform the following configuration in user view.

Table 2-8 Display auto-config

Operation	Command
Display the status of auto-config	**display auto-config**

2.1.6 Auto-config Configuration Example 1

I. Network requirements

The router to be configured R2 supports the auto-config function and is installed with an E1 interface module. The central router R1 is connected to R2 through the E1 interfaces. The administrator implements corresponding configurations on R1, and then loads the configuration file “3ComR2.cfg” to R2 using FTP.

II. Network diagram

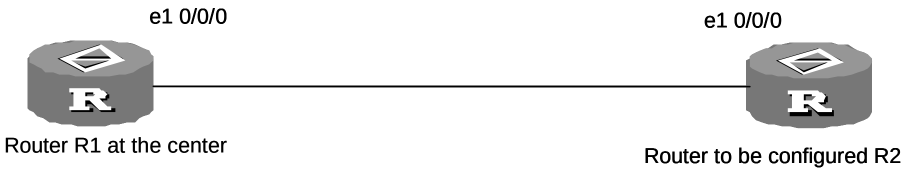


Figure 2-5 Network diagram for auto-config configuration (through E1 interface)

III. Configuration procedure

1) Configure R1 at the center

# Configure controller interface.

```
[3Com] controller e1 0/0/0
[3Com-e1 0/0/0] using e1
```

# Configure e1 interface to originate interface serial 0/0/0 and assign the IP address to the peer.

```
[3Com] ip pool 1 192.10.1.1
[3Com] interface serial0/0/0
[3Com-serial0/0/0] link-protocol ppp
[3Com-serial0/0/0] ip address 192.10.1.2 255.255.255.0
[3Com-serial0/0/0] remote address pool 1
```

# FTP the configuration file to the remote router

```
<3Com > ftp 192.10.1.1
[ftp] put 3ComR2.cfg configv 2.41cfg.cfg
```

Here v 2.41cfg.cfg is the default name of the configuration file on router.

2) Configure R2

R2 starts and runs the auto-config function automatically, generating the following configuration:

```
ftp server enable
local-user admin password cipher admin
service-type telnet terminal
level 3
service-type ftp
controller e1 0/0/0
using e1
interface serial 0/0/0
link-protocol ppp
ip address ppp-negotiate
-negotiate
gotiate
iate
e
-negotiate
gotiate
iate
e
user-interface vty 0 4
authentication-mode scheme
```

Corresponding configuration is auto-genearted concurrently on the fixed interface of the router.

2.1.7 Auto-config Configuration Example 2

I. Network requirements

The router to be configured R2 provides a fixed Ethernet interface which supports the auto-config function. The central router R1 is connected to the R2 through Ethernet. The administrator performs the corresponding configuration and loads the configuration file “3ComR2.cfg” to R2 using FTP.

II. Network diagram

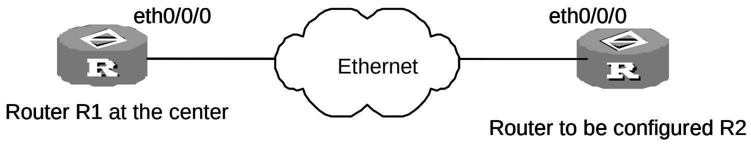


Figure 2-6 Network diagram for auto-config configuration (through E1 interface)

III. Configuration procedure

1) Configure central router R1

# Configure IP address pool and IP address of the interface.

```
[3Com] dhcp server ip-pool 0
[3Com- dhcp-0] network 192.10.1.0 mask 255.255.255.0
[3Com-dhcp-0] quit
[3Com] interface ethernet0/0/0
[3Com-ethernet0/0/0] ip address 192.10.1.2 255.255.255.0
```

# FTP the configuration file to the remote router.

```
<3Com > ftp 192.10.1.1
[ftp] put 3ComR2.cfg v 2.41cfg.cfg
```

You can view the address 192.10.1.1 assigned to R2 using the **display dhcp server ip-in-use** command for a FTP login. The name of the default configuration file on router is v 2.41cfg.cfg.

2) Router to be configured R2

R2 starts and runs the auto-config function automatically, generating the following configuration:

```
ftp server enable
local-user admin password cipher admin
service-type telnet terminal
level 3
```

```
service-type ftp
interface ethernet 0/0/0
ip address dhcp-alloc
user-interface vty 0 4
authentication-mode scheme
```

Corresponding configuration is auto-genearted concurrently on the fixed interface of the router.

2.1.8 Configuration Example 3

I. Network requirements

The router to be configured R2 offers the auto-config function and is installed with a SIC-1AM interface card and an E1 interface module. The AM interface on R2 is connected with the remote console terminal through PSTN. The administrator dials at the remote terminal to log into R2 for configuration,

II. Network diagram

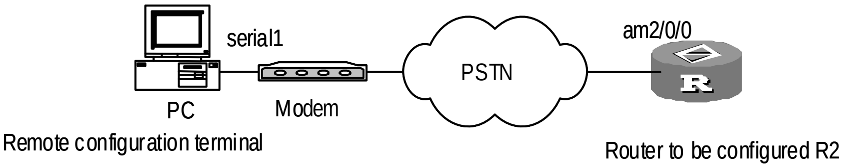


Figure 2-7 Network diagram for auto-config configuration (through AM interface)

III. Configuration procedure

1) Configure R1

Configure the following parameters on the remote console terminal (the HyperTerminal on PC):

Interface for connection: serial interface 1

Baudrate(B): 9600

Data bit (D): 8

Parity check (P): 0

Stop bit (S): 1

Flow control (F): no/hardware

Terminal emulation (E): VT100/auto-detection

You can log into R2 after the dialup connection is established.

2) Router to be configured R2

R2 starts and runs the **auto-config** automatically, generating the following configuration:

```
ftp server enable
local-user admin password cipher admin
service-type telnet terminal
level 3
service-type ftp
interface analogmodem 2/0/0
async mode flow
country-code united-kingdom
user-interface tty 0
modem call-in
authentication-mode scheme
```

Corresponding configuration is auto-genearted concurrently on the fixed interface and E1 interface of the router.

2.2 Maintenance and Debugging Function

2.2.1 Testing Network Connection

I. ping

The **ping** command is mainly used to check a network connection and test whether the host is reachable.

Perform the following operations in any view.

Table 2-9 The **ping** command

Operation	Command
Support ping of IP	**ping** [**-a** *X.X.X.X*] [**-c** *count*] [**-d**][**-f**] [**-h** *ttl_value*] [**-i** {*interface-type interface-number* }][**ip**] [**-n**] [**-p** *pattern*] [**-q**] [**-r**] [**-s** *packetsize*] [**-t** *timeout*] [**tos**] [**-v**] [**vpn-instance** *vpn-instance-name*] *host*

For more information about the options and parameters, refer to the section introducing the **ping** command in the *Command Manual*.

The information output upon the execution of the command includes:

- The response to each **ping** packet. If receiving no response packet upon the expiration of the timeout setting, the system will output “Request time out”. Otherwise, the system will output the information of the response packet in bytes, sequence number, TTL, and response time.
- Sum information of the statistics, including transmitted packets, number of received packets, percentage of unacknowledged packets to all transmitted packets, and minimum, maximum, and mean response times.

For example:

```
<3Com> ping 202.38.160.244
ping 202.38.160.244 : 56 data bytes, press CTRL-C to break
Reply from 202.38.160.244 : bytes=56 sequence=1 ttl=255 time = 1ms
Reply from 202.38.160.244 : bytes=56 sequence=2 ttl=255 time = 2ms
Reply from 202.38.160.244 : bytes=56 sequence=3 ttl=255 time = 1ms
Reply from 202.38.160.244 : bytes=56 sequence=4 ttl=255 time = 3ms
Reply from 202.38.160.244 : bytes=56 sequence=5 ttl=255 time = 2ms
--202.38.160.244 ping statistics--
5 packets transmitted
5 packets received
0% packet loss
round-trip min/avg/max = 1/2/3 ms
```

II. tracert

tracert is used to test the gateways that a packet sent by the host will pass by in order to reach the destination. It is mainly used to test whether a network connection is reachable and to locate the position where faults occur on the network.

The **tracert** command is executed following this procedure: The system first sends a packet with TTL as 1 and the first hop returns an ICMP error message indicating that the packet cannot be transmitted due to TTL timeout. Then the system transmits the packet again with TTL being set to 2 and the second hop returns TTL timeout message similarly. This process continues until the packet reaches its destination. The purpose of such a process is to record the source addresses where these ICMP TTL timeout messages are sent to outline the path along which the IP packet can reach the destination.

Perform the following operation in any view.

Table 2-10 Trace the gateways between a source host and a destination host

Operation	Command
Trace the gateways between a source host and a destination host	**tracert** [**-a** *X.X.X.X*] [**-f** *first_TTL*] [**-m** *max_TTL*] [**-p** *port*] [**-q** *nqueries*] [**vpn-instance** *vpn-instance-name*] [**-w** *timeout*] *host*

For more information about the options and parameters of the command, refer to the section introducing the **tracert** command in the *Command Manual*.

Following are examples of using **tracert** for network analysis.

Example 1:

```
<3Com> tracert 35.1.1.48
traceroute to nis.nsf.net (35.1.1.48), 30 hops max, 56 byte packet
```

```
1  helios.ee.lbl.gov (128.3.112.1)  19 ms  19 ms  0 ms
2  lilac-dmc.Berkeley.EDU (128.32.216.1)  39 ms  39 ms  19 ms
3  ccngw-ner-cc.Berkeley.EDU (128.32.136.23)  39 ms  40 ms  39 ms
4  ccn-nerif22.Berkeley.EDU (128.32.168.22)  39 ms  39 ms  39 ms
5  128.32.197.4 (128.32.197.4)  40 ms  59 ms  59 ms
6  131.119.2.5 (131.119.2.5)  59 ms  59 ms  59 ms
7  129.140.70.13 (129.140.70.13)  99 ms  99 ms  80 ms
8  129.140.71.6 (129.140.71.6)  139 ms  239 ms  319 ms
9  129.140.81.7 (129.140.81.7)  220 ms  199 ms  199 ms
10  nic.merit.edu (35.1.1.48)  239 ms  239 ms  239 ms
```

The information displayed above gives the GWs between the source host and the destination, which is very helpful in network analysis.

Example 2:

```
<3Com> tracert 18.26.0.115
traceroute to allspice.lcs.mit.edu (18.26.0.115), 30 hops max
1  helios.ee.lbl.gov (128.3.112.1)  0 ms  0 ms  0 ms
2  lilac-dmc.Berkeley.EDU (128.32.216.1)  19 ms  19 ms  19 ms
3  lilac-dmc.Berkeley.EDU (128.32.216.1)  39 ms  19 ms  19 ms
4  ccngw-ner-cc.Berkeley.EDU (128.32.136.23)  19 ms  39 ms  39 ms
5  ccn-nerif22.Berkeley.EDU (128.32.168.22)  20 ms  39 ms  39 ms
6  128.32.197.4 (128.32.197.4)  59 ms  119 ms  39 ms
7  131.119.2.5 (131.119.2.5)  59 ms  59 ms  39 ms
8  129.140.70.13 (129.140.70.13)  80 ms  79 ms  99 ms
9  129.140.71.6 (129.140.71.6)  139 ms  139 ms  159 ms
10  129.140.81.7 (129.140.81.7)  199 ms  180 ms  300 ms
11  129.140.72.17 (129.140.72.17)  300 ms  239 ms  239 ms
12  * * *
13  128.121.54.72 (128.121.54.72)  259 ms  499 ms  279 ms
14  * * *
15  * * *
16  * * *
17  * * *
18  ALLSPICE.LCS.MIT.EDU (18.26.0.115)  339 ms  279 ms  279 ms
```

The information displayed above gives the GWs between the source host and the destination, as well as the failed GWs.

2.2.2 Enabling IP Source Routing

Perform the following configuration in system view.

Table 2-11 Enable IP source routing

Operation	Command
Enable IP source routing	**ip option source-routing**
Disable IP source routing	**undo ip option source-routing**

The router can process the packets with the IP source-route option only after IP source routing is enabled.

By default, IP source routing is disabled to decrease the risk of attacks. You may enable and use it in conjunction with the **ping** or **tracert** command executed on other devices when troubleshooting network path faults or transmitting some special service.

2.2.3 Enabling DF-Bit Check for IP Packets

Perform the following configuration in system view.

Table 2-12 Enable DF-bit check for IP packets

Operation	Command
Enable DF-bit check for IP packets	**ip df-check enable**
Disable DF-bit check for IP packets	**undo ip df-check enable**

By default, DF-bit check is enabled for IP packets.

2.2.4 Enabling/Disabling the Router to Send ICMP Unreachable Messages

Perform the following configuration in system view.

Table 2-13 Enable/disable the router to send ICMP unreachable messages

Operation	Command
Enable the router to send ICMP unreachable messages	**icmp unreach send**
Disable the router to send ICMP unreachable messages except for protocol unreachable, port unreachable, and fragmentation needed and DF-set messages)	**undo icmp unreach send**

By default, ICMP unreachable messages are sent.

2.2.5 Debugging the System

The CLI of the system provides a variety of debugging functions for helping the users diagnose and isolate faults. The debugging functions are available for almost all the protocols and functions supported by the router.

The output of debugging information can be controlled by two switches:

- Protocol debugging switch determining whether the debugging information output of a protocol is allowed
- Screen output switch determining whether the debugging information output on the screen of a user is allowed

The relationship of the two switches is displayed in the following diagram.

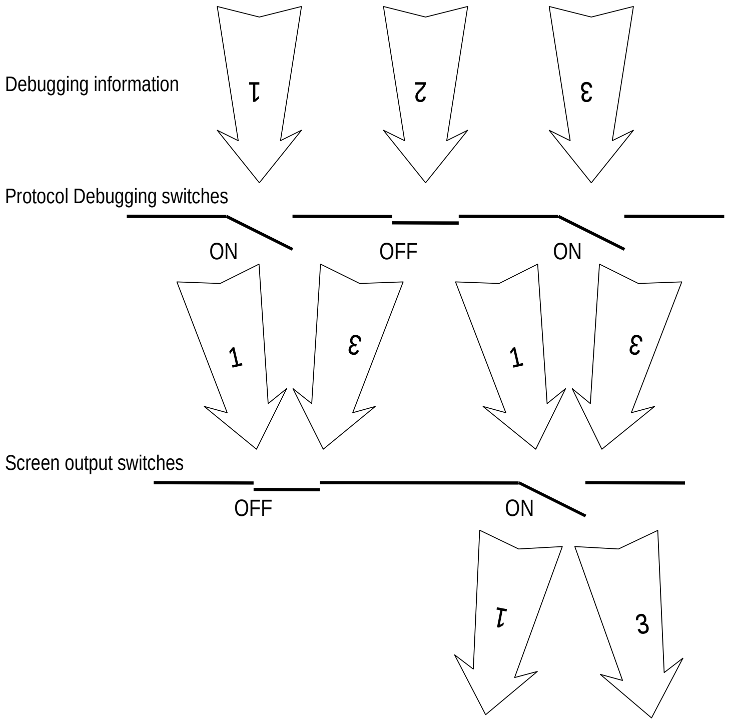


Figure 2-8 Debugging information output diagram

The protocol debugging switch is controlled by the **debugging** command. Perform the following operations in user view.

Table 2-14 Enable, disable, and display the debugging switches

Operation	Command
Enable protocol debugging switches	**debugging** { **all** | *module-name* [*debug-option1*] [*debug-option2*] …}
Disable protocol debugging switches	**undo debugging** { **all** | *module-name* [*debug-option1*] [*debug-option2*] … }

Operation	Command
Display the enabled debugging switches	**display debugging** [**interface** { *interface-type interface-number* }] [*module-name*]

For the use of specific debugging commands and the format of debugging information, refer to the relevant sections.

The screen output switch is controlled by the information center. For more information about it, refer to the next section.

2.2.6 Rebooting the System

Sometimes, it is required to reset the Router to upgrade the file system, or for any other reasons. There is a special command “reboot” that allows the user to reboot the Router. Alternatively, you can simply turn off the power of the Router and then turn it on to produce the same effect.

Perform the following operation in user view.

Table 2-15 Reset the system

Operation	Command
Reboot the Router	**reboot**

⚠ **Caution:**

This command should be used with caution, for the operation will render the network unusable for a short period.
Before rebooting the Router, remember to save the configuration file if necessary,.

2.3 Information Center

2.3.1 Introduction

Information center is an indispensable part of the router's main software and exists as an information hub in the router. The information center manages most information outputs, sorts the information carefully, and hence can screen the information efficiently. Combined with the debug program, it can provide powerful support for the network administrators and developers in network operation monitor and fault diagnosis.

The information center of the system has the following features:

- Available with three types of information, which are log information, trap information, and debug information.
- The information is sorted into eight levels by severity and can be filtered by level.
- The system can support ten channels. The first six channels, or Channels 0 through 5, have their default channel names and are associated with six output directions by default. Both the names of the routers and the associations between the channels and output directions can be changed through commands
- Support six information output directions, including the Console, Telnet terminal and console terminal (monitor), logbuffer, loghost, trapbuffer, and SNMP.
- The system is composed of a variety of protocol modules, board drivers, and configuration modules. The information can be classified and filtered by source module.
- Each information header consists of several fixed parts, which are time stamp, information source module, information level, slot number of the information source, and the information digest.

To sum up, the major task of the information center is to output the three types of information of the modules onto the ten channels in terms of the eight severity levels and according to the user’s settings, and then redirect the ten information channels to the six output directions.

2.3.2 Configuring the Information Center

I. Enabling/Disabling the information center

Perform the following operations in system view.

Table 2-16 Enable/disable the information center

Operation	Command
Enable the information center	**info-center enable**
Disable the information center	**undo info-center enable**

Note:

By default, the information center is enabled. An enabled information center will affect the system performance in some degree due to the work in information sorting and output. Such impact becomes more obvious in the event that there is enormous information waiting for processing.

II. Naming an information channel

Perform the following operation in system view.

Table 2-17 Name an information channel

Operation	Command
Name the information channel numbered *channel-number* as *channel-name*	**info-center channel** *channel-number* **name** *channel-name*

The parameter *channel-number* is ranging from 0 to 9, corresponding to the ten channels of the system. The parameter *channel-name* is a channel name that may comprise up to 30 characters but '-‘, ‘/’ and ’\’.

The system specifies the default names for Channels 0 through 5, which are listed in the following table.

Table 2-18 Default channel names

Channel-number	Channel-name
0	Console
1	monitor
2	loghost
3	trapbuffer
4	logbuffer
5	snmpagent

III. Information severity

The information center classifies the information into eight levels by severity or emergency. If filtered by severity, the information of a severity level greater than the defined threshold will be filtered out for output. A more emergent packet has a smaller severity level. The parameter “emergencies” represents the severity level 1 and debugging the severity level 8. Therefore, all the information will be output if the severity threshold is set to debugging.

Table 2-19 Severities defined in syslog

Severity	Description
emergencies	Emergent errors
alerts	Errors requiring immediate correction
critical	Critical errors
errors	Errors requiring attention but not quite critical
warnings	Warnings indicating possible existence of errors
notifications	Information requiring attention

Severity	Description
informational	Common prompt information
debugging	Debugging information

# Enable to output log information of IP module and allow outputting the information with the severity of warnings and lower levels only.

```
[3Com] info-center source ip channel snmpagent log level warnings
```

IV. Defining the contents of an information channel

Perform the following operations in system view.

Table 2-20 Define the contents of an information channel

Operation	Command
Add a record to an information channel	**info-center source** { *module-name* | **default** } { **channel** { *channel-number* | *channel-name*} } [**log** { **state** { **on** | **off** } | **level** *severity* }* | **trap** { **state** { **on** | **off** } | **level** *severity* } * | **debug** { **state** { **on** | **off** } | **level** *severity* }*]*
Delete a record from an information channel	**undo info-center source** { *module-name* | **default** } { **channel** { *channel-number* | *channel-name* }

module-name specifies a module name and **default** stands for the default record in the information channel. **level** is the severity level of information and the information at a level greater than *severity* is prohibited from being output. *severity* is the setting of information level. *channel-number* and *channel-name* are the information channel number and name to be set.

Each information channel has a default record for which the module name is **default**. But for different channels, the record may have different default settings for logging information, trapping information, and debugging information. If a module has no explicit configuration record in the channel, the default configuration record will be used.

⚠ **Caution:**

When there are multiple Telnet users or terminal server users at the same time, they can share some configuration parameters, including the setting of filtering by module, language selection, and the severity threshold. The changes that one user made on these settings will also be shown on other users' terminals.

V. Information output

By far, the information center of router's main software can output the information to seven directions.

- Output information to a local Console via the Console port.
- Output information to a remote Telnet terminal in support of remote maintenance.
- Allocate a logbuffer of proper size inside the router for recording information.
- Configure the loghost, to which the information center will directly send information and on which information will be stored in files for future retrieval.
- Allocate a trapbuffer of proper size inside the router for recording information.
- Output information to the SNMP Agent.
- Output information to the log file.

Each output direction will be specified with a desired channel by using a configuration command and all the information will be sent to the associated directions after being filtered by the specified channels. By configuring the channel for each output direction and the filtering information of the channel as required, the user could complete the filtration and redirection of different types of the information.

Perform the following operations in system view.

Table 2-21 Output information

Operation	Command
Output information to the console	**info-center console channel** { *channel-number* | *channel-name* }
Disable the information center to output information to the console	**undo info-center console channel**
Output information to a telnet terminal or a terminal server	**info-center monitor channel** { *channel-number* | *channel-name* }
Disable the information center to output information to Telnet terminals	**undo info-center monitor channel**
Output information to SNMP	**info-center snmp channel** { *channel-number* | *channel-name* }
Disable the information center to output information to SNMP	**undo info-center snmp channel**

Operation	Command
Set the size of the logbuffer and set the information channel for information output to the logbuffer	**info-center logbuffer** [**channel** { *channel-number* | *channel-name* } | **max-size** *buffersize*] *
Disable logbuffer or restore the default value	**undo info-center logbuffer** [**channel** | **max-size**]
Set the channel for information output to the loghost and other parameters	**info-center loghost** *X.X.X.X* [**channel** { *channel-number* | *channel-name* } | **facility** *local-number* | **language** { **chinese** | **english** }] *
Disable the information center to output information to a log host	**undo info-center loghost** { *X.X.X.X* | **source** }
Set the channel number for outputting system information to the log file	**info-center logfile channel** { *channel-number* | *channel-name* } *
Disable the information center to output log information to the log file	**undo info-center logfile channel**
Disable the information output to the loghost	**undo info-center loghost** *X.X.X.X*
Set the size of the trapbuffer and set the channel for information output to the trapbuffer	**info-center trapbuffer** [**channel** { *channel-number* | *channel-name* } | **max-size** *buffersize*] *
Disable the trapbuffer or restore the default value	**undo info-center trapbuffer** [**channel** | **size**]

The system assigns six output directions each an information channel by default, as shown in the following table:

Table 2-22 Default information channels assigned to each direction

Output direction	Information channel No.	Default channel name
Console	0	console
Monitor terminal	1	monitor
Log host	2	loghost
Trap buffer	3	trapbuffer
Log buffer	4	logbuffer
SNMP	5	snmpagent

🕮 **Note:**

The settings of the six output directions are independent but you must enable the information center first before the settings can become valid.

VI. Sending source address for system information

Perform the following operations in system view.

Table 2-23 Send source address for logging information

Operation	Command
Send source address for logging information	**info-center loghost source** *interface-type interface-number* [*subinterface-type*]
Cancel the setting	**undo info-center loghost source**

VII. Setting the format of the time stamp

Perform the following configuration in system view.

Table 2-24 Set the format of the time stamp

Operation	Command
Set a time stamp format for the system information output to the information channels except for the log host	**info-center timestamp** { **trap** | **debugging** | **log** } { **boot** | **date** | **none** }
Restore the default time stamp format for the system information output to the information channels except for the log host	**undo info-center timestamp** { **trap** | **debugging** | **log** }
Set a time stamp format for the system information output to the log host	**info-center timestamp loghost** { **date** | **no-year-date** | **none** }
Restore the default time stamp format for the system information output to the log host	**undo info-center timestamp loghost**

By default, the boot time stamp is adopted for debugging information output to the channels except for the log host, whereas the date time stamp is adopted for other information.

By default, the date time stamp is adopted for system information output to the log host.

2.3.3 Setting Display Terminal

Setting a display terminal is to control whether the debug/log/trap information from the information center will be output to a user’s terminal.

Perform the following operations in user view.

Table 2-25 Set a display terminal

Operation	Command
Enable the terminal information display function	**terminal monitor**
Enable the terminal logging information display function	**terminal logging**
Enable the terminal trapping information display function	**terminal trapping**
Enable the terminal debugging information display function	**terminal debugging**
Disable the terminal information display function	**undo terminal monitor**
Disable the terminal logging information display function	**undo terminal logging**
Disable the terminal trapping information display function	**undo terminal trapping**
Disable the terminal debugging information display function	**undo terminal debugging**

These commands can only affect the current terminal at which the commands are input.

The execution of the command **undo terminal monitor** (for disabling the display terminal), is equivalent to that of the commands of **undo terminal debugging**, **undo terminal logging**, and **undo terminal trapping**, that is, all the debugging, log, and trap information will not be displayed at the current terminal. Given that the **terminal monitor** has been enabled, using the **terminal debugging**/**undo terminal debugging**, **terminal logging**/**undo terminal logging**, **terminal trapping**/**undo terminal trapping** commands can respectively enable and disable the output of debugging/logging/trapping information.

By default, terminal display is turned on for console users, allowing all prompt messages to be output to the console terminal.

For other types of terminal user, AUX, VTY, and TTY, terminal display is turned off by default. To have the prompt messages for them output to the console terminal, you need to configure the **terminal monitor** command.

2.3.4 Syslog Overview

The syslog function is a sub-function of the information center module.

This section mainly describes the format of system information (including log, debug, and trap) output to the log host.

For information output to the log host, port 514 and the format described in the following figure are used.

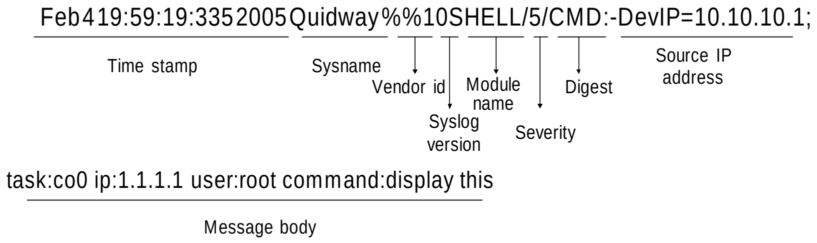

Feb 4 19:59:19:335 2005 Quidway %%10SHELL/5/CMD:-DevIP=10.10.10.1;
Time stamp
Sysname
Vendor id
Module name
Digest
Source IP address
Syslog version
Severity
task:co0 ip:1.1.1.1 user:root command:display this
Message body

Figure 2-9 Format of system information

The following subsections describe the major fields of system information.

II. Time stamp

Use the **info-center timestamp loghost** command to set a time stamp format for system information output to the log host. The following options are available:

- Date, in the format of MM DD hh:mm:ss YY, provides year information.
- No-year-date, in the format of MM DD hh:mm:ss, does not provide year information.
- None, does not provide a timestamp.

The following describes the fields of time stamp:

- MM indicates month of the year, which could be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, or Dec.
- DD indicates day of the month. Numbers less than 10 are prefixed by a space.
- hh:mm:ss indicates the local time, where hh ranges from 00 to 23, and mm and ss from 00 to 59.

The time stamp field is separated from the sysname field by a space.

III. Sysname

This field indicates host name; the default is 3Com.

You may use the **sysname** command to change the name of your router.

The sysname field is separated from the vendor ID field by a space.

IV. Vendor ID

This field is separated from the module name field by a space.

V. Module name

This field indicates the module creating this logging information. For a complete module list, execute the **info-center source ?** command in system view.

The module name field is separated from the severity field by a slash (/).

VI. Severity

There are eight severity levels numbered one through eight. For more information, see "Table 2-19".

The severity field is separated from the digest field by a slash (/).

VII. Digest

This field provides an abstract of information. It is separated from the source address field by a colon (:).

VIII. Source IP address

This field indicates the source address of the message sent to the log host. It is displayed only when the **loghost source** command is configured.

The source IP address field is separated from the message body field by a semicolon (;).

IX. Message body

Message body is created by the sending module. For example, "task:co0 ip:** user:root command:display this" indicates that a console user named root input the **display this** command.

2.3.5 Setting a Log Host

You may specify up to four log hosts. By default, information is sent to a log host through the loghost channel (information channel 2). The command **info-center loghost** is used to set the log host.

The source IP address of the log can be set to the address of a fixed interface. In this way, the log host can be used to perform the classification management for the log through the source address. For example, the **info-center loghost source** *loopback0* command can be used to set all the source addresses of the logs sent by the system to be the address of *loopback0* interface.

2.3.6 Enabling/Disabling Synchronous Terminal Output

When you are editing a command line, the output of system information may interrupt your work. With synchronous terminal output enabled, the system can re-display the input that you are editing after the system information output is completed.

Perform the following configuration in system view.

Table 2-26 Enable/disable synchronous terminal output

Operation	Command
Enable synchronous terminal output	**info-center synchronous**

Operation	Command
Disable synchronous terminal output	**undo info-center synchronous**

By default, synchronous terminal output is disabled.

2.3.7 Displaying and Debugging Information Center

After the above configuration, execute the **display** command in any view to display the running of the information center after configuration, and to verify the configuration.

Execute the **debugging** command in user view for the debugging of the information center.

Table 2-27 Display and debug information center

Operation	Command
Display information in the information center	**display info-center**
Display information in log buffer	**display logbuffer** [**size** *size-value* | **summary**] [**level** *level-number*] [**|** [**begin** | **include** | **exclude**] *string*]
Display information on the specified information channel or all information channels	**display channel** [*channel-number* | *channel-name*]
Display information in trap buffer	**display trapbuffer** [**size** *sizeval*]

2.3.8 Information Center Configuration Example

I. Console information output

1) Enable the info-center.

```
[3Com] info-center enable
```

2) Configure Console log output, permitting the log output of PPP module and setting the severity level to be in the range of emergencies to debugging.

```
[3Com] info-center console channel console
[3Com] info-center source ppp channel console log level debugging
```

3) Enable debugging of the PPP module.

```
<3Com> debugging ppp all
```

II. Outputting log information to the loghost (UNIX workstation)

Step 1: Configure the router

1) Enable the info-center

```
[3Com] info-center enable
```

2) Use the UNIX workstation at 202.38.1.10 as the loghost and set the severity threshold to informational and output language to English, and allow PPP and IP modules to output information using the UNIX device local4.

```
[3Com] info-center loghost 202.38.1.10 language english
[3Com] info-center loghost 202.38.1.10 facility local4
[3Com] info-center source ppp channel loghost log level informational
[3Com] info-center source ip channel loghost log level informational
```

Step 2: Configure the loghost

To implement the above functions, some configurations should also be made on the UNIX host. The configuration procedure described below is completed on SunOS 4.0 and the similar procedure is followed if the UNIX OS of some other vendor is adopted.

3) Execute the following commands as the root user.

```
#mkdir           /var/log/3Com
#touch           /var/log/3Com/information
```

4) Edit the file /etc/syslog.conf and add the following selector/action pairs as the root.

```
# 3Com configuration messages
local4.info    /var/log/3Com/information
```

Note:

When editing the file /etc/syslog.conf, you should note that:

- Remarks must be in independent lines and begin with the character #.
- Use a tab rather than a space as the delimiter between selector/action pairs.
- Do not leave unwanted space behind a file name.

The device name and the permitted log information level specified in /etc/syslog.conf should keep in consistence with the **info-center loghost** and **info-center loghost** a.b.c.d facility that have been configured on the router, in case of the incorrect output of log information to the loghost.

After the log files ‘config’ has been established and the file "/etc/syslog.conf" has been modified, the following command should be executed to send a HUP signal to the system daemon ‘syslogd’ to have it reread its configuration file "/etc/syslog.conf".

```
#ps -ae | grep syslogd
147
#kill -HUP 147
```

Upon completion of the above operations, the router can output the related information to the corresponding log files.

The configuration made above permits outputting informational and higher level system information only, that is, information with severity levels 0 through 6, to the log host.

The lowest level of system information is debugging. The setting of debugging will cause all system information to be output to the loghost and this may affect system performance. Therefore, it is not recommended to set information level to debugging in normal circumstances.

Note:

For purpose of filtering, you can sort information, taking into account facility, severity, filter, and the syslog.conf file.

2.4 Displaying and Debugging the Device Running State — AR46 Series

Note:

The commands in this section are available with the AR 46 Series Routers but not available with the AR 28 Series Routers.

The device operating management includes monitoring the running status of the device and configuring the parameters for the device. In terms of function, the management includes:

- Display the device initialization information and the essential running information.
- Display and reset alarm and status information of the device.
- Reboot the device and set the default boot file.

I. Displaying device

Perform the following operations in any view.

Table 2-28 Display device information

Operation	Command
Display the basic information of the device	**display device** *slot-number*
Display the environment information	**display environment**
Display alarm and state information for the device	**display alarm urgent** [**time | slot | id**]
Display parameter setting for scheduled rebooting	**display schedule reboot**

II. Resetting device

Perform the following operations in user view.

Table 2-29 Reset device

Operation	Command
Clear all the stored alarm information	**reset alarm urgent**

III. Configuring device

Perform the following operations in system view.

Table 2-30 Configure device

Operation	Command
Upgrade a file in an in-service way	**upgrade** [**bootrom** | **pico-code** | **logic**] *filename*
Enable scheduled rebooting on the router and set rebooting date and time	**schedule reboot at** *time* [*date*]
Enable scheduled rebooting on the router and set delay value	**schedule reboot delay** { *time* | *minutes* }
Remove parameter setting for scheduled rebooting	**undo schedule reboot**

📖 **Note:**

- After you configure the **schedule reboot at** command, tuning system time with the **clock** command or through NTP will void the scheduled reboot setting you made. The same applies to the **schedule reboot delay** command.
- Upon the configuration of the **schedule reboot at** command, a timer starts. This timer is cyclic and measured in minutes. For example, if you set at 12:05:26 to have the router reboot at 12:06:00, the router will reboot at 12:06:26 instead of 12:06:00.

IV. Configuring hot-swapping pre-processing

Perform the following operations in user view.

Table 2-31 Configure hot-swapping pre-processing

Operation	Command
Configure hot-swapping pre-processing	**remove slot** *slotnum*
Remove hot-swapping pre-processing	**undo remove slot** *slotnum*

Before inserting or removing a hot-swappable interface card, you must first use the **remove slot** command for pre-processing. You can also cancel a maloperation with the **undo remove slot** command if you change your mind to remove the card after executing the **remove slot** command. The **undo remove slot** command is unnecessary when you remove a card, but insert it immediately.

Chapter 3 Auto Detect Configuration

3.1 Introduction to Auto Detect

Auto detect is a function for checking the connectivity of a network regularly by sending ICMP Request/Reply packets. It works by checking a group of destination IP addresses to see whether the hosts are reachable or unreachable. Based on the result, the router can discover problems and take appropriate actions.

The result of auto detect can be used by other features to control whether the configurations for the features can take effect. These features include:

- Static routing
- Virtual router redundancy protocol (VRRP)
- Interface backup

An auto detect group can be referenced simultaneously by multiple application instances.

Note:

For a detailed description of static routing, refer to the “Routing Protocol” part of this manual.

For a detailed description of VRRP, refer to the “Reliability” part of this manual.

3.2 Basic Auto Detect Configuration

3.2.1 Basic Auto Detect Configuration Tasks

The following table describes the basic auto detect configuration tasks.

Table 3-1 Auto detect configuration tasks

To do…	Use the command…	Remarks
Enter system view	<3Com> **system-view**	–
Create a detect group and enter detect group view	[3Com] **detect-group** *group-number*	Required

To do…	Use the command…	Remarks
Add an IP address to the detect group. You may use the command multiple times to add up to 100 IP addresses.	[3Com-detect-group-X] **detect-list** *list-number* **ip address** *ip-address* [**nexthop** *ip-address*]	Required
Specify the relationship between the addresses in the detect group	[3Com-detect-group-X] **option** [**and** | **or**]	Optional. Defaults to **and**.
Specify the auto detect interval of a detect group	[3Com-detect-group-X] **timer loop** *seconds*	Optional. Defaults to 15 seconds.
Specify the maximum number of probing retries during each auto detect interval	[3Com-detect-group-X] **retry** *retry-times*	Optional. Defaults to 2.
Specify the timeout period of a probing attempt	[3Com-detect-group-X] **timer wait** *seconds*	Optional. Defaults to 2 seconds.
Display configurations of a specified or all detect groups	<3Com> **display detect-group** [*group-number*]	Optional. Available in any view.

📖 **Note:**

- The prompt of detect group view depends on your configuration.
- For information about the parameters and the related **undo** commands, refer to the command manual.

3.2.2 Auto Detect Configuration Example

I. Network requirements

- Create a detect group numbered 10 on Router A and add two IP addresses: 10.1.1.4 and 192.168.2.2.
- Specify the relationship between the addresses to be probed as logical OR.
- Set the auto detect interval to 60 seconds, the number of probing retries during each detect interval to three, and the timeout period of each probing attempt to three seconds.
- The routes between Routers A, B, and C are reachable.

II. Network diagram

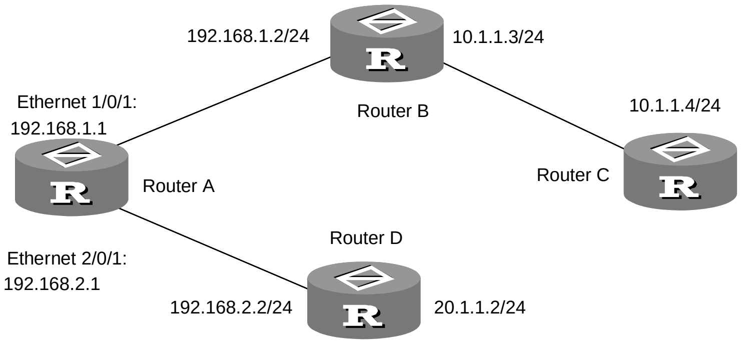


Figure 3-1 Network diagram for basic auto detect configurations

III. Configuration procedure

Configure Router A:

# Enter system view.

```
<3Com> system-view
```

# Create a detect group numbered 10 and enter its view.

```
[3Com] detect-group 10
```

# Add IP address 10.1.1.4 with sequence number 1 to the detect group, taking 192.168.1.2 as the next hop IP address.

```
[3Com-detect-group-10] detect-list 1 ip address 10.1.1.4 nexthop 192.168.1.2
```

# Add IP address 192.168.2.2 with sequence number 2 to the detect group.

```
[3Com-detect-group-10] detect-list 2 ip address 192.168.2.2
```

# Specify the relationship between the two addresses in the detect group as logical OR.

```
[3Com-detect-group-10] option or
```

# Set the auto detect interval to 60 seconds.

```
[3Com-detect-group-10] timer loop 60
```

# Set the maximum number of probing retries during each auto detect interval to 3.

```
[3Com-detect-group-10] retry 3
```

# Set the timeout period of a probing attempt to 3 seconds.

```
[3Com-detect-group-10] timer wait 3
[3Com-detect-group-10] quit
```

# Display the configurations of detect group 10.

```
[3Com] display detect-group 10
```

3.3 Application of Auto Detect in Static Routing

You may reference a detect group in a static route to control validity of the static route according to the result of auto detect as follows:

- When the detect group is reachable, the static route is valid.
- When the detect group is unreachable, the static route is invalid.

3.3.1 Configuring Auto Detect for Static Routing

Note:

Before proceeding with the following configurations, you must define a detect group.

Table 3-2 Configure auto detect for static routing

No.	To do…	Use the command…	Remarks
1	Enter system view	<3Com> **system-view**	–
2	Reference a detect group in a static route	[3Com] **ip route-static** *ip-address* { *mask* **|** *mask-length* } { *interface-type interface-number* | *nexthop* } [**preference** *preference-value*] **detect-group** *group-number*	Required

For information about the parameters, refer to the command manual.

3.3.2 Using Auto Detect with Static Routing

I. Network requirements

- Create a detect group numbered 8 on Router A.
- Configure a static route between Router A and Router C.
- Validate the static route when detect group 8 is reachable.

II. Network diagram

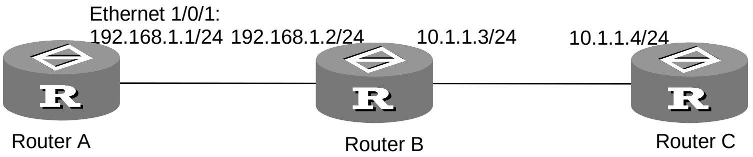


Figure 3-2 Network diagram for application of auto detect in static routing

III. Configuration procedure

Configure Router A:

# Enter system view.

```
<3Com A> system-view
```

# Create a detect group numbered 8 and enter its view.

```
[3Com A] detect-group 8
```

# Add an IP address of 10.1.1.4 with sequence number 1 to the detect group, taking 192.168.1.2 as the next hop IP address.

```
[3Com A-detect-group-8] detect-list 1 ip address 10.1.1.4 nexthop 192.168.1.2
```

# Reference the detect group in a static route, having the route validated when the detect group is reachable.

```
[3Com A] ip route-static 10.1.1.4 24 192.168.1.2 detect-group 8
```

3.4 Application of Auto Detect in VRRP

You may reference a detect group in a VRRP standby group to control the preference levels of the standby interface in the standby group, implementing automatic switching between the master and backup routers as follows:

- When the detect group is unreachable, decrease the preference value of the standby interface in the standby group.
- When the detect group is reachable, restore the preference value of the standby interface in the standby group.

3.4.1 Configuring Auto Detect for VRRP

📖 **Note:**

Before proceeding with the following configurations, you must define a detect group and complete necessary VRRP configuration tasks.

Table 3-3 Configure auto detect for VRRP

No.	To do…	Use the command…	Remarks
1	Enter system view	<3Com> **system-view**	–
2	Enter Ethernet interface view	[3Com] **interface ethernet** *interface-number*	–

No.	To do…	Use the command…	Remarks
3	Reference an auto detect group in VRRP	[3Com-EthernetX] **vrrp vrid** *virtual-router-ID* **track detect-group** *group-number* [**reduced** *value-reduced*]	Required

Note:

- You may configure only up to eight VRRP standby groups.
- The prompt of Ethernet interface view depends on your configuration.
- For information about the parameters and the related **undo** commands, refer to the command manual.

3.4.2 Using Auto Detect with VRRP

I. Network requirements

- Configure dynamic routing on Routers A, B, C, and D, ensuring the routes between Routers A, B, and C are reachable, and the routes between Routers A, D, and C are reachable.
- Router B and Router D form a VRRP standby group numbered 1, whose virtual IP address is 192.168.0.100.
- Normally, data from Router A passes through Router B to reach Router C.
- When the link between Router B and Router C fails, Router D becomes the master in standby group 1 automatically and the data from Router A passes through Router D to reach Router C.

II. Network diagram

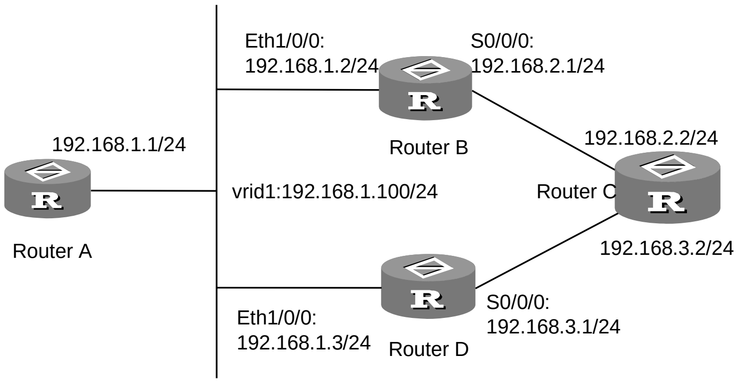


Figure 3-3 Network diagram for application of auto detect in VRRP

III. Configuration procedure

1) Configure Router B:

# Enter system view.

```
<3Com B> system-view
```

# Create a detect group numbered 9 and enter its view.

```
[3Com B] detect-group 9
```

# Add IP address 192.168.2.2 with the sequence number 1 to the detect group.

```
[3Com B-detect-group-9] detect-list 1 ip address 192.168.2.2
[3Com B-detect-group-9] quit
```

# Assign an IP address to Ethernet 1/0/0.

```
[3Com B] interface ethernet1/0/0
[3Com B-Ethernet1/0/0] ip address 192.168.1.2 24
```

# Create a VRRP standby group and assign a virtual IP address to it.

```
[3Com B-Ethernet1/0/0] vrrp vrid 1 virtual-ip 192.168.1.100
```

# Set the standby group preference value of Router B to 110, making this value decrement by 20 when detect group 9 is unreachable.

```
[3Com B-Ethernet1/0/0] vrrp vrid 1 priority 110
[3Com B-Ethernet1/0/0] vrrp vrid 1 track detect-group 9 reduced 20
```

# Configure interface Serial0/0/0.

```
[3Com B-Ethernet1/0/0] interface serial0/0/0
[3Com B-Serial0/0/0] ip address 192.168.2.1 24
```

# Configure dynamic routing. (Omitted)

2) Configure Router D:

# Assign an IP address to Ethernet1/0/0, create a VRRP standby group on the interface, and assign a virtual IP address to the standby group.

```
<3Com D> system-view
[3Com D] interface ethernet1/0/0
[3Com D-Ethernet1/0/0] ip address 192.168.1.3 24
[3Com D-Ethernet1/0/0] vrrp vrid 1 virtual-ip 192.168.1.100
```

# Set the standby group preference value of Router D to 100.

```
[3Com D-Ethernet1/0/0] vrrp vrid 1 priority 100
```

# Configure dynamic routing. (Omitted)

Here, only the auto detect and VRRP configurations on Router B and D are given.

3.5 Application of Auto Detect in Interface Backup

You may use the auto detect function to implement interface backup.

For two interfaces pointing to the same destination, you can specify one of them as the main, and the other as the backup. By referencing a detect group on the backup interface, you can allow the router to do one of the following:

- When the detect group is reachable, use the main interface to transmit data. The backup interface is down.
- When the detect group is unreachable, as the result of a faulty communication link for example, shut down the main interface and enable the backup interface.
- When the unreachable detect group becomes reachable again, that is, when the communication between the main interface and the destination device resumes, fall back to the main interface and shut down the backup interface.

3.5.1 Configuring Auto Detect for Interface Backup

Note:

Before proceeding with the following configurations, you must define a detect group and complete the configurations related to the interfaces.

Table 3-4 Configure auto detect for interface backup

No.	To do…	Use the command…	Remarks
1	Enter system view	<3Com> **system-view**	–
2	Enter Ethernet interface view	[3Com] **interface** *interface-type interface-number*	–
3	Reference a detect group for interface backup	[3Com-interfaceX] **standby detect-group** *group-number*	Required. This detect group must be referenced on the backup interface

Note:

- The prompt of Ethernet interface view depends on your configuration.
- For information about the parameters and the related **undo** commands, refer to the command manual.

3.5.2 Using Auto Detect with Interface Backup

I. Network requirements

- Configure dynamic routing on Routers A, B, C, and D, ensuring the routes between Routers A, B, and C are reachable, and the routes between Routers A, D, and C are reachable.
- Create a detect group numbered 10 on Router A for detecting the state of the link between Router B and Router C.
- When detect group 10 is reachable, use the main interface Serial0/0/0.
- When detect group 10 is unreachable, enable the backup interface Serial1/0/0.

II. Network diagram

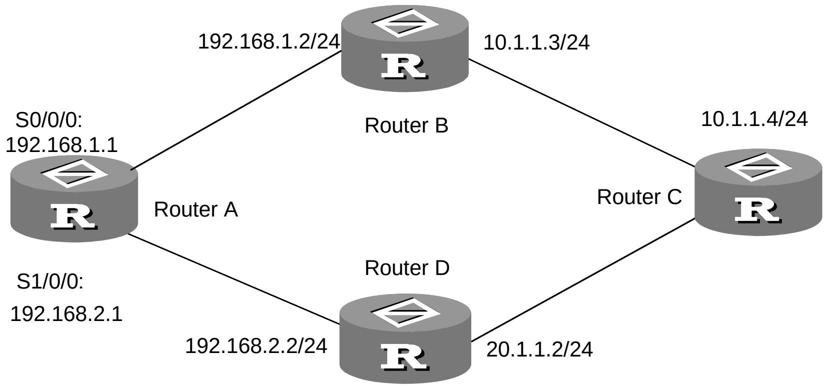


Figure 3-4 Network diagram for application of auto detect in interface backup

III. Configuration procedure

# Enter system view.

```
<3Com A> system-view
```

# Assign an IP address to Serial0/0/0.

```
[3Com A] interface serial 0/0/0
[3Com A-Serial0/0/0] ip address 192.168.1.1 24
```

# Assign an IP address to Serial1/0/0.

```
[3Com A-Serial0/0/0] interface serial 1/0/0
[3Com A-Serial1/0/0] ip address 192.168.2.1 24
[3Com A-Serial1/0/0] quit
```

# Create a detect group numbered 10.

```
[3Com A] detect-group 10
```

# Add an IP address of 10.1.1.4 with sequence number 1 to the detect group, taking 192.168.1.2 as the next hop.

```
[3Com A-detect-group-10] detect-list 1 ip address 10.1.1.4 nexthop 192.168.1.2
```

```
[3Com A-detect-group-10] quit
```

# Specify to enable Serial 1/0/0 when the detect group is unreachable.

```
[3Com A] interface serial 1/0/0
[3Com A-serial1/0/0] standby detect-group 10
```

# Configure dynamic routing. (Omitted)

Here, only the configurations on Router A are given.

Chapter 4 HWPing Configurations

4.1 Introduction to HWPing

HWPing is a tool used for testing performance of the protocols operating on a network. It is an enhancement to the ping function which can test the reachability of a host only by testing roundtrip delay with ICMP. HWPing enhances the ping function in the sense that it can detect the state (enabled or disabled) of a DLSw, DHCP, FTP, HTTP, or SNMP Server and test the response time for each type of service in addition.

You may set parameters of HWPing operations by making use of the network management software and enable HWPing to view the results of the operations. Alternatively, you may execute the **display hwping result** command to view statistics about the HWPing operations.

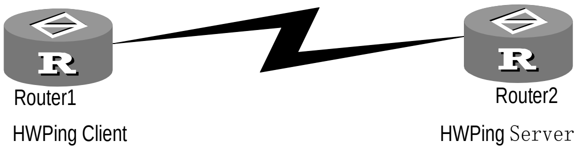


Figure 4-1 Relationship between HWPing Client and Server

4.2 HWPing Configurations

Before you use the HWPing function, you must first configure HWPing Server and HWPing Client.

Caution:

The two ends of HWPing must keep their clocks synchronized.

4.2.1 Configuring HWPing Server

Perform the following tasks to configure HWPing Server:

- Enable HWPing Server
- Configure the services to which HWPing Server listens

I. Enabling HWPing Server

Some testing operations of the HWPing function require the cooperation between Server and Client, such as jitter test (analysis on the delay variations in UDP datagram transmission) and UDP/TCP test on a specified port. HWPing Server is responsible for handling the test packets sent from HWPing Client, but it can work only if it has been enabled on the router.

You may enable both HWPing Client and Server on the same router. In other words, a router can provide both services of HWPing Server and Client.

Perform the following configurations in system view.

Table 4-1 Enable Server

Operation	Command
Enable HWPing Server.	**hwping-server enable**
Disable HWPing Server.	**undo hwping-server enable**

By default, HWPing Server is disabled.

II. Configuring the services to which HWPing Server listens

With respect to TCP or UDP HWPing test, HWPing Server responds to the test initiated by a client via the listening function. HWPing Server only responds to some particular clients, that is, the clients whose addresses and port numbers have been configured on the server.

You may create multiple TCP and UDP listening services on HWPing Server, each for a combination of destination address and port.

Perform the following configurations in system view.

Table 4-2 Configure UDP listening port

Operation	Command
Configure a UDP listening service.	**hwping-server udpecho** *ip-address port-num*
Disable the UDP listening service.	**undo hwping-server udpecho** *ip-address port-num*
Configure a TCP listening service.	**hwping-server tcpconnect** *ip-address port-num*
Disable the TCP listening service.	**undo hwping-server tcpconnect** *ip-address port-num*

By default, no UDP or TCP listening service is configured.

On the HWPing Server, a TCP listening service port cannot take a value greater than 50,000 or one reserved for special purpose, such as 1701.

On the HWPing Server, a UDP listening service port cannot take a value greater than 49,999 or one reserved for special purpose, such as 1701.

4.2.2 Configuring HWPing Client

Perform the following tasks to configure HWPing Client:

- Enable Client
- Create a test group
- Configure the allowed maximum number of concurrent test requests
- Enable trapping

I. Enabling Client

Only after the function of HWPing client has been enabled can various types of tests be set and carried out.

Perform the following configurations in system view.

Table 4-3 Enable HWPing Client

Operation	Command
Enable HWPing Client.	**hwping-agent enable**
Disable HWPing Client.	**undo hwping-agent enable**

By default, HWPing Client is disabled.

II. Creating a test group

HWPing test group is a set of HWPing test items. Each test group includes several test items and is uniquely identified by an administrator name plus an operation tag.

You may perform HWPing test after creating a test group and configuring all the parameters.

Perform the following configurations in system view.

Table 4-4 Create a test group

Operation	Command
Create a test group	**hwping** *administrator-name operation-tag*
Remove the test group.	**undo hwping** *administrator-name operation-tag*

By default, no test group is configured.

Following are the parameters included in an HWPing test group:

- Destination address
- Destination port
- Source interface
- Source address
- Source port
- Test type
- Number of packets sent for a test
- ICMP datagram size
- Packet transmission interval
- Test timeout time
- Time to Live (TTL) value
- Service type
- Packet stuffing character
- HTTP operation type
- HTTP URL
- FTP operation type
- FTP operation username
- FTP operation password
- FTP operation file name
- The maximum number of retained history records
- Test description

1) Configuring a destination address

Destination address is the IP address of HWPing Server, which is equal to the destination address in a **ping** command. It must be the IP address where TCP or UDP listening service has been configured.

Perform the following configurations in HWPing test group view.

Table 4-5 Configure a destination address

Operation	Command
Configure a destination address.	**destination-ip** *ipaddress*
Delete the destination address.	**undo destination-ip**

By default, no destination address is configured.

2) Configuring destination port

You must specify the port number of HWPing Server when making a TCP or UDP test. The port number must be the number of the port on which TCP or UDP listening service has been configured.

Perform the following configurations in HWPing test group view.

Table 4-6 Configure a destination port

Operation	Command
Configure a destination port.	**destination-port** *port-number*
Delete the destination port.	**undo destination-port**

By default, no destination port number is configured.

3) Configuring a source interface

When carrying out a DHCP test, you may specify a source interface, which must be an FE or GE interface, for sending a DHCP request. If a source interface has been specified for the DHCP test, the system will directly use it to send the DHCP request rather than determining an output interface via routing. In addition, the source IP address carried in the DHCP request will be the IP address of the specified interface.

Perform the following configurations in HWPing test group view.

Table 4-7 Bind a source interface

Operation	Command
Bind a source interface.	**source-interface** *interface-type interface-number*
Remove the source interface.	**undo source-interface**

By default, source interface is not configured.

4) Configuring source address

When carrying out a DHCP test, you may specify a source IP address for sending a DHCP request. DHCP Server will use this IP address as the destination address in the returned response packet.

Perform the following configurations in HWPing test group view.

Table 4-8 Configure a source address

Operation	Command
Configure a source address.	**source-ip** *ipaddress*
Delete the source address.	**undo source-ip**

By default, source IP address is not specified.

5) Configure a source port

When doing a DHCP test, you may specify a source port for sending a DHCP request. DHCP Server will use this port number as the destination port number in the returned response packet.

When performing an FTP test, you must specify a source port.

Perform the following configurations in HWPing test group view.

Table 4-9 Configure a source port

Operation	Command
Configure a source port.	**source-port** *port-number*
Delete the configuration of the source port.	**undo source-port**

By default, source port is not specified.

6) Configure test type

You may test various connections by using the HWPing function, but only a type at each time. In other words, a test group can serve only the HWPing test on the connection of one type.

The test types provided by HWPing include **icmp**, **udppublic**, **udpprivate**, **tcppublic**, **tcpprivate**, **dlsw**, **dhcp**, **snmpquery**, **ftp**, and **http**.

Perform the following configuration in HWPing test group view.

Table 4-10 Configure a test type

Operation	Command
Configure a test type.	**test-type** { **icmp** | **udppublic** | **udpprivate** | **tcppublic** | **tcpprivate** | **dlsw** | **dhcp** | **snmpquery** | **ftp** | **http** }

By default, test type is set to ICMP.

7) Configure the number of messages sent for a test

Suppose that the number of the messages sent for a test is greater than 1. After sending the first test message, the system sends the second one upon the receipt of the acknowledgement to the first one or upon the expiration of the test timer in the case that it has not received any acknowledgement, until it sends all the test messages as configured. The parameter discussed in this subsection is equal to the argument "**-n**" in a **ping** command.

Perform the following configurations in HWPing test group view.

Table 4-11 Configure the number of messages sent for a test

Operation	Command
Configure the number of messages sent for a test.	**count** *times*

Operation	Command
Restore the default number of messages sent for a test.	**undo count** *times*

By default, one message is sent for a test.

8) Configuring ICMP datagram size

ICMP datagram size refers to the size of the ECHO-REQUEST message transmitted for an ICMP test, excluding the IP and the ICMP headers. The argument discussed in this subsection is equal to the argument "**-s**" in a **ping** command.

Perform the following configurations in HWPing test group view.

Table 4-12 Configure an ICMP datagram size

Operation	Command
Configure an ICMP datagram size.	**datasize** *size*
Restore the default ICMP datagram size.	**undo datasize**

The *size* argument defaults to 0. Normally, you may set the size of a test packet to 56 bytes for an ICMP test, 100 bytes for an UDP test, and 28 to 100 bytes for a jitter test. The size of the packet for a jitter test can only take a value in the range 28 to 100 bytes.

9) Configuring auto-test interval

Configured with the auto-test feature, the system will automatically test the connection of a specified type at a regular interval.

Perform the following configurations in HWPing test group view.

Table 4-13 Configure auto-test interval

Operation	Command
Configure an auto-test interval.	**frequency** *interval*
Disable auto-test.	**undo frequency**

By default, auto-test interval is set to 0, i.e., only one test is performed.

10) Configuring test timeout time

Test timeout time refers to the period that the system waits for ECHO-RESPONSE after sending an ECHO-REQUEST message, upon the expiration of which the system will regard the destination unreachable. The argument discussed in this subsection is equal to the argument "**-t**" in a **ping** command, but in a different time unit.

Perform the following configurations in HWPing test group view.

Table 4-14 Configure a test timeout time

Operation	Command
Configure a test timeout time.	**timeout** *time*
Restore the default setting of test timeout time.	**undo timeout**

By default, test timeout time is set to three seconds.

11) Configuring TTL

The configured TTL refers to the TTL of test messages. It is equal to the argument "**-h**" in a **ping** command.

Perform the following configurations in HWPing test group view.

Table 4-15 Configure a TTL value

Operation	Command
Configure a TTL value.	**ttl** *number*
Remove the configured TTL.	**undo ttl**

By default, TTL is decided by the transmission attributes of the router.

🕮 **Note:**

The **sendpacket passroute** command voids the **ttl** command.

12) Configure service type

Service type is set in the ToS field of IP header. It is equal to the argument "**-o**" in a **ping** command.

Perform the following configurations in HWPing test group view.

Table 4-16 Configure ToS

Operation	Command
Set the ToS field.	**tos** *value*
Restore the default ToS setting.	**undo tos**

By default, ToS is set to 0.

13) Configuring a datagram stuffing character string

In ICMP test, the system should stuff the data field of each transmitted ICMP message. If the size of a test datagram is smaller than that of the configured stuffing character string, only a portion of the string will be used for stuffing. If the size of the test datagram is larger, the string will be used cyclically for stuffing. Suppose a stuffing string, “abcd”, is configured. If the test datagram size is 3, only “abc” will be used for stuffing; if it is 6, the string “abcdab" will be used.

Perform the following configurations in HWPing test group view.

Table 4-17 Configure datagram stuffing character string

Operation	Command
Configure a stuffing character string.	**datafill** *string*
Remove the stuffing character string.	**undo datafill**

By default, the numbers between 0 and 255 are stuffed into datagrams in a cyclically way.

14) Configuring HTTP operations type

You may configure the type of operations that HWPing Client performs in the HTTP interaction with HWPing Server.

You can perform this configuration task only for an HTTP test.

Perform the following configuration in HWPing test group view.

Table 4-18 Configure an HTTP operations type

Operation	Command
Configure an HTTP operation type.	**http-operation** { **get** | **post** }

By default, operations type is set to **get**.

15) Configuring FTP operations type

You may configure the type of operations that HWPing Client performs in the FTP interaction with HWPing Server.

You can perform this configuration task only for an FTP test.

Perform the following configuration in HWPing test group view.

Table 4-19 Configure an FTP operations type

Operation	Command
Configure an FTP operations type	**ftp-operation** { **get** | **put** }

By default, FTP operations type is **get**.

16) Configuring username and password used in FTP operations

You must provide the proper username and password before you perform FTP operations.

This configuration task can be performed only in an FTP test.

Perform the following configurations in HWPing test group view.

Table 4-20 Configure username and password for FTP operations

Operation	Command
Configure a username.	**username** *name*
Remove the username.	**undo username**
Configure a password.	**password** *password*
Remove the password.	**undo password**

By default, no username or password is configured.

17) Configuring name of the file on which FTP operations are performed

This configuration task is used for specifying name of the file at the server end, on which FTP operations will be performed.

This configuration task can be performed only in an FTP test.

Perform the following configurations in HWPing test group view.

Table 4-21 Configure name of the file on which FTP operations will be performed

Operation	Command
Configure a file name.	**filename** *file-name*
Remove the file name.	**undo filename**

By default, no file name is configured.

18) Configuring the number of test packets sent for a jitter test

Jitter test is carried out for analyzing delay variations in UDP packet transmission. In the test, the source end sends some datagrams at a regular interval (which is configurable), upon the receipt of which the destination end stamps and return them to the source end. The source end can thus work out the jitter delay with these datagrams carrying timestamps. For this purpose, multiple test packets must be sent for each test. The analysis result of a test is in direct proportion to the sent test packets. Naturally, the more the test packets are sent, the longer the test duration will be.

This configuration task can be performed only in a jitter test.

Perform the following configurations in HWPing test group view.

Table 4-22 Configure the number of packets sent for a jitter test

Operation	Command
Configure the number of packets sent for a jitter test.	**jitter-packetnum** *number*
Restore the default setting.	**undo jitter-packetnum**

By default, 20 packets are sent for each jitter test.

19) Configuring the packet transmission interval in a jitter test

You may configure a packet transmission interval in a jitter test. A smaller transmission interval means a faster testing speed. If the interval is set too small, however, there will be some impact on the network.

This configuration task can be performed only in a jitter test.

Perform the following configurations in HWPing test group view.

Table 4-23 Configure packet transmission interval in a jitter test

Operation	Command
Configure packet transmission interval for a jitter test.	**jitter-interval** *interval*
Restore the default setting.	**undo jitter-interval**

By default, packets are sent at an interval of 20 milliseconds in a jitter test.

20) Configuring the maximum number of retained history records

You may specify the maximum number of history records that may be retained for a test group. The system will discard the earlier test results if the number of records to be retained is greater than the specified one.

Perform the following configurations in HWPing test group view.

Table 4-24 Configure the maximum number of retained history records

Operation	Command
Configure the maximum number of retained history records.	**history-records** *number*
Restore the default setting.	**undo history-records**

By default, up to 50 history records can be retained for a test group.

21) Configuring routing table bypass

With routing table bypass, a remote host can bypass the normal routing tables and send ICMP packets directly to a host on an attached network. If the host is not on a directly-attached network, an error is returned. You can use this function when pinging a local host on an interface that has no route defined.

Table 4-25 Configure routing table bypass

Operation	Command
Enable routing table bypass.	**sendpacket passroute**
Disable routing table bypass.	**undo sendpacket passroute**

By default, routing table bypass is disabled.

22) Configuring VPN instance information

Perform the following configuration in HWPing test group view.

Table 4-26 Configure VPN instance information

Operation	Command
Configure VPN instance information	**vpninstance** *name*
Remove VPN instance information	**undo vpninstance**

By default, no VPN instance information is configured.

This command applies to all tests except for DHCP test.

23) Configuring test group description

You may make a simple description on a test group, usually from the aspects of its test items or test purpose.

Perform the following configurations in HWPing test group view.

Table 4-27 Configure test group description

Operation	Command
Configure a test description.	**description** *string*
Remove the test description.	**undo description**

By default, no description information is configured.

24) Configuring trapping

An HWPing test generates trap information regardless of whether it fails or succeeds. You may configure to send or not to send the trap information to the NMS by making use of the following command and its **undo** form.

You can configure HWPing test as well as the number of consecutive probe failures for the system to send a trap for the test.

If send-trap is enabled, a trap is sent for each probe or test failure.

Perform the following configurations in HWPing test group view.

Table 4-28 Enable/disable trap-sending

Operation	Command
Enable trap sending.	**send-trap** { **all** | **probefailure** | **testcomplete** | **testfailure** }
Disable trap sending.	**undo send-trap** { **all** | **probefailure** | **testcomplete** | **testfailure** }
Configure the number of consecutive test failures for HWPing test to send a trap.	**test-failtimes** *times*
Configure the number of consecutive probe failures for HWPing test to send a trap.	**probe-failtimes** *times*

By default, the system does not send trap information to the NMS.

III. Configuring the maximum number of concurrent tests

You may use the command in this subsection to set the maximum number of concurrent tests allowed on a router (HWPing Client). Setting it to 0 means there is no limit.

Perform the following configurations in system view.

Table 4-29 Configure the maximum number of concurrent tests

Operation	Command
Set the maximum number of concurrent tests.	**hwping-agent max-requests** *number*
Restore the default maximum number of concurrent tests.	**undo hwping-agent max-requests** *number*

By default, five concurrent tests are allowed.

4.3 Executing Test

After creating a test group and configuring the required test parameters, you may perform an HWPing test in the test group by executing the **test-enable** command.

Perform the following configuration in HWPing test group view.

Table 4-30 Test

Operation	Command
Execute test.	**test-enable**

📖 **Note:**

After you execute the **test-enable** command, the system does not display the test result. You may view the test result information by executing the **display hwping** command.

4.4 Displaying Test Information

You may view the test history, jitter test information, and the last test information respectively by executing the commands **display hwping history**, **display hwping jitter**, and **display hwping result**.

The history information includes the result that the system retains for each test. The number of records can be set by using the **history-records** command.

Jitter information includes the delay variations in UDP packet transmission that are recorded in a jitter test, and only the information of the last jitter test will be retained. The results of HWPing tests of other types do not include jitter information.

Perform the following operations in any view.

Table 4-31 Display the test information

Operation	Command
Display the test information	**display hwping** { **history** | **jitter** | **result** } [*administrator-name operation-tag*]

4.5 Typical HWPing Configuration Example

4.5.1 ICMP Test

I. Introduction

Like ping test, ICMP test in HWPing determines the roundtrip delay of a packet by making use of ICMP.

II. Configuration procedure

📖 **Note:**

Steps 1 through 3 and 6 are required for an ICMP test and the remaining three steps are optional.

# Enable HWPing Client.

```
[router] hwping-agent enable
```

# Step 1: Create an HWPing test group, given an administrator name “administrator” and a test operations tag “icmp”.

```
[router] hwping administrator icmp
```

# Step 2: Set the test type to ICMP.

```
[router-hwping-administrator-icmp] test-type icmp
```

# Step 3: Configure a destination IP address 169.254.10.2.

```
[router-hwping-administrator-icmp] destination-ip 169.254.10.2
```

# Step 4: Configure the number of test messages

```
[router-hwping-administrator-icmp] count 10
```

# Step 5: Configure the timeout time.

```
[router-hwping-administrator-icmp] timeout 3
```

# Step 6: Enable a test.

```
[router-hwping-administrator-icmp] test-enable
```

# Step 7: View the test result.

```
[router-hwping-administrator-icmp] display hwping result administrator icmp
[router-hwping-administrator-icmp] display hwping history administrator icmp
```

4.5.2 DHCP Test

I. Introduction

DHCP test is used for testing the time required for obtaining an IP address from a DHCP Server.

II. Configuration procedure

Note:

Steps 1 through 3 and 6 are required for a DHCP test and the remaining three steps are optional.

# Enable HWPing Client.

```
[router] hwping-agent enable
```

# Step 1: Create an HWPing test group, given an administrator name “administrator” and a test operations tag “dhcp”.

```
[router] Hwping administrator dhcp
```

# Step 2: Set the test type to DHCP.

```
[router-hwping-administrator-dhcp] test-type dhcp
```

# Step 3: Configure a source interface. This interface must be an Ethernet interface and the tested DHCP Server must locate on the network attached to the interface.

```
[router-hwping-administrator-dhcp] source-interface ethernet1/0/0
```

# Step 4: Configure the maximum number of tests.

```
[router-hwping-administrator-dhcp] count 10
```

# Step 5: Configure a test timeout time.

```
[router-hwping-administrator-dhcp] timeout 3
```

# Step 6: Enable a test.

```
[router-hwping-administrator-dhcp] test-enable
```

# Step 7: View the test result.

```
[router-hwping-administrator-dhcp] display hwping result administrator dhcp
[router-hwping-administrator-dhcp] display hwping history administrator dhcp
```

4.5.3 DLSw Test

I. Introduction

DLSw test is used for testing the response time of a DLSw device.

II. Configuration procedure

Note:

Steps 1 through 3 and 6 are required for a DLSw test and the remaining three steps are optional. In addition, on the destination router specified in Step 3, the DLSw function must have been enabled using the **dlsw enable** command and the appropriate DLSw pair must have been created using the commands **dlsw local** and **dlsw remote**. For more information about that, see the part concerning DLSw configurations in *V 2.41 Operation Manual – Link Layer Protocol*.

# Enable HWPing Client.

```
[router] hwping-agent enable
```

# Step 1: Create an HWPing test group, given an administrator name “administrator” and a test operations tag “dlsw”.

```
[router] Hwping administrator dlsw
```

# Step 2: Set the test type to DLSw.

```
[router-hwping-administrator- dlsw] test-type dlsw
```

# Step 3: Configure a destination address.

```
[router-hwping-administrator- dlsw] destination-ip 169.254.10.2
```

# Step 4: Configure the maximum number of tests.

```
[router-hwping-administrator- dlsw] count 10
```

# Step 5: Configure a test timeout time.

```
[router-hwping-administrator- dlsw] timeout 3
```

# Step 6: Enable a test.

```
[router-hwping-administrator- dlsw] test-enable
```

# Step 7: View the test result.

```
[router-hwping-administrator- dlsw] display hwping result administrator dlsw
[router-hwping-administrator- dlsw] display hwping history administrator dlsw
```

4.5.4 FTP Test

I. Introduction

FTP test is used for testing the time required for setting up a connection with a specified FTP server and finishing the transmission of a file over it. You may choose to get a file from the FTP server or put a file on the FTP server.

II. Configuration procedure

Note:

Steps 1 through 6 and step 9 are required for an FTP test and the remaining three steps are optional.

# Configure the IP address of the Ethernet interface.

```
[router] interface Ethernet 0/0/0
[router-Ethernet0/0/0 ] ip address 169.254.0.1 16
```

# Enable HWPing Client.

```
[router] hwping-agent enable
```

# Step 1: Create an HWPing test group, given an administrator name “administrator” and a test operations tag “ftp”.

```
[router] hwping administrator ftp
```

# Step 2: Set the test type to FTP.

```
[router-hwping-administrator-ftp] test-type ftp
```

# Step 3: Configure the IP address of an FTP server, 169.254.10.2 for example.

```
[router-hwping-administrator-ftp] destination-ip 169.254.10.2
```

# Step 4: Configure the username.

```
[router-hwping-administrator-ftp] username administrator
```

# Step 5: Configure a password.

```
[router-hwping-administrator-ftp] password hwping
```

# Step 6: Configure name of the file to be gotten.

```
[router-hwping-administrator-ftp] filename config.txt
```

# Step 7: Configure the maximum number of tests.

```
[router-hwping-administrator-ftp] count 10
```

# Step 8: Configure a test timeout time.

```
[router-hwping-administrator-ftp] timeout 30
```

# Step 9: Configure the source address.

```
[router-hwping-administrator-ftp] source-ip 169.354.0.1
```

# Step 10: Enable a test.

```
[router-hwping-administrator-ftp] test-enable
```

# Step 11: View the test result.

```
[router-hwping-administrator-ftp] display hwping result administrator ftp
[router-hwping-administrator-ftp] display hwping history administrator ftp
```

At the opposite end, you only need to enable FTP Server and configure the corresponding user.

4.5.5 HTTP Test

I. Introduction

HTTP test is used for testing the time required for setting up a connection with a specified HTTP server and obtaining a file from it over the connection.

II. Configuration procedure

Note:

Steps 1 through 3 described in this example are required for an HTTP test and the remaining steps are optional.

# Enable HWPing Client.

```
[router] hwping-agent enable
```

# Step 1: Create an HWPing test group, given an administrator name "administrator" and a test operations tag "http".

```
[router] Hwping administrator http
```

# Step 2: Set the test type to HTTP.

```
[router-hwping-administrator-http] test-type http
```

# Step 3: Configure the IP address of an HTTP server, 169.254.10.2 for example.

```
[router-hwping-administrator-http] destination-ip 169.254.10.2
```

# Step 4: Configure the maximum number of tests.

```
[router-hwping-administrator-http] count 10
```

# Step 5: Configure a test timeout time.

```
[router-hwping-administrator-http] timeout 30
```

# Step 6: Enable a test.

```
[router-hwping-administrator-http] test-enable
```

# Step 7: View the test result.

```
[router-hwping-administrator-http] display hwping result administrator http
[router-hwping-administrator-http] display hwping history administrator http
```

4.5.6 Jitter Test

I. Introduction

Jitter test is performed to test the jitter delay in UDP packet transmission between the local end (HWPing Client) and a specified destination (HWPing Server).

II. Configuration procedure

🕮 **Note:**

Steps 1 through 4 and 8 are required for a jitter test and the remaining three steps are optional. These operations are performed on the HWPing Client.

# Enable HWPing Client.

```
[router] hwping-agent enable
```

# Step 1: Create an HWPing test group, given an administrator name “administrator” and a test operations tag “jitter”.

```
[router] Hwping administrator jitter
```

# Step 2: Set the test type to jitter.

```
[router-hwping-administrator-jitter] test-type jitter
```

# Step 3: Configure the IP address of an HWPing server, 169.254.10.2 for example.

```
[router-hwping-administrator-jitter] destination-ip 169.254.10.2
```

# Step 4: Configure the destination port.

```
[router-hwping-administrator-jitter] destination-port 9000
```

# Step 5: Configure the maximum number of tests.

```
[router-hwping-administrator-jitter] count 10
```

# Step 6: Configure a test timeout time.

```
[router-hwping-administrator-jitter] timeout 30
```

# Step 7: Enable a test.

```
[router-hwping-administrator-jitter] test-enable
```

# Step 8: View the test result.

```
[router-hwping-administrator-jitter]  display  hwping  result  administrator
jitter
[router-hwping-administrator-jitter]  display  hwping  history  administrator
jitter
[router-hwping-administrator-jitter]  display  hwping  jitter  administrator
jitter
```

⚠ **Caution:**

At the destination end, you must perform the following configurations:

```
[router] hwping-server enable
[router] hwping-server udpecho 169.254.10.2 9000
```

The address and port number configured using the **hwping-server udpecho** command on the HWPing server for handling UDP test packets must be the same IP address and port number configured in steps 3 and 4 described above.

4.5.7 SNMP Test

I. Introduction

SNMP test is performed to test the duration between the transmission of an SNMP query and the receipt of the acknowledgement.

II. Configuration procedure

🕮 **Note:**

Steps 1 through 3 and 6 are required for an SNMP test and the remaining three steps are optional. These operations are performed on the HWPing Client.

# Enable SNMP Client.

```
[router ] snmp-agent trap enable
```

# Enable HWPing Client.

```
[router] hwping-agent enable
```

# Step 1: Create an HWPing test group, given an administrator name “administrator” and a test operations tag “snmp”.

```
[router] Hwping administrator snmp
```

# Step 2: Set the test type to SNMP.

```
[router-hwping-administrator-snmp] test-type snmpquery
```

# Step 3: Configure a destination IP address, 169.254.10.2 for example.

```
[router-hwping-administrator-snmp] destination-ip 169.254.10.2
```

# Step 4: Configure the maximum number of tests.

```
[router-hwping-administrator-snmp] count 10
```

# Step 5: Configure a test timeout time.

```
[router-hwping-administrator-snmp] timeout 30
```

# Step 6: Enable a test.

```
[router-hwping-administrator-snmp] test-enable
```

# Step 7: View the test result.

```
[router] display hwping result administrator snmp
[router] display hwping history administrator snmp
```

⚠ **Caution:**

You must enable the network management function on the device specified by the destination address configured in Step 3; otherwise, it will be unable to make response. If that device is 3Com’s router, you may enable the network management function on it using the **snmp-agent** command. For more information about that, see the part concerning SNMP configuration in this manual.

4.5.8 TCP Test of a Specified Port

I. Introduction

TCP test on a specified port is performed to test the time required for setting up a TCP connection between the local end and a specified destination.

II. Configuration procedure

🕮 **Note:**

Steps 1 through 4 and 7 are required for a TCP test and the remaining three steps are optional.

# Enable HWPing Client.

```
[router] hwping-agent enable
```

# Step 1: Create an HWPing test group, setting the administrator name to administrator and test operation tag to tcpprivate.

```
[router] Hwping administrator tcpprivate
```

# Step 2: Set the test type to TCP-private.

```
[router-hwping-administrator-tcpprivate] test-type tcpprivate
```

# Step 3: Configure the IP address of an HWPing server, 169.254.10.2 for example.

```
[router-hwping-administrator- tcpprivate] destination-ip 169.254.10.2
```

# Step 4: Configure a destination port.

```
[router-hwping-administrator- tcpprivate] destination-port 9000
```

# Step 5: Configure the number of transmitted test packets.

```
[router-hwping-administrator- tcpprivate] count 10
```

# Step 6: Configure a test timeout time.

```
[router-hwping-administrator- tcpprivate] timeout 3
```

# Step 7: Enable a test.

```
[router-hwping-administrator- tcpprivate] test-enable
```

# Step 8: View the test result.

```
[router] display hwping result administrator tcpprivate
[router] display hwping history administrator tcpprivate
```

⚠ **Caution:**

At the destination end, you must enable HWPing Server and create an HWPing TCP listening service by making the following configurations:

```
[router] hwping-server enable
[router] hwping-server tcpconnect 169.254.10.2 9000
```

The address and port number configured using the **hwping-server tcpconnect** command on the HWPing server must be the same IP address and port number configured in steps 3 and 4 described above.

4.5.9 UDP Test of a Specified Port

I. Introduction

UDP test on a specified port is performed to test the roundtrip time of a UDP packet.

II. Configuration procedure

🕮 **Note:**

Steps 1 through 4 and 7 are required for a UDP test and the remaining three steps are optional.

# Enable HWPing Client.

```
[router] hwping-agent enable
```

# Step 1: Create an HWPing test group, setting administrator name to administrator and test operation tag to udpprivate.

```
[router] Hwping administrator udpprivate
```

# Step 2: Set the test type to UDP-private.

```
[router-hwping-administrator-udpprivate] test-type udpprivate
```

# Step 3: Configure the IP address of an HWPing server, 169.254.10.2 for example.

```
[router-hwping-administrator-udpprivate] destination-ip 169.254.10.2
```

# Step 4: Configure a destination port.

```
[router-hwping-administrator-udpprivate] destination-port 9000
```

# Step 5: Configure the number of transmitted test packets.

```
[router-hwping-administrator-udpprivate] count 10
```

# Step 6: Configure a test timeout time.

```
[router-hwping-administrator-udpprivate] timeout 3
```

# Step 7: Enable a test.

```
[router-hwping-administrator-udpprivate] test-enable
```

# Step 8: View the test result.

```
[router] display hwping result administrator udpprivate
[router] display hwping history administrator udpprivate
```

⚠ **Caution:**

At the destination end, you must perform the following configurations:

```
[router] hwping-server enable
[router] hwping-server udpecho 169.254.10.2 9000
```

The address and port number configured using the **hwping-server udpecho** command on the HWPing server must be the same IP address and port number configured in steps 3 and 4 described above.

Chapter 5 File Management

5.1 File System

5.1.1 Brief Introduction

The major function of the file system is to manage storage devices and store files in these devices. Currently, the storage devices supported by the router includes Flash and hard disk.

The file system manages files and directories, such as to establish the file system, to establish, delete, modify, rename a file and a directory, and to display the contents of a file. All these operations are only performed in the user view. Please notice that a full file name can support up to 64 bytes and the ultra-long file name will make you unable to perform the file operations normally.

5.1.2 Directory Operations

The file system can establish and delete a directory and display the current working directory, and display the files or directories in a specified directory.

Perform the following operations in the user view.

Table 5-1 Directory operations

Operation	Command
Make a directory	**mkdir** *directory*
Remove a directory	**rmdir** *directory*
Print the current working directory	**pwd**
Display the files or directories	**dir** [**/all** | */h*] [*file-url*]
Change the current directory	**cd** *directory*

5.1.3 File Operations

The file system can delete a file (dump into the recycle bin), restore a deleted file, delete a file or files in the recycle bin, display the contents of a file, rename a file, copy a file, move a file, execute the batch file, display the information of specified files (even including private files) , as displayed in Table 5-2.

I. Basic operations

Perform the following operations in the user view, (and the **execute** command is performed in system view).

Table 5-2 File operations

Operation	Command
Delete a file	**delete** [/**unreserved**] *file-url*
Restore a deleted file	**undelete** *file-url*
Empty the recycle bin	**reset recycle-bin** [*filename*] [*flash:/*] [**/force**]
Display the contents of a file	**more** *file-url*
Rename a file	**rename** *fileurl-source fileurl-dest*
Copy a file	**copy** *fileurl-source fileurl-dest*
Move a file	**move** *fileurl-source fileurl-dest*
Display files or directories	**dir** [/**all** | /*h*] [*file-url*]
Execute the batch file	**execute** *filename*

II. Configuring the dual image function

On a router installed with a Flash larger than 8 MB, you can load the software version that can provide the dual image function. In this case, three boot files are defined in the system by default: main boot file, backup boot file, and secure boot file. If they are loaded into the Flash, the system uses them in order to boot the router as follows:

- Main boot file, with the default name being main.bin and file type being M, is the default file for system boot;
- Backup boot file, with the default name being backup.bin and file type being B, is the boot file used in case of the boot failure using the main boot file;
- Secure boot file, with the default name being secure.bin and file type being S, is the boot file used in case of the boot failure using the backup boot file. If the boot attempts using all these files fail, the system prompts the boot failure.

You can use the commands in the following table to view files in the Flash and specify the main and backup boot files.

Perform the following operations in system view.

Table 5-3 Display files and select main/backup boot file

Operation	Command
Display all the boot files in the Flash.	**bootfile dir**
Specify the main boot file used when booting the router.	**bootfile main** *main-bootfile-name*
Specify the backup boot file used when booting the router.	**bootfile backup** *backup-bootfile-name*

🕮 **Note:**

Secure boot file is the last system boot resort. You can download it in the Boot ROM menu and must name it secure.bin. However, you cannot modify this file or change the type of another file to S. If you change the name of the secure boot file with the **rename** command after the system boots, no secure boot file exists in Flash memory. To use the secure boot file after that, you need to download it again.

You can also perform these operations in the Boot ROM menu, with reference to the *Installation Manual* accompanying the device you work with.

5.1.4 Storage Device Operation

The file system can format a specified storage device.

Perform the following operations in the user view.

Table 5-4 Storage device operation

Operation	Command
Format a storage device	**format** *device-name*

5.1.5 File System Prompt Mode

The user can use the command to modify the prompt mode of the current file system.

Perform the following configuration in system view.

Table 5-5 Set the prompt mode of the file system

Operation	Command
Set the prompt mode of the current file system.	**file prompt** { **alert** | **quiet** }

5.1.6 Restoring the Space of a Storage Device

Perform the following configuration in user view.

Table 5-6 Restore the space of a storage device

Operation	Command
Restore the space of a storage device when it becomes unavailable because of some abnormal operation	**fixdisk** *device-name*

5.1.7 Example for the File System Usage

# Display the current files under root directory and the test directory.

```
<3Com> dir
Directory of *
   0   -rw-   2145123  Jul 12 2001 12:28:08   AR46.bin
   1   -rw-       595   Jul 12 2001 10:47:50   v 2.41cfg.txt
   2   drw-          0  Jul 12 2001 19:41:20   test
6477 KBytes total (2144 KBytes free)
<3Com> dir flash:/test/
Directory of flash:/test/
   0   drw-         -  Jul 12 2001 20:23:37   subdir
   1   -rw-       595  Jul 12 2001 20:13:19   v 2.41cfg.txt
   2   -rw-        50  Jul 12 2001 20:08:32   sample.txt
6477 KBytes total (2144 KBytes free)
```

# Move the file from flash:/test/sample.txt to flash:/sample.txt.

```
<3Com> move flash:/test/sample.txt flash:/sample.txt
Move flash:/test/sample.txt to flash:/sample.txt ?[Y/N]:y
% Moveded file flash:/test/sample.txt flash:/sample.txt
```

# Display the current information after moving the file.

```
<3Com> dir
Directory of *
   0   -rw-   2145123  Jul 12 2001 12:28:08   ne80.bin
   1   -rw-       595   Jul 12 2001 10:47:50   v 2.41cfg.txt
   2   drw-         0   Jul 12 2001 19:41:20   test
   3   -rw-        50   Jul 12 2001 20:26:48   sample.txt
6477 KBytes total (2144 KBytes free)
<3Com> dir flash:/test/
Directory of flash:/test/
   0   drw-             Jul 12 2001 20:23:37   subdir
   1   -rw-       595   Jul 12 2001 20:13:19   v 2.41cfg.txt
```

```
6477 KBytes total (2144 KBytes free)
```

5.2 File System Checking Configuration

5.2.1 Introduction

At present, file system checking only checks for/handles corrupted files instead of the entire Flash. After you enable file system checking, the system scans all files, checks files that are reported to be zero byte in size by the **dir** command but actually are not, and handles these files in the following ways:

- Checking for corrupted files
- Fixing corrupted files
- Discarding the contents of corrupted files
- Recycling storage space automatically

The settings of file fixing, file discarding, and storage space recycling remain valid during the course of file system self-test when the system restarts.

5.2.2 Configuring File System Checking

Table 5-7 Configuring file system checking

No.	To do…	Use the command…	Remarks
1	Enter system view	<3Com> **system-view**	–
2	Specify automatic file fixing to be the file system checking method	[3Com] **vfs check check-method fix**	Optional. The automatic file fixing method is the default file system checking method.
3	Specify discarding the contents of the corrupted files to be the file system checking method	**vfs check check-method discard**	
4	Specify discarding the contents of the corrupted files and recycling the corresponding storage space to be the file system checking method	**vfs check check-method discard auto**	
5	Quit to system view	**quit**	–
6	Check the file system	**vfs check file-system**	

Note:

Versatile file system (VFS) is used to manage storage devices in V 2.41. Note that the **vfs check check-method fix** and **vfs check check-method discard/vfs check check-method discard auto** command are mutually exclusive. That is, configuring the former invalidates the later, and configuring either of the later invalidates the former.

The **vfs check check-method discard** command only discards the contents of the corrupted files. It does not recycle the corresponding storage space. To recycle storage space, use the **fixdisk** command.

The **vfs check check-method discard auto** command only discards the contents of corrupted files and recycles the corresponding storage space. It does not delete corrupted files. To delete a corrupted file, use the **delete** command.

When a router starts, the file checking during the course of self-test is performed in the latest file checking way set by users.

5.2.3 File System Checking Configuration Example

I. Requirements

Delete corrupted files and recycle the corresponding storage space.

II. Configuration procedure

```
<3Com> system-view
System View: return to User View with Ctrl+Z.
[3Com] vfs check check-method discard auto
 VFS: The space will be take back automatically after discard.
[3Com] quit
<3Com> vfs check file-system
 Checking file system, please wait...
 Check file system complete.
```

5.3 FTP Configuration

5.3.1 Brief Introduction

FTP is an application layer protocol in the TCP/IP protocol suite and provides users with file transfer services between different hosts. The implementation of FTP relies on the special file system on which it runs.

FTP services provided by a router include:

- FTP Server service, that is, the user can run the FTP client program to log on to the router to access the files in the router.

- FTP Client service, that is, the user can directly input the **ftp** command in the user view to establish a connection with a remote FTP Server to access the files in the remote host.

FTP Server Configuration includes:

- Start up the FTP server
- Configure the authentication and authorization of the FTP server
- Configure operating parameters of the FTP server
- Display and debug the FTP server

5.3.2 Startup

Only after the FTP server function is enabled can the FTP client log into the server and access the files on the router.

Perform the following operations in the system view.

Table 5-8 Start up the FTP server

Operation	Command
Start up the FTP server	**ftp server enable**
Shut down the FTP server	**undo ftp server**

The FTP server can support multiple user accesses simultaneously. When a remote FTP user sends a request to the FTP server, the server will execute corresponding actions and return the results of the execution to the user.

5.3.3 Configuring Authentication and Authorization

The authorizing information of the FTP server includes the operating directory provided for the FTP user. Only those who have passed the authentication and been authorized successfully can gain the service of the FTP server. Before a user can use the FTP service, you must configure the user type and FTP operating directory on the router.

Table 5-9 Configure the authentication and authorization

Operation	Command
Create a local FTP user and enter the corresponding view (in system view)	**local-user** *user-name*
Delete a specified local user	**undo local-user** { *user-name* **|** **all** }
Configure the password of the FTP user (in local user view)	**password** [**cipher** **|** **simple**] *password*
Cancel the password of the FTP user (in local user view)	**undo password**

Operation	Command
Configure the authorization information of the FTP user (in local user view)	**service-type ftp** [**ftp-directory** *directory*]
Disable FTP service	**undo service-type ftp**
Restore the default directory authorized to FTP users	**undo service-type ftp ftp-directory**

The following is an example of configuring the authentication and authorization of the FTP server.

# Configure authentication and information of FTP users.

```
[3Com] local-user 3Com
[3Com-luser-3Com] password simple 3Com
[3Com-luser-3Com] service-type ftp ftp-directory flash:/ftp/3Com
```

5.3.4 Configuring Operating Parameters of FTP Server

I. Configuring the upgrading mode with FTP server

The FTP server updates the data of files in its Flash memory in two modes: normal and fast, when receiving files transferred by the user using the FTP command **put**. Each of two modes is demonstrated respectively as follows:

Fast mode: The FTP server writes the data to the Flash memory after the completion of the file transfer. This can safeguard that the files in the Flash memory of the Router will not be damaged even on abnormal occasions such as power failure.

Normal mode: The FTP server writes the data to the Flash memory during the file transfer. This means that the occurrence of some abnormal conditions such as power failure might cause the damage of the files in the Flash memory of the Router. But the normal updating mode consumes less memory.

Perform the following operations in the system view.

Table 5-10 Configure the update of the FTP server

Operation	Command
Configure the update of the FTP server	**ftp update** { **fast** | **normal** }
Restore the update of the FTP server to the default value	**undo ftp update** { **fast** | **normal** }

The updating mode of FTP server defaults to **fast**.

II. Configuring idle-timeout disconnection of FTP

To prevent illegal accesses, the connection with an FTP client will be disconnected if no service request from the client has been received for a certain period.

Perform the following configuration in the system view.

Table 5-11 Configure the timeout of the FTP server

Operation	Command
Configure the timeout time of the FTP server.	**ftp timeout** *minutes*
Restore the timeout time of the FTP server to the default value.	**undo ftp timeout**

The default idle-timeout time is 30 minutes.

III. Specifying a source interface/IP address for the FTP server

Perform the following configuration in system view.

Table 5-12 Specify a source interface or source IP address for the FTP server

Operation	Command
Specify a source interface for the FTP server	**ftp-server source-interface** *interface-type interface-number*
Delete the source interface specified for the FTP server	**undo ftp-server source-interface**
Specify a source IP address for the packets sent by the FTP server	**ftp-server source-ip** *ip-address*
Delete the source IP address specified for the FTP server	**undo ftp-server source-ip**

By default, the source IP address in each packet sent by the FTP server is the IP address of the interface where the packet is sent out.

🕮 **Note:**

You may specify a source IP address for the packets sent by the FTP server with the **ftp-server source-interface** command or with the **ftp-server source-ip** command. If both commands are configured, the one configured later overrides the former.

5.3.5 Displaying and Debugging

After the above configuration, execute the **display** command in any view to display the running of the FTP server after configuration, and to verify the configuration.

Table 5-13 Commands for monitoring and maintaining the FTP server

Operation	Command
Display the FTP server	**display ftp-server**
Display the current source IP address of the FTP server	**display ftp-server source-ip**
Display logon FTP users	**display ftp-user**

The **display ftp-server** command will display the configuration of the current FTP server, including maximum number of users that the server can support and timeout. The **display ftp-user** command will display the specific information of logon FTP users.

5.3.6 Introduction to FTP Client

FTP Client is an additional function offered to users. It allows your router to operate as an FTP client to connect to an FTP server and to perform operations with FTP client commands. At present, only one FTP client is supported.

I. Operation commands available with the FTP client

The commands available the FTP client include operations such as creating FTP connections and creating/deleting directories. For the use of specific commands, refer to the section of "FTP client command" in *V 2.41 Command Manual.*

II. Specifying a source interface/IP address for the FTP client

Perform the following configuration in system view.

Table 5-14 Specify a source interface or source IP address for the FTP client

Operation	Command
Specify a source interface for the FTP client	**ftp source-interface** *interface-type interface-number*
Delete the source interface specified for the FTP client	**undo ftp source-interface**
Specify a source IP address for the packets sent by the FTP client	**ftp source-ip** *ip-address*
Delete the source IP address specified for the FTP client	**undo ftp source-ip**

By default, the source IP address in each packet sent by the FTP server is the IP address of the interface where the packet is sent out.

Note:

You may specify a source IP address for the packets sent by the FTP server with the **ftp source-interface** command or with the **ftp source-ip** command. If both commands are configured, the one configured later overrides the former.

5.3.7 Configuration Example 1: Upgrading the V 2.41 Application Program with FTP

I. Network requirements

Upgrade V 2.41 main software through FTP, with the router being the client. IP address of the FTP server is 172.16.104.110; FTP username is 8040 and its password is 3Com.

II. Network diagram

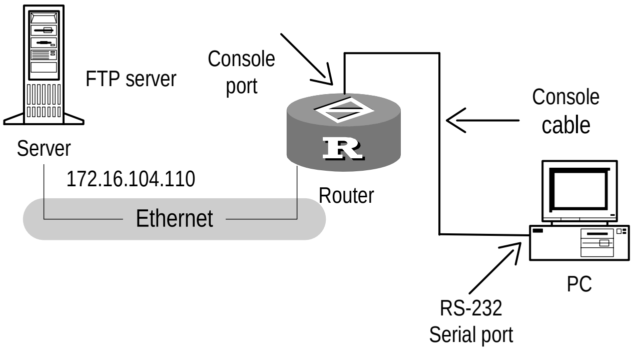


Figure 5-1 Smooth upgrade through FTP client

III. Configuration procedure

Follow these steps to upgrade V 2.41 main software through FTP:

# (Prompt) Delete the redundant files in the memory device on the router to allow enough space for storing new system files.

```
<3Com> dir
Directory of flash:/

   0   -rw-   5709691  Jul 16 2004 16:17:30   secure.bin
   1   -rw-       939  Nov 29 2004 15:08:44   v 2.41cfg.cfg
   2   -rw-   8985472  Dec 19 2004 14:52:08   main.bin
   3   -rw-       969  Oct 29 2004 16:10:20   sip.cfg
   4   -rw-    524288  Nov 08 2004 14:32:41   bootromfull
31877 KB total (17007 KB free)
```

```
<3Com> delete sip.cfg
```

# Log into the FTP server, get the main software of the system and store it in the root directory of the memory device on the router.

# The obtained system file must be stored in the root directory of the router memory device, that is, flash:, and named main.bin.

```
<3Com> ftp 172.16.104.110
Trying 172.16.104.110 ...
Connected to 172.16.104.110.
220 WFTPD 2.0 service (by Texas Imperial Software) ready for new user
User(172.16.104.110:(none)):8040
331 Give me your password, please
Password:xxxxxxx
230 Logged in successfully
[ftp] binary
[ftp] get v 2.413.cc main.bin
200 PORT command okay
150 "D:\8040\system\v 2.413.cc" file ready to send (58051
00 bytes) in IMAGE / Binary mode
226 Transfer finished successfully.
FTP: 5805100 byte(s) received in 19.898 second(s) 291.74Kbyte(s)/sec.
[ftp] bye
Reboot the router to run the upgraded program after the upgrade is completed.
```

5.3.8 Configuration Example 2: Upgrading the V 2.41 Application Program with FTP

I. Network requirements

Upgrade V 2.41 main software through FTP, with the router being the server. IP address of the Ethernet interface on the router is 172.16.104.110; FTP username is 8040 and its password is 3Com.

II. Network diagram

See Figure 5-1.

III. Configuration procedure

1) Configure the router

# Add an authorized FTP username and password.

```
[3Com ] local-user 8040
[3Com-luser-8040] password simple 3Com
[3Com-luser-8040] service-type ftp
[3Com-luser-8040] ftp-directory flash:/ftp/3Com
```

# Enable FTP server.

```
[3Com ] ftp server enable
```

# (Prompt) Delete the redundant files in the memory device on the router to allow enough space for storing new system files.

```
<3Com> dir
Directory of flash:/

   0   -rw-   5709691  Jul 16 2004 16:17:30   secure.bin
   1   -rw-       939  Nov 29 2004 15:08:44   v 2.41cfg.cfg
   2   -rw-   8985472  Dec 19 2004 14:52:08   main.bin
   3   -rw-       969  Oct 29 2004 16:10:20   sip.cfg
   4   -rw-    524288  Nov 08 2004 14:32:41   bootromfull

31877 KB total (17007 KB free)
<3Com> delete sip.cfg
```

2) Configure the PC

# Log into the router through FTP, upload the V 2.41 software, and stores it in the root directory of the memory device on the router.

```
ftp> put v 2.413.cc main.bin
```

Reboot the router upon completion of the upgrade to run the upgraded software version.

🕮 **Note:**

You can upgrade configuration files through FTP following the same procedures of upgrading the main software. Note that the obtained configuration file config.cfg also needs to be placed under the root directory (flash:/).

As for remote Boot ROM program upgrading with FTP, you must name the file bootromfull (firm file) or bootrom (file for upgrade) and execute the **upgrade** command after the file is completely transferred.

5.4 TFTP Configuration

5.4.1 TFTP Overview

TFTP (Trivial File Transfer Protocol) is a kind of simple file transfer protocol. Compared with another file transfer protocol FTP, TFTP has no complex interactive access interface and authentication control, which is applicable in the environment in which no complex interaction is needed between the client and the server. For example, the

TFTP protocol is used to obtain the memory mirror of the system when the system is started. Generally, the TFTP protocol is performed based on UDP.

In TFTP, file transfer is originated by the client. When it is necessary to download files, the client end will send a reading request packet to the TFTP server, receive the respond packet from the server, and send acknowledgement to the server. When it is necessary to upload files, the client will send writing request packet to the TFTP server and then send packet to the server and receive confirmation from the server. Router works as a TFTP client.

5.4.2 TFTP Client Configuration

Perform the following operations in user view.

I. Using TFTP to download files

Table 5-15 Use TFTP to download files

Operation	Command
Use TFTP to download files	**tftp** *X.X.X.X* **get** *source-filename* [*destination-filename*]
Download files in the safe mode.	**tftp** *X.X.X.X* **sget** *source-filename* [*destination-filename*]

⚠ **Caution:**

If you choose the safe mode, make sure that the current system has adequate memory to save the files to be downloaded.
The AR 18 series does not support the **sget** command.

II. Using TFTP to upload files

Table 5-16 Use TFTP to upload files

Operation	Command
Use TFTP to upload files	**tftp** *X.X.X.X* **put** *source-filename* [*destination-filename*]

III. Setting relevant access control list

This task is used to set TFTP server access control list, which associates with that set by the **acl** command to implement the access control over the remote TFTP server address.

Perform the following configuration in system view.

Table 5-17 Set access control list

Operation	Command
Specify the access control list for accessing TFTP server	**tftp-server acl** *acl-number*
Delete the set access control list	**undo tftp-server acl**

IV. Accessing a TFTP server using a source interface or source IP address

Perform the following configuration in user view.

Table 5-18 Access a TFTP server using a source interface or source IP address

Operation	Command
Specify the TFTP client to access a TFTP server through a source interface	**tftp** *host* **source-interface** *interface-type interface-number*
Specify the TFTP client to access a TFTP server through a source IP address	**tftp** *host* **source-ip** *ip-address*

By default, the TFTP client uses the IP address of the outbound interface when accessing a TFTP server.

V. Specifying a source interface/IP address for the TFTP client

Perform the following configuration in system view.

Table 5-19 Specify a source interface or source IP address for the TFTP client

Operation	Command
Specify a source interface for the TFTP client	**tftp source-interface** *interface-type interface-number*
Delete the source interface specified for the TFTP client	**undo tftp source-interface**
Specify a source IP address for the packets sent by the TFTP client	**tftp source-ip** *ip-address*
Delete the source IP address specified for the packets sent by the TFTP client	**undo tftp source-ip**

By default, the source IP address in each packet sent by the FTP server is the IP address of the interface where the packet is sent out.

🕮 **Note:**

You may specify a source IP address for the packets sent by the FTP server with the **tftp source-interface** command or with the **tftp source-ip** command. If both commands are configured, the one configured later overrides the former.

5.4.3 Displaying and Debugging TFTP

After completing the above configurations, execute the **display** command in any view to verify them.

Table 5-20 Display and debug TFTP

Operation	Command
Display the current source IP address of the TFTP client	**display tftp source-ip**

5.5 Xmodem Configuration

Xmodem is a file transfer protocol widely adopted for its simplicity and good performance.

Xmodem transfers files through serial interfaces. It supports:

- Two data packet sizes: 128 bytes and 1 KB
- Two check methods: generic checksum and cyclic redundancy check (CRC)
- Retransmission when error occurs (normally, 10 times)

Xmodem comprises receiver and sending programs. The following is how it operates:

1) The receiver sends a negotiation character to negotiate check method.
2) After the negotiation is passed, the sender starts sending packets.
3) When a complete data packet is received, the receiver checks it with the agreed-upon check method. If the check is passed, it sends an ACK asking the sender to send the next packet. If the check fails, it sends a NAK asking the sender to retransmit the packet.

V 2.41 implements the receiving program of Xmodem. It is used on the AUX port, supporting 128-byte packets and CRC check. The sending program is integrated in the HyperTerminal.

You can use Xmodem to upgrade the Boot ROM program, V 2.41 program and configuration file.

⚠ **Caution:**

The **xmodem get** command is not supported on asynchronous serial interfaces but the AUX port. In addition, simultaneous operations are not allowed.

5.5.1 Configuring Xmodem

Perform the following configuration in user view.

Table 5-21 Get a file by using Xmodem

Operation	Command
Get the specified file by using Xmodem	**xmodem get** *filename*

⚠ **Caution:**

filename must be an absolute file path.

When upgrading the Boot ROM program, V 2.41 program or configuration file, you must name the to-be-saved file following the naming convention. You can check their file names with the **dir** command. If a file with the same name has existed, it will be rewritten. Before doing that, the system will ask for confirmation.

5.6 Configuration File Management

5.6.1 Overview

I. Contents and format of the configuration file

The configuration file is a text file in the following format:

- Saved in a format of commands.
- Only non-default parameters are saved for space economy (For the default values of the configuration parameters, refer to the following sections).
- Command mode is the basic frame for organizing these commands. All commands of the same command mode are grouped into a section and blank lines or comment lines (which begin with "#") are used to separate these sections. Blank lines or comment lines can be one line or multiple lines.
- In general, these sections are arranged in the sequence of global configuration, physical interface configuration, logical interface configuration, and routing protocol configuration.

II. Displaying the current and initial configurations of the router

When the router is powdered on, it reads out a configuration file in the default storage path to execute the initialization. So the configuration file in the default storage path is called startup configuration. If there is no configuration file in the default storage path, the router will use default parameters to execute the initialization. Compared with the startup configuration, the valid configuration of the router during running is called current configuration.

Perform the following configuration in any view.

Table 5-22 Display the router configuration

Operation	Command
Display the configuration file loaded at this startup	**display saved-configuration** [**by-linenum**]
Display the configuration file used at this startup and the one used for next startup	**display startup**
Display the configurations for current view	**display this** [**by-linenum**]
Display the running configurations of the router	**display current-configuration** [**controller** | **interface** *interface-type* [*interface-number*] | **configuration** [**isp** | **luser** | **radius-template** | **system** | **user-interface**|]] [| [**begin** | **include** | **exclude**] *string*] [**by-linenum**]

🕮 **Note:**

The format used for displaying the configuration file is the same as that for saving the file.

III. Modifying and saving the current configuration

The user can modify the current configuration of the router through the command line interface. In order to make the current configuration as the startup configuration of the router at the next power-on, use the **save** command to save the current configuration into the default storage device.

Perform the following configuration in any view.

Table 5-23 Save the current configuration

Operation	Command
Save the current configuration	**save** [*file-name*] [**safely**]

When the *file-name* argument is not specified, the configurations you made are saved to the configuration file loaded at this startup.

Executing this command without the **safely** keyword can make the speed of saving configuration files fast, but these files cannot survive a reboot or power-off during the saving process; executing this command with the **safely** keyword, however, makes the saving speed slower, but these files can survive a reboot or power-off during the saving process.

By default, fast saving applies, which is recommended in an environment where stable power supplies are available. In an environment where stable power supplies are not available or in the case of remote maintenance, however, you are recommended to execute the command with the **safely** keyword.

🕮 **Note:**

You are recommended to save the configurations using the **save** command before rebooting the router, so that the router can keep exactly the same configurations after reboot.

IV. Deleting a configuration file

To delete the configuration file loaded at this startup from the Flash, execute the **reset saved-configuration** command. After the configuration file is deleted, the default or the prespecified configuration file is used for initialization at next startup.

You may need to delete the configuration file loaded at this startup for one of the following reasons:

- After the software of the router has been upgraded, it may cause the mismatch between the software and the configuration file.
- It is found that the configuration file in the Flash has been damaged, for example, a wrong configuration file is loaded.

After deleting the configuration file, you may use the **save** command to save the current configurations to a new configuration file.

Perform the following configuration in user view.

Table 5-24 Erase the configuration file in the storage devices

Operation	Command
Delete the configuration file loaded at this startup from the Flash	**reset saved-configuration**

V. Setting the configuration file to be used at the next boot

Table 5-25 Set the configuration file to be used at the next boot

Operation	Command
Set the configuration file to be used at next startup	**startup saved-configuration** *filename*
Configure the system to boot without any configuration file at next startup	**undo startup saved-configuration**

5.6.2 Naming Configuration Files and Setting Their Selection Order at Boot

I. Naming configuration files

Table 5-26 Name configuration files

File name	Description
v 2.41cfg.cfg	Default name for the configuration file. It is vendor-specified but you can modify the contents of the file.
v 2.41cfg.def	Factory default configuration file name; its contents are vendor-specified.
v 2.41cfg.txt	Name of the configuration files for 3Com devices manufactured before.

II. Selecting the configuration file

Following are how configuration files are selected at a system boot:

1) If you do not set to ignore configuration file booting, configuration files are selected in the order described in 2) and 3). Otherwise, the system boots with empty configuration.
2) If you specify a boot configuration file, the system selects its boot configuration file in this order: the specified configuration file and then v 2.41cfg.def. In case v 2.41cfg.def does not exist, the system boots with empty configuration.
3) If you do not specify a boot configuration file, the configuration file is selected in this order: v 2.41cfg.cfg, v 2.41cfg.txt, and v 2.41cfg.def. If none of them exists, the system boots with empty configuration.

5.6.3 Backing Up Configuration Files

You can back up configuration files by:

- Backing up the display information of the **display current-configuration** command;

- Using FTP;
- Using TFTP.

I. Backing up the display information of the current-configuration command

Executing the **display current-configuration** command can display all the configurations in the router except for the defaults. In the HyperTerminal, you can back up them by copying all the display information into a text file.

II. Backing up using FTP

You can use FTP to backup configuration files by two means:

One option is to take the router as the FTP server to FTP the configuration files from the router to the PC (the FTP client).

After the router boots, perform the following configurations:

```
[3Com] local-user 3Com
[3Com-luser-3Com] password simple 3Com
[3Com-luser-3Com] service-type ftp ftp-directory flash:/ftp/3Com
```

Then create an FTP connection on the PC connected to the router and back up the configuration files:

```
C:\>ftp x.x.x.x
<ftp> get remotefile [localfile]
200 Port command okay.
150 Server okay , now transmit file .
226 file transmit success.
ftp: 735 bytes received in 0.06Seconds 12.25Kbytes/sec.
```

Where, *remotefile* is a configuration file (v 2.41cfg.cfg) on the router.

Alternatively, you can take the router as the FTP client to FTP its configuration files to the PC (the FTP server).

Enable the FTP server and configure authorization information on the PC connected to the router. Then execute the following commands on the router:

```
<3Com> ftp x.x.x.x
[ftp] put localfile [ remotefile ]
```

Where, *remotefile* is a configuration file (v 2.41cfg.cfg) on the router.

III. Backing up using TFTP

The router is operating as TFTP Client.

To upload the configuration file from the router to TFTP Server, a PC, execute the following command:

```
<3Com> tftp x.x.x.x put localfile [remotefile]
```

Where, *localfile* specifies the name of the configuration file on the router and *remotefile* specifies the name of the uploaded configuration file to be saved on TFTP Server.

Chapter 6 User Interface Configuration

6.1 User Interface Overview

6.1.1 Brief Introduction

User interface view is a new feature provided by the system to manage asynchronous interfaces working in the flow mode. The emergence of this kind of view allows the user to configure the login parameters of various users in a similar way, for these different kinds of interfaces are usually used for system configuration management.

So far, the system supports:

- Local configuration via the Console port
- Local/Remote configuration via the AUX port
- Local/Remote configuration via the serial port working in asynchronous mode (TTY)
- Local/Remote configuration through Telnet or SSH

There are four types of user interfaces commensurate with these configuration modes. They are:

- Console port (CON)

Console port is a kind of line device port. On a router, a Console port of EIA/TIA-232 DCE type is provided for users to make configuration.

- AUX port (AUX)

AUX port is also a kind of line device port. On a router, an AUX port of EIA/TIA-232 DTE type is provided for the dialup access via modem.

- Asynchronous serial port (TTY)

TTY user interface is used if a user logs in to the router via an asynchronous serial port or synchronous/asynchronous serial port (working in asynchronous mode)

- Virtual line (VTY)

Virtual port is a logical terminal line that is used for Telnet access to the router and is generally known as VTY.

6.1.2 Numbering User Interfaces

User interfaces can be numbered in two ways, that is, absolute numbering and relative numbering.

I. Absolute numbering

There are four categories of user interfaces in the system and they are ordered in certain sequence, specifically, CON, AUX, TTY, and VTY.

- There is only one Console port and one AUX port, but there can be several TTY and VTY user interfaces, with the interfaces of each type being numbered separately in sequence. With the absolute numbering approach, user interfaces are numbered starting at ui0 (Console port) and in ascending order. The Console and AUX ports each have one number while for the TTY and VTY interfaces, different products can have multiple numbers and you can use the **display user-interface** command to view the number. An absolute number can uniquely specify a user interface or a group of user interfaces.

II. Relative numbering

A relative number is in the form of user interface type + number. This number is significant only inside the user interfaces of each type. In other words, such a number can only specify one user interface or a user interface group among the same type of user interfaces rather than among all the user interfaces in a unique way. Following is the relative numbering rules:

- CON is numbered con 0.
- AUX is numbered aux 0.
- TTYs are numbered starting at 0 in an ascending order.
- VTYs are numbered starting at 0 in an ascending order.

6.2 User Interface Configuration

Perform the following tasks to configure a user interface:

- Enter user interface view
- Configure the protocol supported by the current user interface
- Configure the attributes of asynchronous interface
- Configure terminal attributes
- Configure user management
- Set modem attributes
- Configure the auto-execute command
- Configure incoming and outgoing call restriction on VTY user interface
- Enable/disable console login re-authentication
- Define shortcut keys for starting terminal sessions/aborting tasks

6.2.1 Entering User Interface View

Access a user interface view by entering the corresponding command in system view. You can access a single-user interface view to configure one user interface or access a multi-user interface view to configure several user interfaces at the same time.

Table 6-1 Access user interface view

Operation	Command
Access a single-user or multi-user interface view	**user-interface** [*type-keyword*] *number* [*ending-number*]

For example: Access the view of the user interface aux.

```
[3Com] user-interface aux 0
[3Com-ui-aux0]
```

In user interface view, you can configure and manage the attributes of each asynchronous interface, including

1) Set the asynchronous attributes in speed, flow control, parity, stopbits and databits.
2) Configure terminal attributes including enabling terminal service (shell), setting timeout disconnection (idle-timeout) of terminal user, setting the screen length (screen-length) of the terminal screen, configuring authentication, and setting the size of the history command buffer.
3) Set privilege including assigning privilege to the users accessing the system via user interfaces, etc.
4) Configure modem attributes including configuring modem and its script.

6.2.2 Configuring the Current User Interface to Support the Protocol(s)

You can configure the current user interface to support the protocol(s) using the following command. By default, the user interface supports all the protocols: PAD, Telnet, and SSH.

Perform the following configurations in VTY user interface view:

Table 6-2 Configure the current user interface to support the protocol(s)

Operation	Command
Configure the current user interface to support the protocol(s)	**protocol inbound** { **all** | **ssh** | **telnet** | **pad** }

6.2.3 Configuring Asynchronous Interface Attributes

You can configure the asynchronous attributes of a user interface in the view for it. The following configuration commands are valid only when the interface is working in asynchronous flow mode.

Perform the following operations in user interface view.

I. Configuring transmission speed

Table 6-3 Configure transmission speed

Operation	Command
Set a transmission speed	**speed** *speed-value*
Restore the default transmission speed	**undo speed**

Asynchronous serial interfaces support the transmission at the speed of

- 300 bps
- 600 bps
- 1200 bps
- 2400 bps
- 4800 bps
- 9600 bps
- 19200 bps
- 38400 bps
- 57600 bps
- 115200 bps
- 4096000 bps

The transmission rate of an asynchronous interface defaults to 9600 bps. But the transmission rate depends on interface type. For example, the rate at a Console port can only be 115200 bps, but not 4096000 bps.

II. Configuring flow control mode

Table 6-4 Configure flow control mode

Operation	Command
Configure a flow control mode	**flow-control** { **none** | **software** | **hardware** }
Restore the default flow control mode	**undo flow-control**

By default, TTY interfaces use hardware flow control.

The following are descriptions of the parameters.

none: No flow control

software: Software flow control

hardware: Hardware flow control, which is only effective for console port , AUX port, and serial port in asynchronous mode

III. Setting parity bit

Table 6-5 Set parity bit

Operation	Command
Set parity bit	**parity** { **none** | **even** | **odd** | **mark** | **space** }
Set parity bit to the default value	**undo parity**

Following are the descriptions of the parameters.

none: No parity check

even: Even parity check

odd: Odd parity check

mark: Mark parity check

space: Space parity check

The parity check defaults to **none**, that is, no parity.

IV. Setting stop bits

Table 6-6 Set stop bits

Operation	Command
Set stop bits	**stopbits** { **1.5 | 1 | 2** }
Restore the default stop bit setting	**undo stopbits**

The stop bit setting defaults to 1.

V. Setting databits

Table 6-7 Set data bits

Operation	Command
Set data bits	**databits** { **5 | 6 | 7 | 8** }
Restore the default data bit setting	**undo databits**

The data bits supported by an asynchronous interface are 5, 6, 7, and 8.

The **databits** defaults to 8.

6.2.4 Configuring Terminal Attributes

Perform the following operations in user interface view.

I. Starting the terminal service

Table 6-8 Enable the terminal service

Operation	Command
Enable the shell service	**shell**
Disable the shell service	**undo shell**

⚠ **Caution:**

By default, the terminal service is enabled on all user interfaces.

For example:

```
[3Com] user-interface vty 0 4
[3Com-ui-vty0-4] undo shell
```

After you configure the **undo shell** command, no connection can be set up. This, however, does not affect those users that have telnetted onto the router.

II. Setting idle-timeout disconnection of a terminal user

Table 6-9 Set the idle-timeout disconnection function for terminal users

Operation	Command
Set the idle-timeout disconnection function for the users.	**idle-timeout** *minutes* [*seconds*]
Restore the default idle-timeout disconnection setting for the users.	**undo idle-timeout**

By default, the idle-timeout disconnection function is enabled and the timeout time is set to 10 minutes. In other words, if there is no operation in 10 minutes, the TTY will automatically disconnect. Configuring **idle-timeout 0** will disable the idle-timeout disconnection function.

III. Configuring user interface locking function

This configuration is used to lock the current terminal line and remind you to enter the password, in case any other person operates on the terminal line without your presence.

Table 6-10 Configure user interface locking function

Operation	Command
Lock user interface.	**lock**

# For example, you have accessed the router via VTY1, and you lock the user-interface vty 1 now because you will leave for a while.

```
<3Com> lock
```

Password: xxxx

Again: xxxx

IV. Setting screen-length of terminal screen

Table 6-11 Set screen-length of terminal screen

Operation	Command
Set screen-length of terminal screen	**screen-length** *screen-length*
Restore the default screen-length of terminal screen	**undo screen-length**

By default, the full screen-length of terminal screen is 24 lines.

screen-length 0 disables screen split.

undo screen-length restores the default setting.

V. Setting the size of the history command buffer

Table 6-12 Set the size of the buffer for the history command

Operation	Command
Set the size of the buffer for the history commands	**history-command max-size** *size-value*
Restore the default size of the buffer for the history commands	**undo history-command max-size**

The parameter *size-value* is the history command buffer size which defaults to 10, that is, the buffer is allowed to restore a maximum of ten history commands.

VI. Enabling message transfer between user interfaces

You may configure the router to transfer messages between user interfaces.

Table 6-13 Enable message transfer between user interfaces

Operation	Command
Enable message transfer between user interfaces.	**send** { **all** | *number* | *type-name number* }

6.2.5 Configuring Modem Attributes

In the event of dial-in via a modem into an asynchronous interface, you can manage and configure the modem-concerned parameters in user interface view. You should note that the configuration commands in this case are only valid for the AUX interface and the serial interfaces working in asynchronous mode.

Table 6-14 Make modem configurations

Operation	Command
Set the time interval that the system waits for the CD_UP signal after receiving the RING signal	**modem timer answer** *seconds*
Restore the default time interval that the system waits for the CD_UP signal after receiving the RING signal	**undo modem timer answer**
Set the answer mode to auto-answer	**modem auto-answer**
Set the answer mode to manual answer	**undo modem auto-answer**
Enable the modem to dial in and dial out	**modem** [**both** | **call-in** | **call-out**]
Disable the modem to dial in or dial out	**undo modem** [**both** | **call-in** | **call-out**]

For example, set **modem** auto-answer on the **aux** port.

```
[3Com-ui-aux0] modem auto-answer
```

6.2.6 Configuring the auto-execute command

You should be aware of the following restrictions before using the **auto-execute command** command:

- CON does not support **auto-execute command**.
- If there is only AUX but no CON on a router (AUX and CON shares the same port), the AUX will not support **auto-execute command** as well.
- These constraints do not apply to other types of user interfaces.

When a user logs on, some command configured using **auto-execute command** on the terminal will automatically be executed. The user line will be disconnected automatically once the execution of the command is finished.

A common approach is to configure the Telnet command using the **auto-execute command** command on the terminal so that the user may automatically connect to the specified host.

⚠ **Caution:**

You should use this command with cautions because it will probably make you unable to perform the regular configurations for the system via the terminal line to which the command is applied. Before configuring the **auto-execute command** command and saving the configuration (by executing the **save** command), you should make sure that you can access the system to remove the configuration by other means.

Perform the following operations in user interface view.

Table 6-15 Set the auto-execute command

Operation	Command
Set the automatic execution of a command	**auto-execute command** *command*
Disable automatic command execution	**undo auto-execute command**

The **auto-execute command** command that a user has configured will be automatically executed when the user makes a new access attempt.

# For example, the **telnet** command will be executed automatically for the user to access the destination host.

The steps to be executed are:

1) Execute the **auto-execute command** command in user interface view.

```
[3Com-ui4] auto-execute command telnet 10.110.100.1
```

2) Exit the system view and log on again. The **telnet** 10.110.100.1 command will be executed automatically.

6.2.7 Configuring Inbound/Outbound Call Restriction on the VTY User Interface

You can configure the inbound/outbound call restriction on the VTY (Telnet) user interface through referencing an ACL.

Perform the following operations in user interface view.

Table 6-16 Configure the inbound/outbound call restriction on the VTY user interface

Operation	Command
Configure the inbound/outbound call restriction on the VTY user interface	**acl** *acl-number* { **inbound** | **outbound** }
Cancel the inbound/outbound call restriction on the VTY user interface	**undo acl** { **inbound** | **outbound** }

6.2.8 Enabling/Disabling Console Login Re-Authentication

You may configure console login re-authentication to provide additional security for the console port.

Perform the following configuration in user interface view.

Table 6-17 Enable/disable console login re-authentication

Operation	Command
Enable console login re-authentication	**re-authentication**
Disable console login re-authentication	**undo re-authentication**

By default, console login re-authentication is disabled.

To use console login re-authentication, you must configure the **flow-control hardware** command as well.

When the scheme authentication mode is adopted, set the priority of the corresponding user to three with the **level** command in local user view. Otherwise, you can only execute level-0 commands after re-logging in from the console port.

6.2.9 Defining Shortcut Keys for Starting Terminal Sessions/Aborting Tasks

Perform the following configuration in user interface view.

Table 6-18 Define shortcut keys for starting terminal sessions/aborting tasks

Operation	Command
Define a shortcut key or key combination for starting terminal sessions	**activation-key** *character*
Delete the existing shortcut key or key combination used to start terminal sessions	**undo re- activation-key**
Define a shortcut key or key combination for aborting tasks	**escape-key** { **default** | *character* }

Operation	Command
Delete the existing shortcut key or key combination used to abort tasks	**undo escape-key**

The default shortcut key combination for aborting tasks is <CTL+C>.

6.3 Displaying and Debugging

After the above configuration, execute the **display** command in any view to display the user interface configuration, and to verify the configuration.

6.3.1 Displaying Use Information

Perform the following operations in any view.

Table 6-19 Display the information of users on all user interfaces

Operation	Command
Display the use information on all the user interfaces	**display users** [**all**]

6.3.2 Displaying Physical Attributes and Some Configurations

Perform the following operations in any view.

Table 6-20 Display the physical attributes and some configurations on a user interface

Operation	Command
Display the physical attributes and some configurations on a user interface	**display user-interface** [*type-name*] [*number*]

Chapter 7 User Management

7.1 User Management Overview

A router is not configured with a user password when it is powered on for the first time. In that condition, any user can perform configuration on the router as long as connecting his PC with the router via a Console port. The remote user can also access the router via Telnet if the router has been configured with IP address of Main Processing Unit (MPU) or the interface board, and it is possible for the remote user to access the network by establishing PPP connection with the router. To ensure the network security, it is necessary to configure a user and user password for the router to facilitate the management of the user.

📖 **Note:**

This chapter focuses on the authentication management over terminal users and Telnet users. Refer to the Security module in *V 2.41 Operation Manual* for other user types and AAA RADIUS/HWTACACS authentication.

7.1.1 User Classification

According to the service for a user, the user of a router can be classified into the following types:

- HyperTerminal user, accessing the router via a Console port or AUX port;
- Telnet user, accessing the router via Telnet command;
- FTP user, establishing FTP connection with the router to transmit packets;
- PPP user, establishing PPP connections (such as dialing and PPPoA) with the router to access the network.
- SSH user, establishing SSH connection to log into the router;
- PAD user, establishing PAD connection with the router to access the network.

A user can have several services at the same time. In this way, only one user can execute multiple functions.

7.1.2 User Priority

The system manages HyperTerminal and Telnet users hierarchically. According to this hierarchy, users are sorted into four levels: visit, monitor, system and manage, identified by 0 through 3. After users at different levels log in, they can only use commands at their own, or lower, levels. If password authentication or no authentication applies, the command level that a user can access depends on the level of the user interface where he logs in.

For example, if the priority level of a user is 2, he can access the command levels 0 through 2. The user with the priority level 3 can access all the commands. The commands that the user of each level can access are shown in Table 7-1.

Table 7-1 User priority

User Priority	Name	Command
0	Visit	**Ping**, **tracert**, **telnet**
1	Monitor	**ping**, **tracert**, **telnet**, **display**, **debugging**
2	System	All configuration commands (except the Manage command) and the commands with the priority level 0 and 1.
3	Manage	All commands

🕮 **Note:**

The Manage command refers to the file system command, FTP command, or TFTP command.

7.1.3 User Authentication

The system authenticates users at login. There are four types of authentication schemes: local authentication, AAA server authentication, password authentication, and non-authentication. Non-authentication is not preferred, because a user can log into the router without username and password when it applies. Password authentication is somewhat securer, because it requires each login user to provide the password even though without the username. When local authentication or AAA server authentication applies, however, a login user must provide the username and password that are the same as the ones configured on the router or the AAA server. Dialup users are often authenticated through AAA servers whereas telnet and terminal users are authenticated at the local.

7.1.4 Router User Planning

Router user planning can be performed according to actual requirement. Usually, at least one HyperTerminal user (Console user) can be established on a router, and it is needed to configure a Telnet user to meet the remote access requirement. A FTP user can upload or download files on the router from the remote, and a PPP user can access the network via the PPP connection with the router.

The configuration of Telnet/HyperTerminal user will be introduced in this section. For the configuration of FTP users, refer to the section “5.3 FTP Configuration” in “Chapter 5 File Management” of this module. For the configuration of PPP users, refer to *V 2.41 Operation Manual – Security* and *V 2.41 Operation Manual – Link Layer Protocol*.

7.2 User Management Configuration

The user management configuration includes:

- Configure user authentication mode
- Configure username and password
- Configure user priority
- Enable per-command accounting

The purpose of user authentication is to enable the legal users to log on and use the router and prevent the illegal users from passing the authentication.

7.2.1 Configuring User Authentication Mode

By configuring the user authentication mode, you can set the authentication method when a user accesses the router from the user interface specified in the view.

Perform the following configuration in user interface view.

Table 7-2 Configure the user authentication method

Operation	Command
Enable user authentication	**authentication-mode** { **password** | **scheme** [**command-authorization**] }
Disable user authentication	**authentication-mode none**
Restore the default authentication mode	**undo authentication-mode**

The keyword **none** indicates not to authenticate users; **password** indicates to authenticate the password but not the username; **scheme** indicates to authenticate to use an AAA authentication scheme (a local authentication scheme or RADIUS/HWTACACS authentication scheme) as specified by the **scheme** command.

By default, the authentication mode is **password** for TTY (asynchronous interface), VTY, and AUX user interfaces and is **none** for other user interfaces.

Telnet and terminal user authentications usually use the local authentication scheme. Refer to *V 2.41 Operation Manual – Security*.

7.2.2 Configuring Username and Password

I. Setting password for password authentication

If you choose password authentication when configuring the authentication mode, you need to set the password.

Perform the following configuration in user interface view.

Table 7-3 Set password for password authentication

Operation	Command
Set password for password authentication	**set authentication password** { **cipher** | **simple** } *password*
Cancel password for password authentication	**undo set authentication password**

The keyword **simple** indicates to configure the password in plain text, while **cipher** indicates to configure the password in cipher text.

II. Configuring username and password for local authentication

If you choose local authentication when configuring the authentication mode, you need to set a username and password.

Table 7-4 Configure username and password for local authentication

Operation	Command
Configure a username (in system view)	**local-user** *user-name*
Remove the user (in system view)	**undo local-user** { *user-name* **| all** }
Set a password for the local user (in local user view)	**password** { **cipher | simple** } *password*
Cancel the password of the local user (in local user view)	**undo password**

Where, **simple** indicates to configure the password in plain text, while **cipher** indicates to configure the password in ciphertext.

Then configure the user to adopt local authentication scheme.

Table 7-5 Configure the user in the domain to adopt local authentication scheme

Operation	Command
Create an ISP domain or enter the view of an existing ISP domain (in system view)	**domain** { *isp-name* | **default** { **disable | enable** *isp-name* } }
Delete a specified ISP domain (in system view)	**undo domain** *isp-name*

Operation	Command
Configure the user in the current ISP domain to adopt local authentication scheme (in ISP domain view)	**scheme local**

7.2.3 Configuring User Priority

The priority configuration of the user interface and the user determines the system commands that can be accessed.

I. Setting the priority of the user interface

You can set the priority of each user interface. Perform the following configuration in user interface view.

Table 7-6 Set the priority of the user interface

Operation	Command
Set the priority of the user interface	**user privilege level** *level*
Restore the default priority of the user interface	**undo user privilege level**

By default, the priority of the Console port is 3 and that of other user interfaces is 0.

# Set the priority of the Console port to 3 and that of VTY 0 user interface to 2.

```
[3Com-ui-console0] user privilege level 3
[3Com-ui-vty0] user privilege level 2
```

Suppose that a user does not have to pass authentication in order to log on via the two user interfaces. The commands that can be accessed are different when a user logs on from the Console port and VTY 0 respectively. He can access all the commands when logging on from the Console port, but he can only access the command with the priority level lower than 2 when logging on from the VTY 0.

II. Setting the priority of the user

Perform the following configuration in local user view.

Table 7-7 Set the priority of the user

Operation	Command
Set the priority of the user	**level** *level*
Restore the default priority of the user	**undo level**

level indicates the priority of the user, ranging from 0 to 3. 0 indicates the lowest level and 3 the highest. The default priority is 1 after the user configuration.

Note:

If password authentication or no authentication applies, the command level that a user can access depends on the level of the user interface where the user logs in.

If authentication requires username and password, user priority determines which priority of commands the login user can access. If the user has not been assigned a priority, the level of the user interface applies.

7.2.4 Enabling Per-Command Accounting on a User Interface

Perform the following configuration in user interface view.

Table 7-8 Enable per-command accounting on the user interface

Operation	Command
Enable per-command accounting for the terminal users logged in from the user interface	**accounting commands scheme**
Disable per-command accounting on the user interface	**undo accounting commands scheme**

By default, per-command accounting is disabled on the user interface.

7.3 Displaying User Information

Using the following command, you can view the information of the configured user, local user and on-line user.

Perform the following configuration in any view.

Table 7-9 Display user information

Operation	Command
Display the information of all users	**display users** [**all**]
Display the information of local user	**display local-user**
Display the information about the user who is currently authorized to perform configurations.	**display configure-user**

7.4 Typical Example of User Management

7.4.1 Performing Password Authentication

The user need enter the password 3Com when logging onto the system from the VTY 0 by password authentication. The user priority is 3. The operation commands are shown as follows:

```
<3Com> system-view
[3Com] user-interface vty 0
[3Com-ui-vty0] authentication-mode password
[3Com-ui-vty0] set authentication password simple 3Com
[3Com-ui-vty0] user privilege level 3
```

7.4.2 Performing User Authentication Using the Local User Database

The user need enter the configured username v 2.41 and password 3Com when logging onto the system from the VTY 0. The operation commands are shown as follows:

```
<3Com> system-view
[3Com] user-interface vty 0
[3Com-ui-vty0] authentication-mode scheme
[3Com-ui-vty0] quit
[3Com] local-user v 2.41
[3Com-luser-v 2.41] password simple 3Com
[3Com-luser-v 2.41] service-type telnet
[3Com-luser-v 2.41] level 3
[3Com] domain system
[3Com-isp-system] scheme local
```

Chapter 8 NTP Configuration

8.1 Brief Introduction

Network time protocol is a TCP/IP protocol intended for advertising precise time throughout a network. Its transmission is based on UDP. The basic principle is illustrated in the following figure:

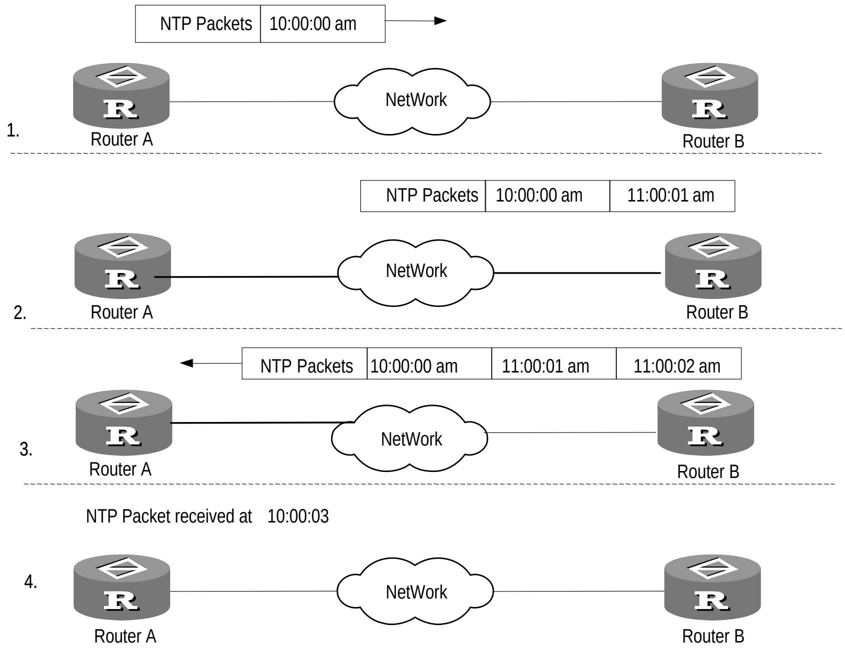


Figure 8-1 NTP basic principle diagram

The above figure displays NTP basic operating principle. Router A and Router B are connected via the serial port. Both of them have their own independent system clock. To implement automatic synchronization of their system clocks, suppose:

- Before the system clocks of Router A and Router B are synchronized, the clock of Router A is set to 10:00:00am and the clock of Router B is set to 11:00:00am.
- Router B acts as the NTP time server. That is, Router A will synchronize its clock with that of Router B.
- One-way transmission of data packets between Router A and Router B needs 1 second.

The operating procedure of the system clocks synchronization includes:

- Router A transmits an NTP packet to Router B. The packet carries the timestamp when it leaves Router A, which is 10:00:00am (T1).
- When the NTP packet reaches Router B, Router B adds its timestamp to it, which is 11: 00:01am (T2).

- When the NTP packet leaves Router B, Router B adds its timestamp to it again, which is 11:00:02am (T3).
- When Router A receives the response packet, it adds a new timestamp to it, which is 10:00:03am (T4).

Until now, Router A has enough information to calculate the following two important parameters:

- Time delay for the NTP message cycle: Delay = (T4-T1)-(T3-T2).
- Time offset of Router A relative to Router B: offset = ((T2-T1)+(T3-T4))/2.

In this case, Router A can set its own clock according to the information to synchronize with the clock of Router B. This is only a simple description of the NTP operating principle. In RFC1305, NTP uses complex algorithm to ensure the precise of clock synchronization.

Depending on network structure and position of the router on the network, the router can operate in one of these six modes:

- Client mode, where the remote server is operating as the local time server. In this mode, the local client can synchronize to the remote server but not vice versa.
- Symmetric active mode, where the remote server is a peer. In this mode, the local server can synchronize or be synchronized by the peer. If both of them have reference clock, the one with lower stratum is preferred.
- Broadcast server mode, where an interface on the router is configured to broadcast NTP messages.
- Broadcast client mode, where an interface on the router is configured to receive NTP broadcast messages.
- Multicast server mode, where an interface on the router is configured to multicast NTP messages.
- Multicast client mode, where an interface on the router is configured to receive NTP multicast messages.

The first two modes are unicast. They support NTP multi-instances and can synchronize time on an MPLS VPN, allowing network devices (CEs and PEs) located on different physical network segments to synchronize so long as they belong to the same VPN. The following are the available functions:

- The NTP client on a CE synchronizes to the NTP server on a PE.
- The NP client on a PE synchronizes to the NTP server on a CE through the specified VPN instance.
- The NTP server on a PE can synchronize the NTP clients on multiple CEs.

8.2 NTP Configuration

NTP is used for time synchronization in the entire network. NTP configuration includes:

- Configure NTP operating mode
- Set NTP ID authentication

- Set the interface for the local to transmit the NTP messages
- Set the local clock as the NTP master clock
- Enable/disable the interface to receive the NTP messages
- Set the access control authority of the local server service
- Set the number of sessions allowed to be established locally

8.2.1 Configuring NTP Operation Mode

The operation mode of the local router in the NTP protocol can be configured according to the position of the router in the network and the network structure. For example, the remote server can be set as local time server, and the local router must work in client mode in accordance; the remote server can also be set as the peer of the local router, accordingly, the local router must work in symmetric active mode. An interface of the local router can be set to send NTP broadcast packet, while the local router works in broadcast mode; it can also be set to send NTP multicast packet, while the local router works in multicast mode, or be set to receive NTP multicast packet, while the local router works in multicast client mode.

- Configure NTP server mode
- Configure NTP peer mode
- Configure NTP broadcast server mode
- Configure NTP broadcast client mode
- Configure NTP multicast server mode
- Configure NTP multicast client mode

I. Configuring NTP server mode

The following configuration is used to set the remote server specified by *X.X.X.X* or *server-name* as the local time server. The *X.X.X.X* is a host address and cannot be the address of the broadcast, multicast or reference clock. The local router operates in client mode. In this mode, the local client device can be synchronized to the remote server, but the remote server cannot be synchronized to the local client device. After you specify the *vpn-instance-name* argument on the PE, the NTP client on the PE can synchronize to the NTP server on the CE, but the server does not synchronize to the local clients.

Perform the following operations in system view.

Table 8-1 Configure NTP server mode

Operation	Command
Configure NTP server mode	**ntp-service unicast-server** [**vpn-instance** *vpn-instance-name*] {*X.X.X.X* | *server-name* } [**version** *number* | **source-interface** *interface-type interface-number* | **priority**] *

Operation	Command
Remove NTP server mode	**undo ntp-service unicast-server** {*X.X.X.X* | *server-name* }

The range of the NTP version *number* is 1 to 3. It is 3 by default. The range of the authentication key ID number is 1 to 4294967295. The *interface-type interface-number* specifies an interface, whose IP address will be used as the source IP address in the NTP packets sent to the time server. The parameter **priority** specifies that the time server is the preferred one.

II. Configuring NTP peer mode

The following configuration is used to set the remote server specified by the *X.X.X.X* as the peer of the local router. The local router is run in symmetric active mode. The *X.X.X.X* is a host address and cannot be the address of the broadcast, multicast or reference clock. In this configuration, the local router can be synchronized to the remote server and vice versa.

Perform the following operations in system view.

Table 8-2 Configure NTP peer mode

Operation	Command
Configure NTP peer mode	**ntp-service unicast-peer** [**vpn-instance** *vpn-instance-name*] {*X.X.X.X* | *server-name* } [**version** *number* | **authentication-key** *keyid* | **source-interface** *interface-type interface-number* | **priority**] *
Remove NTP peer mode	**undo ntp-service unicast-peer** { *X.X.X.X* | *server-name* }

The range of the NTP version *number* is 1 to 3. It is 3 by default. The range of the authentication key ID number is 1 to 4294967295. The *interface-type interface-number* specifies an interface whose IP address will be used as the source IP address in the NTP packets sent to the time server. The parameter **priority** specifies that the time server is the preferred one.

III. Configuring NTP broadcast server mode

The following configuration specifies an interface on the local router to broadcast NTP messages. The local router is running in broadcast server mode to broadcast messages periodically to the broadcast clients.

Perform the following operations in interface view.

Table 8-3 Configure NTP broadcast server mode

Operation	Command
Configure NTP broadcast server	**ntp-service broadcast-server** [**authentication-keyid** *keyid* | **version** *number*] *
Remove NTP broadcast server mode	**undo ntp-service broadcast-server**

The range of the NTP version *number* is 1 to 3. It is 3 by default. The range of the authentication *keyid* is 1 to 4294967295. This command must be configured on the interface that is to transmit NTP broadcast packets.

IV. Configuring NTP broadcast client mode

The following configuration is used to specify the local interface on the local router to receive the NTP broadcast packets. The local router is run in broadcast client mode. It first listens discreetly to the broadcast packets from the server. When the first broadcast packet is received, the local router starts a short client/server process to exchange messages with the remote server in order to estimate network delay. Then it enters the broadcast client mode to listen discreetly to the broadcast packets and synchronize the local clock according to the coming broadcast packets.

Perform the following operations in interface view.

Table 8-4 Configure NTP broadcast client mode

Operation	Command
Configure NTP broadcast client (interface view)	**ntp-service broadcast-client**
Remove NTP broadcast server mode	**undo ntp-service broadcast-client**

This command must be configured on the interface that is to receive NTP broadcast packets.

V. Configuring NTP multicast server mode

This configuration specifies an interface on the local router to transmit NTP multicast packets. The local router is running in broadcast mode to multicast periodically to the multicast clients.

Perform the following operations in interface view.

Table 8-5 Configure NTP multicast server mode

Operation	Command
Configure NTP multicast server mode	**ntp-service multicast-server** [*X.X.X.X*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* | **version** *number*] *
Remove NTP multicast server mode	**undo ntp-service multicast-server**

The range of the NTP version *number* is 1 to 3. It is 3 by default. The range of the ID authentication *keyid* is 1 to 4294967295. The range of the *ttl-number* of the multicast packets is 1 to 255. The default multicast IP address is 224.0.1.1.

This command must be configured on the interface that is to transmit NTP multicast packets.

VI. Configuring NTP multicast client mode

The following configuration is used to specify an interface on the local router to receive the NTP multicast packets. The local router is run in multicast client mode. It first listens discreetly to the multicast packets from the server. When the first multicast packet is received, the local router starts a short client/server process to exchange messages with the remote server in order to estimate network delay. Then it enters the multicast client mode to listen discreetly to the multicast packets and synchronize the local clock according to the coming multicast packets.

Perform the following operations in interface view.

Table 8-6 Configure NTP multicast client mode

Operation	Command
Configure NTP multicast client mode	**ntp-service multicast-client** [*X.X.X.X*]
Remove NTP multicast client mode	**undo ntp-service multicast-client**

By default, the multicast *X.X.X.X* is 224.0.1.1. This command must be configured on the interface that is to receive NTP multicast packets.

8.2.2 Configuring NTP ID Authentication

When configuring NTP ID authentication, you must configure it at both ends of server and client and make sure that the same key is configured on them. To ensure a successful authentication, you must also make sure that the key is reliable.

I. Enabling NTP ID authentication

Perform the following operations in system view.

Table 8-7 Configure NTP ID authentication

Operation	Command
Enable NTP ID authentication	**ntp-service authentication enable**
Disable NTP ID authentication	**undo ntp-service authentication enable**

II. Setting NTP Authentication Key

The following configuration is used to set NTP authentication key.

Perform the following operations in system view.

Table 8-8 Configure NTP authentication key

Operation	Command
Set NTP authentication key	**ntp-service authentication-keyid** *number* **authentication-mode md5** *value*
Remove NTP authentication key	**undo ntp-service authentication-keyid** *number*

The range of the key *number* is 1 to 4294967295. The key *value* is 1 to 32 ASCII characters.

III. Setting the Specified Key to Be Reliable

The following configuration is used to declare or deny that the key is reliable.

Perform the following operations in system view.

Table 8-9 Set the specified key to be reliable

Operation	Command
Specify the key to be reliable	**ntp-service reliable authentication-keyid** *key-number*
Remove the specified reliable key	**undo ntp-service reliable authentication-keyid** *key-number*

The range of the key number is 1 to 4294967295.

IV. Associating the authentication key with the NTP Server

For server and peer modes, you must associate the specified key with the NTP server at the client. This is because in either mode, the client may be configured with multiple servers and therefore needs an authentication key to decide which one to use.

Table 8-10 Associate the specified key with the NTP server

Operation	Command
In server mode, associate the specified key with the NTP server.	**ntp-service unicast-server** { *X.X.X.X* | *server-name* } **authentication-keyid** *keyid*
In peer mode, associate the specified key with the NTP server.	**ntp-service unicast-peer** { *X.X.X.X* | *server-name* } **authentication-key** *keyid*

For broadcast and multicast server modes, you must associate the specified key with the server at the server.

Table 8-11 Associate the specified key with the NTP server

Operation	Command
In broadcast server mode, associate the specified key with the NTP server.	**ntp-service broadcast-server authentication-keyid** *keyid*
In multicast server mode, associate the specified key with the NTP server.	**ntp-service multicast-server authentication-keyid** *keyid*

8.2.3 Setting the Interface for the Local to Transmit NTP Messages

When specifying the local end to transmit all the NTP messages, the source IP addresses in all the packets use only one specified IP address, which is obtained from the specified interface.

Perform the following operations in system view.

Table 8-12 Set the interface for the local to transmit NTP messages

Operation	Command
Set the interface for the local to transmit NTP messages	**ntp-service source-interface** *interface-type interface-number*
Remove the interface for the local to transmit NTP messages	**undo ntp-service source-interface**

The interface is determined by the *interface-type interface-number* arguments. The source IP addresses in the packets are obtained from the interface. If the command **ntp-service unicast-server** or **ntp-service unicast-peer** has specified the transmitting interface, it will be taken as the transmitting interface.

8.2.4 Setting the Local Clock as the NTP Master Clock

Perform the following operations in system view.

Table 8-13 Set the local clock as the NTP master clock

Operation	Command
Set the local clock as the NTP master clock	**ntp-service refclock-master** [*X.X.X.X*] [*layers-number*]
Remove the NTP master clock setting	**undo ntp-service refclock-master** [*X.X.X.X*]

The parameter *X.X.X.X* is the IP address of the reference clock, which is 127.127.1.u. The stratum number of the NTP master clock can be specified. The argument *layers-number* is used to specify the stratum number of the local clock, which is in the range of 1 to 15 and defaults to 8. When no IP address is specified, the local clock is the NTP master clock by default.

8.2.5 Configuring an Interface to Receive NTP Messages

The following configuration is used to enable or disable an interface to receive the NTP messages.

Perform the following operations in interface view.

Table 8-14 Enable/disable an interface to receive NTP messages

Operation	Command
Disable an interface to receive NTP messages	**ntp-service in-interface disable**
Enable an interface to receive NTP messages	**undo ntp-service in-interface disable**

These configurations must be configured on the interface disabled/enabled to receive NTP messages.

8.2.6 Setting Access Control Authority of the Local Router Services

The following configuration is used to set the access authority of the NTP service of the local router. This is only a low level security approach. The more secure approach is to perform ID authentication. When there is an access request, this command can be used to make the matches in sequence in a way from the minimum access authority to the maximum authority. All matches are based on the first match. The match order is **peer**, **server**, **server only(synchronization)**, and **query only**.

Perform the following operations in system view.

Table 8-15 Set the access authority of the NTP service of the local router

Operation	Command
Set the access authority of the NTP service of the local router	**ntp-service access** { **query** | **synchronization** | **server** | **peer** } *acl-number*
Remove the access authority of the NTP service of the local router	**undo ntp-service access** { **query** | **synchronization | server | peer** }

The range of the *access-list-number* is 2000 to 2999. Meanings of other access authorities include:

query : Query can be performed only on the local NTP service.

synchronization: Time request can be performed only on the local NTP service.

Server: Time request and query can be performed on the local NTP service but the local clock can not be synchronized to the remote server.

Peer: Time request and query can be performed on the local NTP service and the local clock can be synchronized to the remote server.

8.2.7 Setting Number of Sessions Allowed to be Established Locally

The following configuration is used to set the number of sessions allowed to establish locally.

Perform the following operations in system view.

Table 8-16 Set the number of sessions allowed to be established locally

Operation	Command
Set the number of sessions allowed to be established locally	**ntp-service max-dynamic-sessions** *number*
Restore the default number of sessions allowed to be established locally	**undo ntp-service max-dynamic-sessions**

The *number* of the sessions allows to be established locally is in the range of 0 to 100. It is 100 by default.

8.3 Displaying and Debugging

After the above configuration, execute the **display** command in any view to display the running of the NTP, and to verify the configuration.

Perform the configuration of the **debugging** command in user view.

Table 8-17 NTP monitoring and maintenance

Operation	Command
Display the state information of the NTP service	**display ntp-service status**
Display the association state of the NTP service maintenance	**display ntp-service sessions** [**verbose**]
Display the summary information of each NTP time server from the local device tracing to the reference clock source	**display ntp-service trace**
Enable NTP debugging	**debugging ntp-service** { **all** | **access** | **adjustment** |**authentication** | **event** | **filter** | **packet** | **parameter** | **refclock** | **selection** | **synchronization** | **validity** }

Note:

The picture of the time synchronization path drawn by the **display ntp-service trace** command is complete only when all NTP servers on the path can be pinged.

8.4 NTP Typical Configuration Examples

8.4.1 Configuring NTP Server

I. Network requirements

3Com1 sets the local clock as the NTP master clock and the stratum number is 2. 3Com2 takes 3Com1 as the time server and set it to server mode. 3Com2 sets itself as client mode.

II. Network diagram

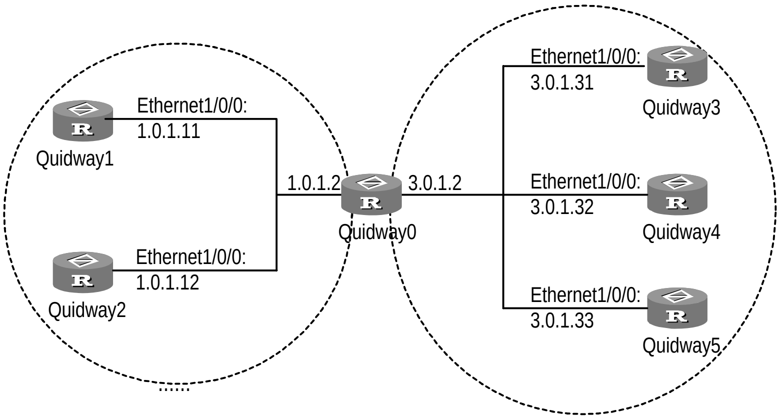


Figure 8-2 NTP typical configuration network diagram

III. Configuration procedure

1) Configure 3Com1

# Enter the system view.

```
<3Com1> system-view
```

# Set the local clock as the NTP master clock and the stratum number is 2.

```
[3Com1] ntp-service refclock-master 2
```

2) Configure 3Com2

# Enter the system view.

```
<3Com2> system-view
```

# Set 3Com1 as the time server.

```
[3Com2] ntp-service unicast-server 1.0.1.11
```

The above configurations synchronize the time of 3Com2 and 3Com1. The state of 3Com2 before synchronization includes:

```
[3Com2] display ntp-service status
Clock status: unsynchronized
 Clock stratum: 16
 Reference clock ID: none
 Nominal frequency: 99.8562 Hz
 Actual frequency: 99.8562 Hz
 Clock precision: 2^17
 Clock offset: 0.0000 ms
 Root delay: 0.00 ms
 Root dispersion: 0.00 ms
 Peer dispersion: 0.00 ms
 Reference time: 00:00:00.000 UTC Jan 1 1900(00000000.00000000)
```

The state of 3Com2 after synchronization includes:

```
[3Com2] display ntp-service status
Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 1.0.1.11
 Nominal frequency: 250.0000 Hz
 Actual frequency: 249.9992 Hz
 Clock precision: 2^19
 Clock offset: 198.7425 ms
 Root delay: 27.47 ms
 Root dispersion: 208.39 ms
 Peer dispersion: 9.63 ms
 Reference time: 17:03:32.022 UTC Thu Sep 6 2001 (BF422AE4.05AEA86C)
```

Now 3Com2 is synchronized with 3Com1. Its stratum number is 3, higher than that of 3Com1 by one.

The association state of 3Com2 displays that 3Com2 has established connection with 3Com1.

```
[3Com2] display ntp-service sessions
       source     reference     stra  reach  poll  now  offset  delay  disper
*******************************************************************
[12345]1.0.1.11    127.127.1.0    2      1    64    377    26.1    199.53    9.7
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

8.4.2 Configure NTP Peer Examples

I. Network requirements

3Com3 sets the local clock as the NTP master clock and the stratum number is 2. 3Com4 sets 3Com3 as the time server and sets it to server mode. 3Com4 sets itself as client mode. 3Com5 sets 3Com4 as the peer.

II. Network diagram

See Figure 8-2.

III. Configuration procedure

1) Configure 3Com3

# Enter the system view.

```
<3Com3> system-view
```

# Set the local clock as the NTP master clock and the stratum number is 2.

```
[3Com3] ntp-service refclock-master 2
```

2) Configure 3Com4

# Enter the system view.

```
<3Com4> system-view
```

# Set 3Com3 as the time server and the stratum number is 3 after synchronization.

```
[3Com4] ntp-service unicast-server 3.0.1.31
```

3) Configure 3Com5 (3Com4 has been synchronized to 3Com3)

# Enter the system view.

```
<3Com5> system-view
```

# Set the local clock as the NTP master clock and stratum number is 1.

```
[3Com5] ntp-service refclock-master 1
```

# Set 3Com4 peer after the local is synchronized.

```
[3Com5] ntp-service unicast-peer 3.0.1.32
```

The above configurations make 3Com4 and 3Com5 as peers. 3Com5 is in active peer mode and 3Com4 is in passive peer mode. Because the stratum number of 3Com5 is 1 and that of 3Com4 is 3, 3Com4 is synchronized to 3Com5.

The state of 3Com4 includes:

```
[3Com4] display ntp-service status
Clock status: synchronized
 Clock stratum: 2
 Reference clock ID: 3.0.1.33
 Nominal frequency: 250.0000 Hz
 Actual frequency: 249.9992 Hz
 Clock precision: 2^19
 Clock offset: 198.7425 ms
 Root delay: 27.47 ms
 Root dispersion: 208.39 ms
 Peer dispersion: 9.63 ms
 Reference time: 17:03:32.022 UTC Thu Sep 6 2001 (BF422AE4.05AEA86C)
```

Now 3Com4 is synchronized with 3Com5. Its stratum number is 2, which is 1 number larger than that of 3Com5.

The association state of 3Com4 displays that 3Com4 has established connection with 3Com5.

```
[Quidwa4] display ntp-service sessions
       source       reference   stra  reach  poll  now  offset  delay  disper
********************************************************************
[12345]3.0.1.33   127.127.1.0    2      1     64    377   26.1   199.53  9.7
```

note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured

8.4.3 Configuring NTP Broadcast Mode

I. Network requirements

3Com3 sets the local clock as the NTP master clock and the stratum number is 2. It transmits broadcast packets from Ethernet 1/0/0. 3Com4 and 3Com1 are set to listen to the broadcast message from their interfaces respectively.

II. Network diagram

See Figure 8-2.

III. Configuration procedure

1) Configure 3Com3

# Enter the system view.

```
<3Com3> system-view
```

# Set the local clock as the NTP master clock and the stratum number is 2.

```
[3Com3] ntp-service refclock-master 2
```

# Enter the interface Ethernet 1/0/0 view.

```
[3Com3] interface ethernet 1/0/0
```

# Set the broadcast server.

```
[3Com3-Ethernet1/0/0] ntp-service broadcast-server
```

2) Configure 3Com4

# Enter the system view.

```
<3Com4> system-view
```

# Enter the interface Ethernet 1/0/0 view.

```
[3Com4] interface ethernet 1/0/0
[3Com4-Ethernet1/0/0] ntp-service broadcast-client
```

3) Configure 3Com1

# Enter the system view.

```
<3Com1> system-view
```

# Enter the interface Ethernet 1/0/0 view.

```
[3Com1] interface ethernet 1/0/0
[3Com1-Ethernet1/0/0] ntp-service broadcast-client
```

In the above configuration, 3Com4 and 3Com1 are configured to listen to broadcast messages from Ethernet 1/0/0 and 3Com3 is configured to transmit broadcast packets from Ethernet 1/0/0. Because 3Com1 and 3Com3 are on different network segment, 3Com1 cannot receive the broadcast packets transmitted by 3Com3. 3Com4 is synchronized with 3Com3 after receiving the broadcast packets transmitted by 3Com3.

The state of 3Com4 after synchronization includes:

```
[3Com4] display ntp-service status
Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 3.0.1.31
 Nominal frequency: 250.0000 Hz
 Actual frequency: 249.9992 Hz
 Clock precision: 2^19
 Clock offset: 198.7425 ms
 Root delay: 27.47 ms
 Root dispersion: 208.39 ms
 Peer dispersion: 9.63 ms
 Reference time: 17:03:32.022 UTC Thu Sep 6 2001 (BF422AE4.05AEA86C)
```

Now 3Com4 is synchronized with 3Com3. Its stratum number is 3, which is 1 number larger than that of 3Com3.

The association state of 3Com4 displays that 3Com4 has established connection with 3Com3.

```
[3Com2] display ntp-service sessions
       source      reference    stra  reach  poll  now  offset  delay  disper
********************************************************************
[12345]1.0.1.11   127.127.1.0    2     1     64    377   26.1    199.53  9.7
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

8.4.4 Configuring NTP Broadcast Mode with ID Authentication

I. Network requirements

3Com3 sets the local clock as the NTP master clock and the stratum number is 3. It transmits broadcast packets from Ethernet1/0/0. 3Com4 is set to listen to the broadcast message from Ethernet1/0/0.

II. Network diagram

See Figure 8-2.

III. Configuration procedure

1) Configure 3Com3

# Enter the system view.

```
<3Com3> system-view
```

# Set the local clock as the NTP master clock and the stratum number is 3.

```
[3Com3] ntp-service refclock-master 3
```

# Enable the authentication function.

```
[3Com3] ntp-service authentication enable
```

# Set NTP authentication key.

```
[3Com3] ntp-service authentication-keyid 88 authentication-mode md5 123456
```

# Set the local authentication key as reliable.

```
[3Com3] ntp-service reliable authentication-keyid 88
```

# Enter the interface Ethernet1/0/0 view.

```
[3Com3] interface ethernet 1/0/0
```

# Set the local router as NTP broadcast server and specify authentication ID.

```
[3Com3-Ethernet1/0/0] ntp-service broadcast-server authentication-id 88
```

2) Configure 3Com4

# Enter the system view.

```
<3Com4> system-view
```

# Enable the authentication function.

```
[3Com4] ntp-service authentication enable
```

# Set NTP authentication key.

```
[3Com4] ntp-service authentication-keyid 88 authentication-mode md5 123456
```

# Set the local authentication key as reliable.

```
[3Com4] ntp-service reliable authentication-keyid 88
```

# Enter the interface Ethernet1/0/0 view.

```
[3Com4] interface ethernet 1/0/0
```

# Set the local router as NTP broadcast Client.

```
[3Com4-Ethernet1/0/0] ntp-service broadcast-client
```

In the above configuration, 3Com4 is configured to listen to broadcast messages from Ethernet1/0/0 and 3Com3 is configured to transmit broadcast packets from Ethernet1/0/0. 3Com4 is synchronized with 3Com3 after receiving the broadcast packets transmitted by 3Com3.

The state of 3Com4 after synchronization includes:

```
<3Com4> display ntp-service status
clock status: synchronized
clock stratum: 4
reference clock ID: 3.0.1.31
nominal frequency: 250.0000 Hz
actual frequency: 249.9992 Hz
clock precision: 2^19
clock offset: 198.7425 ms
root delay : 27.47 ms
root disper: 208.39 ms
peer disper: 9.63 ms
```

```
reference time: 17:03:32.022 UTC Sep 6 2003(BF422AE4.05AEA86C)
```

Now 3Com4 is synchronized with 3Com3. Its stratum number is 4, higher than that of 3Com3 by one.

8.4.5 Configuring NTP Multicast Mode

I. Network requirements

3Com3 sets the local clock as the NTP master clock and the stratum number is 2. It transmits multicast packets from Ethernet 1/0/0. 3Com4 and 3Com1 are set to listen to the multicast message from their interfaces respectively.

II. Network diagram

See Figure 8-2

III. Configuration procedure

1) Configure 3Com3

# Enter system view.

```
<3Com3> system-view
```

# Set the local clock as the NTP master clock and the stratum number is 2.

```
[3Com3] ntp-service refclock-master 2
```

# Enter the interface Ethernet 1/0/0 view.

```
[3Com3] interface ethernet 1/0/0
```

# Set the multicast server.

```
[3Com3-Ethernet1/0/0] ntp-service multicast-server
```

2) Configure 3Com4

# Enter system view.

```
<3Com4> system-view
```

# Enter the interface Ethernet 1/0/0 view.

```
[3Com4] interface Ethernet 1/0/0
```

# Set the multicast client mode.

```
[3Com4-Ethernet1/0/0] ntp-service multicast-client
```

3) Configure 3Com1

# Enter system view.

```
<3Com1> system-view
```

# Enter the interface Ethernet 1/0/0 view.

```
[3Com1] interface ethernet 1/0/0
```

# Set the multicast client mode.

```
[3Com1-Ethernet1/0/0] ntp-service multicast-client
```

In the above configuration, 3Com4 and 3Com1 are configured to listen to broadcast messages from Ethernet 1/0/0 and 3Com3 is configured to transmit broadcast packets from Ethernet 1/0/0. Because 3Com1 and 3Com3 are on different network segment, 3Com1 cannot receive the broadcast packets transmitted by 3Com3. 3Com4 is synchronized with 3Com3 after receiving the broadcast packets transmitted by 3Com3.

The state of 3Com4 after synchronization includes:

```
[3Com4] display ntp-service status
Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 3.0.1.31
 Nominal frequency: 250.0000 Hz
 Actual frequency: 249.9992 Hz
 Clock precision: 2^19
 Clock offset: 198.7425 ms
 Root delay: 27.47 ms
 Root dispersion: 208.39 ms
 Peer dispersion: 9.63 ms
 Reference time: 17:03:32.022 UTC Thu Sep 6 2001 (BF422AE4.05AEA86C)
```

Now 3Com4 is synchronized with 3Com3. Its stratum number is 3, which is 1 number larger than that of 3Com3.

The association state of 3Com4 displays that 3Com4 has established connection with 3Com3.

```
[3Com4] display ntp-service sessions
       source      reference    stra  reach  poll  now  offset  delay  disper
********************************************************************
[12345]3.0.1.33    127.127.1.0    2     1     64    377   26.1    199.53   9.7
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
```

8.4.6 Configuring NTP Server Mode with ID Authentication

I. Network requirements

3Com1 sets the local clock as the NTP master clock and the stratum number is 2. 3Com2 sets 3Com1 as the time server and sets it to server mode. 3Com2 sets itself as client mode and adds ID authentication to it.

II. Network diagram

See Figure 8-2.

III. Configuration procedure

1) Configure 3Com1

# Enter the system view.

```
<3Com1> system-view
```

# Set the local clock as the NTP master clock and the stratum number is 2.

```
[3Com1] ntp-service refclcok-master 2
```

2) Configure 3Com2

# Enter the system view.

```
<3Com2> system-view
```

# Set 3Com1 as the time server.

```
[3Com2] ntp-service unicast-server 1.0.1.11 authentication-keyid 42
```

# Enable ID authentication.

```
[3Com2] ntp-service authentication enable
```

# Set the key.

```
[3Com2] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
```

# Specify the key as reliable.

```
[3Com2] ntp-service reliable authentication-keyid 42
```

The above configurations synchronize the time of 3Com2 and 3Com1. Because 3Com1 does not enable ID authentication, 3Com2 cannot be synchronized to 3Com1. Now the following configurations are added to 3Com1.

# Enable ID authentication.

```
[3Com1] ntp-service authentication enable
```

# Set the key.

```
[3Com1] ntp-service authentication-keyid 42 authentication-mode md5 aNiceKey
```

# Specify the key as reliable.

```
[3Com1] ntp-service reliable authentication-keyid 42
```

Now 3Com2 can be synchronized to 3Com1. The state of 3Com2 includes:

```
<3Com2> display ntp-service status
clock status: synchronized, stratum: 3, reference clock ID: 1.0.1.11
nominal freq: 250.0000 Hz, actual freq: 249.9992 Hz, precision: 2**19
offset: 198.7425 ms, reftime: 17:03:32.022 UTC Thu Sep 6 2001
(BF422AE4.05AEA86C)
root delay : 27.47 ms, root disper: 208.39 ms, peer disper: 9.63 ms
Clock status: synchronized
 Clock stratum: 3
 Reference clock ID: 1.0.1.11
 Nominal frequency: 250.0000 Hz
 Actual frequency: 249.9992 Hz
 Clock precision: 2^19
 Clock offset: 198.7425 ms
 Root delay: 27.47 ms
 Root dispersion: 208.39 ms
 Peer dispersion: 9.63 ms
 Reference time: 17:03:32.022 UTC Thu Sep 6 2001 (BF422AE4.05AEA86C)
```

Now 3Com2 is synchronized with 3Com1. Its stratum number is 3, higher number larger than that of 3Com1 by one.

8.4.7 Configuring Server/Client Time Synchronization for MPLS VPN

I. Network requirements

As shown in the following figure,

- Two VPNs, VPN 1 and VPN 2 represented by a red curve and a blue curve respectively, on both PE1 and PE 2.
- CE 1 and CE 2 are located in VPN 1 and CE 3 and CE 4 in VPN 2.

Configure the devices to achieve these goals:

- CE 2 synchronizes CE 1.
- CE 1 synchronizes to the local clock source, and functions at stratum 1.

Note:

At present, NTP can provide only unitcast synchronization (in server/client or peer-to-peer model) for MPLS VPNs.

II. Network diagram

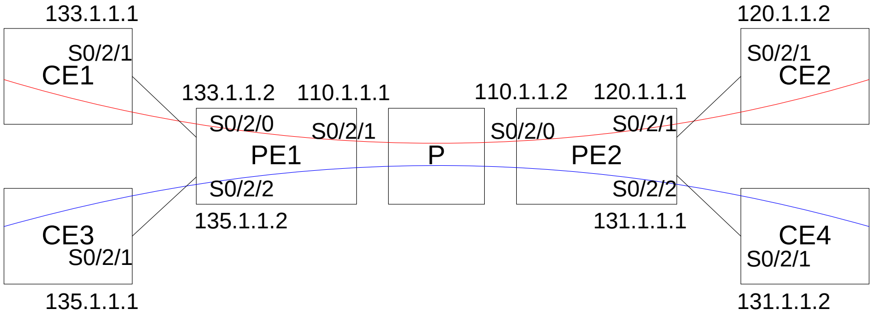


Figure 8-3 Network diagram for time synchronization on an MPLS VPN

III. Configuration procedure

Note:

This example assumes that:

- MPLS VPN configuration is complete.
- CE 1 and PE 1 can ping each other, so can PE 1 and PE 2, and PE 2 and CE 2.

1) Configure CE 1

# Set the local clock to function as the NTP master clock at stratum 1.

```
<CE1> system-view
[CE1] ntp-service refclcok-master 1
```

2) Configure CE 2

# Set CE 1 in VPN 1 as the NTP server for CE 2.

```
<CE2> system-view
[CE2] ntp-service unicast-server 133.1.1.1
```

# Display information about NTP sessions and status.

```
[CE2] display ntp-service status
 Clock status: synchronized
 Clock stratum: 2
 Reference clock ID: 133.1.1.1
 Nominal frequency: 63.9100 Hz
 Actual frequency: 63.9100 Hz
 Clock precision: 2^7
 Clock offset: 0.0000 ms
 Root delay: 47.00 ms
 Root dispersion: 0.18 ms
 Peer dispersion: 34.29 ms
 Reference time: 02:36:23.119 UTC Jan 1 2001(BDFA6BA7.1E76C8B4)
[CE2] display ntp-service sessions
        source       reference     stra reach poll  now offset  delay disper
**************************************************************************
[12345]133.1.1.1       LOCL         1    7   64   15    0.0   47.0    7.8
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
[CE2]  display ntp-service trace
 server 127.0.0.1,stratum 2, offset -0.013500, synch distance 0.03154
 server 133.1.1.1,stratum 1, offset -0.506500, synch distance 0.03429
 refid LOCL
```

You may find out that CE 2 has synchronized to CE 1 and is functioning at stratum 2.

8.4.8 Configuring Symmetric Time Synchronization for MPLS VPN

I. Network requirements

Configure devices to achieve these goals:

- PE 2 synchronizes to PE 1.
- PE 1 synchronizes to local clock source at stratum 1.

II. Network diagram

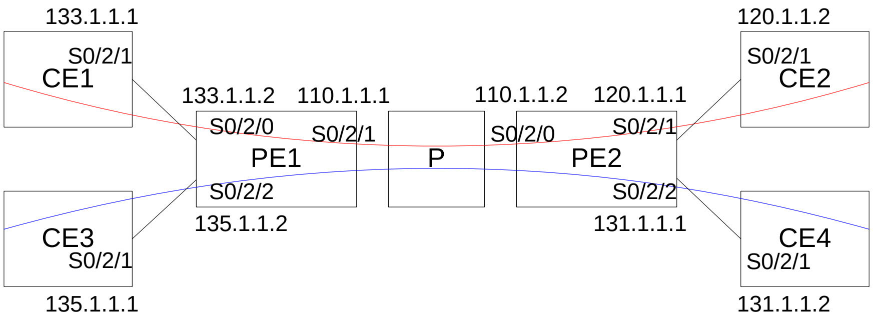


Figure 8-4 Network diagram for time synchronization on an MPLS VPN

III. Configuration procedure

1) Configure PE 1

# Set the local clock to function as the NTP master clock at stratum 1.

```
<PE1> system-view
[PE1] ntp-service refclcok-master 1
```

2) Configure PE 2

# Set PE 1 in VPN 1 as the NTP server for PE 2.

```
<PE2> system-view
[PE2] ntp-service unicast-peer vpn-instance vpn1 133.1.1.2
```

# Display information about NTP sessions and status.

```
[PE2] display ntp-service status
 Clock status: synchronized
  Clock stratum: 2
  Reference clock ID: 133.1.1.2
  Nominal frequency: 63.9100 Hz
  Actual frequency: 63.9100 Hz
  Clock precision: 2^7
  Clock offset: 0.0000 ms
  Root delay: 32.00 ms
  Root dispersion: 0.60 ms
  Peer dispersion: 7.81 ms
  Reference time: 02:44:01.200 UTC Jan 1 2001(BDFA6D71.33333333)
```

```
[PE2] display ntp-service sessions
        source        reference      stra reach poll  now offset  delay disper
**************************************************************************
[12345]133.1.1.2       LOCL         1    1   64   29    -12.0   32.0    15.6
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
[PE2] display ntp-service trace
 server 127.0.0.1,stratum 2, offset -0.012000, synch distance 0.02448
  server 133.1.1.2,stratum 1, offset 0.003500, synch distance 0.00781
  refid LOCL
```

You may find out that PE 2 has synchronized to PE 1 and is functioning at stratum 2.

The NTP configuration on PE2 however is different if CE 1 is the clock source. To have PE 2 synchronize to CE 1, you need to specify a source address in addition to specifying the VPN where CE 1 is located by using the following command:

```
[PE2] ntp-service unicast-server vpn-instance vpn1 133.1.1.1 source-interface
loopback1
```

Chapter 9 SNMP Configuration

9.1 Protocol Introduction

9.1.1 Brief Introduction

Currently, the most widely used network management protocol in computer network is Simple Network Management Protocol (SNMP), which is an applicable industrial standard adopted widely. Its purpose is to ensure the transmission of management information between any two points so that the network administrator can retrieve the information at any point on the network and perform appropriate modification, troubleshooting, fault diagnosis, and volume planning and reporting. It adopts a polling mechanism and offers an underlying function set, which is appropriate especially in a small environment in need of high speed and low cost. It only requires unacknowledged transport layer protocol UDP and is widely supported by a variety of products.

Structurally, SNMP can be divided into two parts, NMS and AGENT. The NMS (Network Management Station) is a workstation on which the client program is running. Currently, commonly used network management platforms are Sun NetManager and IBM NetView while the AGENT is a server-side software running on a network device. The NMS can send packets of GetRequest, GetNextRequest, Getbulk, or SetRequest to the AGENT. Once the AGENT receives request packets from the NMS, it will perform read or write operations on variables being managed according to the type of the packets and generate a Response packet to return to the NMS. On the other hand, if any exception happens to the device, like a hot or cold start, the AGENT also can send a Trap packet to the NMS on its own initiative, reporting the event happened.

9.1.2 SNMP Versions and MIB

In order to identify a management variable uniquely in the SNMP packets, SNMP uses a hierarchical naming convention to distinguish different managed objects and the hierarchical structure is like a tree with its nodes representing managed objects. Displayed in the diagram below, a managed object can be identified uniquely by the path from the root to the node representing it.

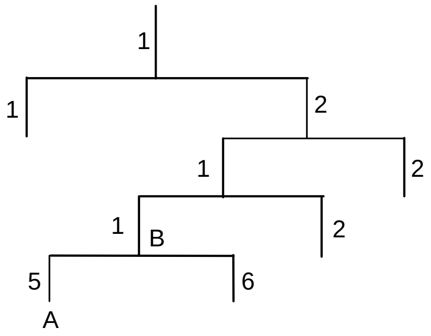


Figure 9-1 MIB tree structure

In the diagram above, the managed object B can be uniquely determined by a string of digits {1.2.1.1}, which is the Object Identifier of the managed object. While the MIB (Management Information Base) is used to describe the hierarchical structure of the tree and is a collection of the definitions of standard variables on monitored network devices.

Currently, the SNMP Agent in router system supports SNMP V3 and is compatible with SNMP V1 and SNMP V2C. Its supported MIB is displayed in the table below.

Table 9-1 MIB supported by router system

MIB Property	Contents of MIB	Standard or Specification
Public MIB	MIB II based on TCP/IP network devices	RFC1213
	RIP-2 MIB	RFC1724
	Ethernet MIB	RFC 2665, RFC2668
	PPP MIB	RFC 1471, RFC1473
	OSPF MIB	RFC1253
	BGP MIB	RFC1657
	IF MIB	RFC1573
	SNMPV2 MIB	RFC1907
	Framework MIB	RFC2571
	Usm MIB	RFC2573
	Mpd MIB	RFC2572
	Vacm MIB	RFC2275
	Target MIB	RFC2273
	Notification MIB	RFC2273
	RADIUS MIB	RFC2618, RFC2620

MIB Property	Contents of MIB	Standard or Specification
Private MIB	Performance trap MIB	—
	Device panel MIB	—
	Device resource MIB	—
	VLAN	—
	QoS	—

9.2 SNMP Configuration

The SNMP configuring includes:

- Set the SNMP Agent service
- Set the corresponding versions of SNMP
- Set community name
- Set an SNMP group
- Set an SNMP user
- Set sysContact
- Set sending Trap
- Set the engine ID of a local device
- Set the address of the Trap destination host
- Set sysLocation
- Set the source address for sending Traps
- Set a view
- Set packet queue length of Trap sent to destination host
- Set the saving time of Trap packets
- Set the maximum size of SNMP packets that an agent can receive or send

9.2.1 Setting the SNMP Agent Serve

This configuration is used to enable the SNMP Agent serve, which is disabled by default.

Perform the following operations in the system view.

Table 9-2 Set the SNMP Agent serve

Operation	Command
Enable the SNMP Agent serve	**snmp-agent**
Disable the SNMP Agent serve	**undo snmp-agent**

9.2.2 Setting the Corresponding Versions of SNMP

This configuration is used to enable the corresponding version of SNMP and the SNMP V3 is enabled by default. Therefore the command needs to be configured to enable SNMP V1 and SNMP V2C.

Perform the following operations in the system view.

Table 9-3 Set the corresponding version of SNMP

Operation	Command
Enable the corresponding version of SNMP	**snmp-agent sys-info version** { { **v1** | **v2c** | **v3** } * | **all** }
Disable the corresponding version of SNMP	**undo snmp-agent sys-info version** { { **v1** | **v2c** | **v3** } * | **all** }

"*" indicates to select several versions from **v1**, **v2c** and **v3**, with one at least and all three at most.

Example: Enable version SNMP V2C and SNMP V3.

```
[3Com] snmp-agent sys-info version v3 v2c
```

Example: Disable version SNMP V2C and SNMP V1.

```
[3Com] undo snmp-agent sys-info version v1 v2c
```

9.2.3 Setting the Community Name

SNMPV1, SNMPV2C use community names for authentication and SNMP packets that do not match the authenticated community name of the device will be dropped. An SNMP community is named with a character string called Community Name. Different communities can have **read** or **write** access mode. A community with the privilege of **read** can only perform queries on device information and a community with the privilege of **write** can configure the devices additionally.

Perform the following operations in the system view.

Table 9-4 Set the Community Name

Operation	Command
Set a community name and its access privilege	**snmp-agent community** { **read** | **write** } *community-name* [[**mib-view** *view-name*] | [**acl** *acl-number*]]*
Remove a community name previously set	**undo snmp-agent community** *community-name*

If you perform configuration on a community name more than once, the attribute last configured will be adopted.

# Set the public community to read privilege.

```
[3Com] snmp-agent community read public
```

# Set the private community to write privilege.

```
[3Com] snmp-agent community write private
```

9.2.4 Setting the SNMP Group

This configuration can be used to set and delete an SNMP group.

Perform the following operations in the system view.

Table 9-5 Set the SNMP group

Operation	Command
Set an SNMP group	**snmp-agent group** { **v1** | **v2c** } *group-name* [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**acl** *acl-number*] **snmp-agent group** { **v1** | **v2c** } *group-name* **acl** *acl-number* **snmp-agent group v3** *group-name* [**authentication** | **privacy**] [**read** *read-view*] [**write** *write-view*] [**notify** *notify-view*] [**acl** *acl-number*] **snmp-agent group v3** *group-name* **acl** *acl-number*
Delete an SNMP group	**undo snmp-agent group** { **v1** | **v2c** } *group-name* **undo snmp-agent group v3** *group-name* [**authentication** | **privacy**]

9.2.5 Setting the SNMP User

This configuration can be used to add or delete a new user to the SNMP group.

Perform the following operations in the system view.

Table 9-6 Set the SNMP user

Operation	Command
Add a new user to the SNMP group	**snmp-agent usm-user** { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number*] **snmp-agent usm-user v3** *user-name group-name* [[**authentication-mode** { **md5** | **sha** } *auth-password*] [**privacy des56** *priv-password*]] [**acl** *acl-number*]

Operation	Command
Delete a user from the SNMP group	**undo snmp-agent user** { **v1** | **v2c** } *user-name group-name* **undo snmp-agent user v3** *user-name group-name* [**engineid** *engine-id* | **local**]

# Add a user "John" to SNMP group "Johngroup", with security level being authentication-mode, the specified authentication protocol being "HMAC-MD5-96", and the authentication password being "hello".

```
[3Com] snmp-agent usm-user v3 John Johngroup authentication-mode md5 hello
```

9.2.6 Setting the ID and Contact of the Administrator

*S*ystem contact is a management variable of the group *system* in MIB II and it contains the ID and contact of relevant administrator of the managed devices (router). Through configuring this parameter, the user can store the important information in the router so as to query when emergency occurs.

Perform the following operations in the system view.

Table 9-7 Set the ID and contact of the administrator

Operation	Command
Set the ID and contact of the administrator	**snmp-agent sys-info contact** *sysContact*
Restore the ID and contact of the administrator to default values	**undo snmp-agent sys-info contact**

# Use the following command to set the ID and contact.

```
[3Com] snmp-agent sys-info contact Mr.zhang 13800138002.
```

9.2.7 Setting the Sending Trap

Traps are pieces of information sent to the NMS by the agent without being solicited, reporting some emergent and significant events.

Perform the following operations in the system view.

Table 9-8 Set the sending Trap

Operation	Command
Enable sending Trap	**snmp-agent trap enable** [*trap-type* [*trap-list*]]

Operation	Command
Disable sending Trap	**undo snmp-agent trap enable** [*trap-type* [*trap-list*]]

By default, trap sending is allowed.

The command **snmp-agent trap enable** without parameter indicates allowing sending Trap of all types in all modules.

9.2.8 Setting the Engine ID of a Local Device

This configuration can be used to set the engine ID of a local device. The ID is a string of 10 to 64 hexadecimal numbers and its default value is the company's enterprise number plus the device information, which can be an IP address, an MAC address or a self-defined text.

Perform the following operations in the system view.

Table 9-9 Set the engine ID of a local device

Operation	Command
Set the engine ID of a device	**snmp-agent local-engineid** *engineid*
Set the engine ID of a device to the default value	**undo snmp-agent local-engineid**

9.2.9 Setting the Address of the Trap Target Host

Perform the following operations in the system view.

Table 9-10 Set/remove the address of the destination host for receiving Trap packets

Operation	Command
Set the address of the destination host for receiving Trap packets	**snmp-agent target-host trap address udp-domain** *X.X.X.X* [**udp-port** *port-number*] [**vpn-instance** *vpn-name*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]
Remove the address of the destination host for receiving Trap packets	**undo snmp-agent target-host** *X.X.X.X* **securityname** *security-string*

# Use the following commandFor example, to set the address of the Trap target host to 202.38.160.6, using and to use the community name *public.*

```
[3Com] snmp-agent target-host trap address udp-domain 202.38.160.6 udp-port
5000 params securityname public
```

9.2.10 Setting the Router's Location (sysLocation)

The argument *sysLocation* is a management variable of the *system* group in MIB and stands for the location of a managed device.

Perform the following operations in the system view.

Table 9-11 Set the location of a router

Operation	Command
Set the location of the router	**snmp-agent sys-info location** *sysLocation*
Restore the location of the router to the default value	**undo snmp-agent sys-info location**

# Use the following command to set the physical location of the router to hwbj.

```
[3Com] snmp-agent sys-info location hwbj
```

9.2.11 Setting the Source Address for Sending Traps

This configuration can be used to specify the source address for sending Traps.

Perform the following operations in the system view.

Table 9-12 Set the source address for sending Trap packet

Operation	Command
Specify the source address for sending Traps	**snmp-agent trap source** *interface-type interface-number*
Remove the source address for sending Traps	**undo snmp-agent trap source**

# Use the following command to take the IP address of the Ethernet interface 1/0/0 as the source address of the Trap packet.

```
[3Com] snmp-agent trap source ethernet 1/0/0
```

9.2.12 Setting the SNMP View

These configurations can be used to establish, update or delete the view information.

Perform the following operations in the system view.

Table 9-13 Set the SNMP view

Operation	Command
Establish or update view information	**snmp-agent mib-view** { **included** | **excluded** } *view-name oid-tree*

Operation	Command
Delete a view	**undo snmp-agent mib-view** *view-name*

# Use the following command to establish a view named mib1 containing all the objects of Internet.

```
[3Com] snmp-agent mib-view included mib1 1.3.6.1
```

9.2.13 Setting the Maximum Size of SNMP Packets

This configuration can be used to set the maximum size of SNMP packets, which an Agent can receive or send.

Perform the following operations in the system view.

Table 9-14 Set the maximum size of SNMP packets that an Agent can receive or send

Operation	Command
Set the maximum size of SNMP packets that an Agent can receive or send	**snmp-agent packet max-size** *byte-count*
Restore the maximum size of SNMP packets to the default value	**undo snmp-agent packet max-size**

The range of the maximum size of SNMP packets that an Agent can receive or send is 484 to 17,940 bytes and the default size is 1500 bytes.

# Set the maximum size of SNMP packets that an Agent can receive or send as 1042 bytes.

```
[3Com] snmp-agent packet max-size 1042
```

9.2.14 Setting the Packet Queue Length of Trap Packet

The configuration can be used to set the packet queue length of the Trap packets sent to the destination host.

Perform the following operations in the system view.

Table 9-15 Set the packet queue length of Trap sent to destination host

Operation	Command
Set the packet queue length of the Trap packets sent to the destination host	**snmp-agent trap queue-size** *size*
Restore to the default value of the packet queue length	**undo snmp-agent trap queue-size**

The range of the packet queue length is 1 to 1000 with the default value as 100.

# Set the packet queue length of the host sending the Trap packets as 200.

```
[3Com] snmp-agent trap queue-size 200
```

9.2.15 Setting the Saving Time of Trap Packets

The configuration is used to set the saving time of Trap packets, and all the Trap packets exceeding this time will be deleted.

Perform the following operations in the system view.

Table 9-16 Set the saving time of Trap packets

Operation	Command
Set the saving time of Trap packets	**snmp-agent trap life** *seconds*
Restore to the default value of Trap packets saving time	**undo snmp-agent trap life**

The range of Trap packets saving time is 1 to 2592000, with the default value as 120 seconds.

# Set the saving time of Trap packets as 60 seconds.

```
[3Com] snmp-agent trap life 60
```

9.3 Displaying and Debugging

After the above configuration, execute the **display** command in any view to display the running of the SNMP configuration, and to verify the configuration, but the **debugging** command should be performed in the user view.

Table 9-17 Monitoring and maintenance of SNMP

Operation	Command
Display the versions enabled by SNMP	**display snmp-agent sys-info version**
Display the statistics of SNMP packets	**display snmp-agent statistics**
Display the engine ID of the current device	**display snmp-agent** { **local-engineid** | **remote-engineid** }
Display the group name, security mode, status of views, and storage modes of groups	**display snmp-agent group** [*group-name*]
Display all the SNMP user names in a group user name list	**display snmp-agent usm-user** [**engineid** *engineid* | **username** *user-name* | **group** *group-name*] *
Display the community name of the current configuration	**display snmp-agent community** [**read** | **write**]

Operation	Command
Display the MIB view of the current configuration	**display snmp-agent mib-view** [**exclude** | **include** | **viewname** *view-name*]
Display the character string of system contact	**display snmp-agent sys-info contact**
Display the character string of system location	**display snmp-agent sys-info location**
Display whether trap sending is enabled for each module	**display snmp-agent trap-list**
Enable SNMP debugging	**debugging snmp-agent** { **header** | **packets** | **trap** | **process** }

9.4 Example of Typical Configuration

I. Network requirements

Taking the diagram below as an example, a network management station with the IP address of 129.102.149.23 is connected to a router with the IP address of 129.102.0.1 via an Ethernet. NMS receives Trap packets at the port 5000 and the SNMP version is V1.

II. Network diagram

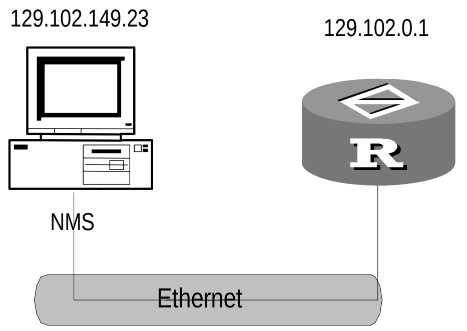


Figure 9-2 Configure SNMP

III. Configuration procedure

Step 1: Set the community name and its access privilege.

```
[3Com] snmp-agent community read public
[3Com] snmp-agent community write private
```

Step 2: Set the ID and contact of the administrator and the physical location of the router.

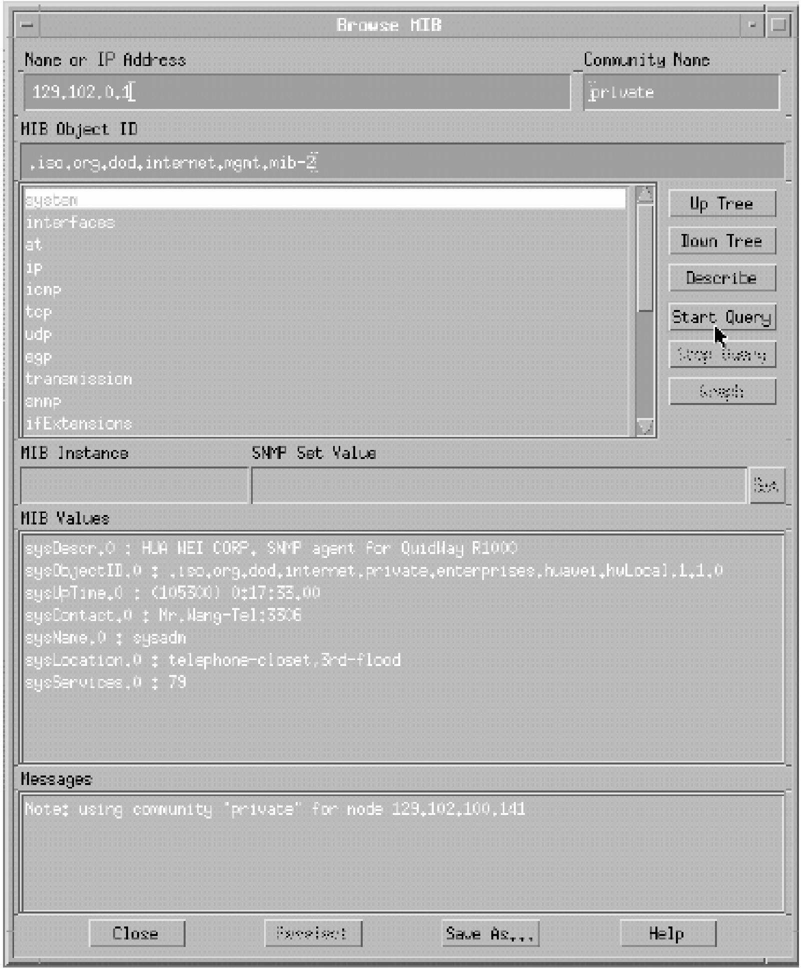
```
[3Com] snmp-agent sys-info contact Mr.Wang-Tel:3306
[3Com] snmp-agent sys-info location telephone-closet,3rd-floor
```

Step 3: Permit to send trap messages to the Network Management Station (NMS) 129.102.149.23, using public as the community name.

```
[3Com] snmp-agent trap enable
[3Com] snmp-agent target-host trap address udp-domain 129.102.149.23 udp-port
5000 params securityname public
```

IV. Using NMS

Take IBM xnmbrowser as an example. Set the Name of IP Address as 129.102.0.1 and the Community Name as **private**. Then, you can use the NMS Client program to perform queries and configuration operations on the router.



Name or IP Address: 129.102.0.1
Community Name: private
MIB Object ID: .iso.org.dod.internet.mgmt.mib-2

```
system
interfaces
at
ip
icmp
tcp
udp
egp
transmission
snmp
ifExtensions
```

MIB Instance
SNMP Set Value

MIB Values

```
sysDescr.0 : HUA WEI CORP. SNMP agent for QuidWay R1000
sysObjectID.0 : .iso.org.dod.internet.private.enterprises.huawei.hwLocal.1.1.0
sysUpTime.0 : (105300) 0:17:33.00
sysContact.0 : Mr.Wang-Tel:3306
sysName.0 : sysadm
sysLocation.0 : telephone-closet,3rd-flood
sysServices.0 : 79
```

Messages

```
Note: using community "private" for node 129.102.100.141
```

Figure 9-3 NMS user interface

As shown in Figure 9-3, enter the instance "iso.org.dod.internet.mgnt.mib-2.system" for query. Click <Start Query>to get the following results:

```
SysDescr.0 :  STRING: HUA WEI CORP. SNMP agent for 3Com Routers
```

```
SysUpTime.0 :     (105300) 00:17:33:00
SysContact.0 :    Mr.Wang-Tel:3306
SysName.0 :       sysadm
SysLocation.0 :   telephone-closet,3rd-floor
SysServices.0 :   79
```

If you cannot understand the meanings of these management variables in the MIB, you can get the related explanations just by clicking <Describe>.

Chapter 10 RMON Configuration

10.1 Introduction

Remote monitoring (RMON) is a kind of management information base (MIB) defined by Internet Engineering Task Force (IETF); it is the most important enhancement to MIB-II. RMON MIBs comprise sets of statistics data, analyzing data, and diagnostic data. Unlike a standard MIB which only provides the raw data about the managed objects for a port, RMON MIBs provide the statistics and resultant data about the entire network segment. RMON thus allows you to monitor traffic over a network segment and even the entire network.

RMON is implemented fully based on SNMP architecture, allowing for compatibility with the current simple network management protocol (SNMP) framework.

RMON comprises two parts: network management system (NMS) and the agents running on network devices. On the network monitor or probe for an interface, the RMON agent monitors the traffic over the segment connected to the interface. It can provide statistics about the traffic on the segment, such as the total number of packets over a specified period, and the number of correct packets to a specific host.

RMON enables SNMP to monitor remote network devices more effectively and proactively, increasing subnet monitoring efficiency. In addition, RMON decreases the traffic between network management stations and agents, simplifying the management of your network, especial when it is a large-scale internet.

RMON allows the presence of multiple managers. It provides two ways of data collection:

- Using RMON probes. An NMS can obtain management information from RMON probes directly and control the network resources. You can obtain all information in the RMON MIB by using this method.
- Embedding RMON agents in network devices such as routers, switches, or Hubs to have them provide the RMON probe function. When collecting network management information, RMON NMSs use basic SNMP commands to exchange data with SNMP agents. The amount of information collected is limited by the resources of network devices however. Instead of obtaining all data of RMON MIB, RMON NMSs only collect four groups of information in most cases: alarm, event, history, and statistics.

V 2.41 implements RMON in the second way. Through the RMON-capable SNMP agents on monitors, an NMS obtains information about the network segments connected to the interfaces on the administered network devices, such as the overall traffic, and statistics about errors and performance. Thus, it can administer the entire network.

10.2 RMON Configuration

Note:

To allow an NMS to administer your router, you must configure SNMP agents before configuring RMON on the router. Then, you can retrieve alarms and logs about the router on the NMS.

RMON configuration tasks are described in the following sections:

- Adding/Removing an Event Entry
- Adding/Removing an Alarm Entry
- Adding/Removing a History Control Entry
- Adding/Removing a Prialarm Entry
- Adding/Removing a Statistics Entry

10.2.1 Adding/Removing an Event Entry

You can set an event entry and specify the action taken when the event is triggered by an alarm:

- Generate a log entry.
- Send a trap to the NMS.
- Generate a log entry and send a trap to the NMS.

Perform the following configuration in system view.

Table 10-1 Add/remove an event entry

Operation	Command
Add an event entry	**rmon event** *event-entry* [**description** *string*] { **log** | **trap** *trap-community* | **log-trap** *log-trapcommunity* | **none** } [**owner** *text*]
Remove an event entry	**undo rmon event** *event-entry*

10.2.2 Adding/Removing an Alarm Entry

The alarm group of RMON can monitor the specified alarm variables such as statistics about an interface. When the value of the monitored variable exceeds the specified threshold, an alarm is triggered. The alarm in turns trigger an event, which is defined in the event group.

📖 **Note:**

Before adding an alarm entry, you need to define its associated event with the **rmon event** command.

Perform the following configuration in system view.

Table 10-2 Add/remove an alarm entry

Operation	Command
Add an alarm entry	**rmon alarm** *alarm-entry alarm-variable sampling-time* { **delta** | **absolute** } **rising_threshold** *threshold-value1 event-entry1* **falling_threshold** *threshold-value2 event-entry2* [**owner** *text*]
Remove an alarm entry	**undo rmon alarm** *alarm-entry*

After you set the alarm entry, the system does the following:

1) Sample the defined alarm variables at the specified interval.
2) Compare each sample with the thresholds: if the value of the sample exceeds the rising threshold or is below the falling threshold, trigger the associated event.

10.2.3 Adding/Removing a History Control Entry

The history group of RMON can collect historical data and periodically collect and save data on interfaces, providing information such as utilization, number of errors, and total number of packets for later retrieval.

Perform the following configuration in Ethernet interface view.

Table 10-3 Add/remove a history control entry

Operation	Command
Add a history control entry	**rmon history** *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *text-string*]
Remove a history control entry	**undo rmon history** *entry-number*

History control entries record periodic statistical samples. To view information about the history table of RMON or a specified history entry, use the **display rmon history** command.

10.2.4 Adding/Removing a Prialarm Entry

Prialarm entries can operate on the samples of the monitored variables according to the defined calculating formula and compare the resultant values with the predefined thresholds. You can thus obtain more alarm functions.

🕮 **Note:**

Before adding a prialarm entry, you need to define its associated event with the **rmon event** command.

Perform the following configuration in system view.

Table 10-4 Add/remove a prialarm entry

Operation	Command
Add a prialarm entry	**rmon prialarm** *prialarm-entry prialarm-formula prialarm-des sampling-timer* { **delta | absolute | changeratio** } **rising_threshold** *threshold-value1 event-entry1* **falling_threshold** *threshold-value2 event-entry2* **entrytype** { **forever | cycle** *cycle-period* } [**owner** *text*]
Remove a prialarm entry	**undo rmon prialarm** *entry-number*

After you set the alarm entry, the system does the following:

1) Sample the defined alarm variables at the specified interval.
2) Operate on each sample according to the defined calculating formula.
3) Compare the result with the thresholds: if the value of the sample exceeds the rising threshold or is below the falling threshold, trigger the associated event.

10.2.5 Adding/Removing a Statistics Entry

The statistics group of RMON monitors the use of an interface and count the errors, providing statistics about collision, CRC and queues, undersize and oversize packets, timeout, fragments, broadcast, multicast, and unicast, and bandwidth utilization.

Perform the following configuration in Ethernet interface view.

Table 10-5 Add/remove a statistics entry

Operation	Command
Add a statistics entry	**rmon statistics** *entry-number* [**owner** *text-string*]

Operation	Command
Remove a statistics entry	**undo rmon statistics** *entry-number*

A statistics entry holds the accumulative value since the corresponding event is defined. You can check information about the statistics table of RMON or the specified statistics entry with the **display rmon statistics** command.

10.2.6 Displaying and Debugging RMON

After completing the above configuration, you can execute the **display** command in any view to display information about RMON's statistics table, history control table, alarm table, prialarm table, event table, and event table.

Table 10-6 Display and debug RMON

Operation	Command
Display the statistics table of RMON	**display rmon statistics** [*interface-type interface-number*]
Display the history control table of RMON	**display rmon history** [*interface-type interface-number*]
Display the alarm table of RMON	**display rmon alarm** [*alarm-entry*]
Display the prialarm table of RMON	**display rmon prialarm** [*prialarm-entry*]
Display the event table of RMON	**display rmon event** [*event-entry*]
Display the log table of RMON	**display rmon eventlog** [*event-entry*]

10.3 RMON Configuration Example

I. Network requirements

Router A is connected to a console terminal through its console port and to an NMS installed with system through Ethernet. You can view the operating state of the router on the NMS.

Do the following:

- Set a RMON alarm entry, which can trigger two Trap events respectively when the sample increment of the 1.3.6.1.2.1.16.1.1.1.4.1 node exceeds the rising and falling threshold;
- Monitor the performance of the Ethernet interface;
- View the statistics about the monitored interface on the console terminal with the **display rmon statistics** command.

II. Network diagram

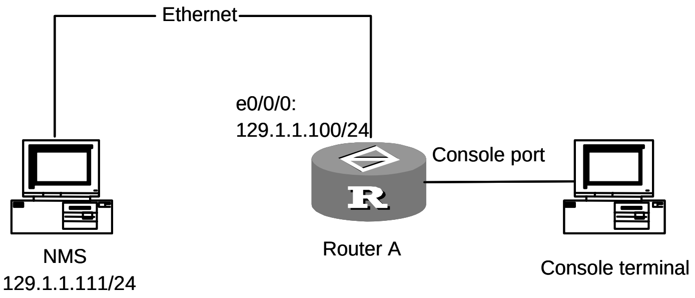


Figure 10-1 Network diagram for RMON

III. Configuration procedure

# Configure SNMP, using the same read/write community and version configured on .

```
[3Com] snmp-agent
[3Com] snmp-agent community read public
[3Com] snmp-agent community write private
[3Com] snmp-agent sys-info version v1
[3Com] snmp-agent trap enable
[3Com] snmp-agent target-host trap address udp-domain 129.1.1.111 params
securityname 3Com
```

# Configure a RMON alarm entry.

```
[3Com] rmon event 1 description rising trap router1 owner 3Com-rmon
[3Com] rmon event 1 description falling trap router1 owner 3Com-rmon
[3Com] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 5 delta rising_threshold 100 1
falling_threshold 50 2
```

# Assign an IP address to interface Ethernet 0/0/0.

```
[3Com] interface ethernet 0/0/0
[3Com-Ethernet0/0/0] ip address 129.1.1.100 255.255.255.0
```

# Set a RMON statistics entry for the Ethernet interface.

```
[3Com-Ethernet0/0/0] rmon statistics 1 owner 3Com-rmon
[3Com-Ethernet0/0/0] quit
```

# Display information about RMON alarm entry 1 and statistics about the Ethernet interface.

```
<3Com> display rmon alarm 1
<3Com> display rmon statistics ethernet 0/0/0
```

When the alarm event is triggered, you can find its record in the fault management module of .

Chapter 11 Terminal Services

11.1 Terminal Services Overview

System provides three types of terminal services entering the command line interface:

- Local configuration through the Console
- Local or remote configuration through AUX port
- Local or remote configuration through Telnet or SSH
- PAD terminal services
- Dumb terminal services

11.2 Console Terminal Services

The local configuration environment can be set up through the Console. Refer to relative parts for the setup of local configuration environment.

For the characteristics of the Console terminal service, see “Table 11-1”.

Table 11-1 Console terminal service characteristics

Service	Characteristics
Echo mode	Without local echo
Terminal type	VT100
Baud rate	9600
Data bit	8
Parity check	None
Stop bit	1 bit
Flow control	None
Binary transport protocol	Xmodem

11.3 Remote Terminal Services on AUX Port

11.3.1 Function Description

Besides performing the local configurations as the CON port, the AUX port can also perform the remote configuration. Please refer to the former section for the methods of local configuration. The remote terminal services will be described in this section.

System supports remote configuration through the AUX port. The serial interface of PC and the AUX port of the router are installed with Modems which are connected through

PSTN, so that the user can establish the connection between PC and the remote router by dial-up on the PC. After the dial-up is successful, the user can set the working parameters of the remote routers through entering the configuration commands on the terminal. The configuration environment is displayed in Figure 11-1.

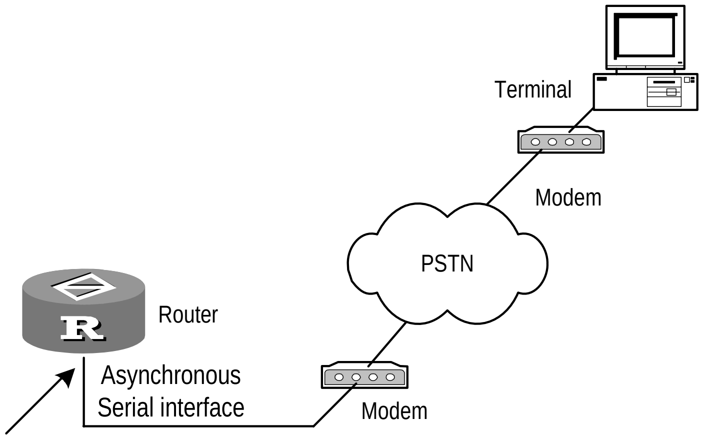


Figure 11-1 Establish remote configuration environment through AUX interface

11.3.2 Terminal Service Characteristics of the Remote Config on AUX Port

System terminal service characteristics of the remote configuration are listed in the following table.

Table 11-2 Terminal service characteristics of the remote configuration

Service	Characteristics
Echo mode	Without local echo
Terminal type	VT100
Baud rate	Consistent with the interface configuration, 9600 bps by default
Data bit	Consistent with the interface configuration, 8 bits by default
Parity check	Consistent with the interface configuration, none by default
Stop bit	Consistent with the interface configuration, 1 bit by default
Flow control	Consistent with the interface configuration, none by default

The terminal program running on PC should accord with parameters set in the above table. The baud rate, data bit, parity check and flow control should be consistent with the corresponding configurations on the AUX port of the router.

11.4 Telnet Terminal Services

11.4.1 Telnet Service Types

The Telnet protocol belongs to application layer protocol in the TCP/IP protocol suite, which provides the function of remote logon and virtual terminal through the network. The Telnet services provided by system include:

I. Telnet Server

Telnet Server services as displayed in the following diagram. The user can run the Telnet client program on a computer to log into the router for configuration and management.

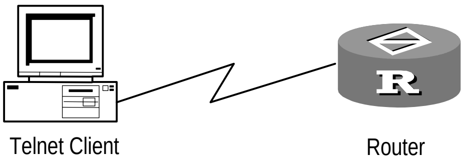


Figure 11-2 Provide the Telnet Server services

II. Telnet Client

The Telnet Client services as displayed in the following diagram. After setting up connection with the router by running the terminal emulation program or the Telnet program on the computer, the user can input the Telnet command to log into other routers for configuration and management.

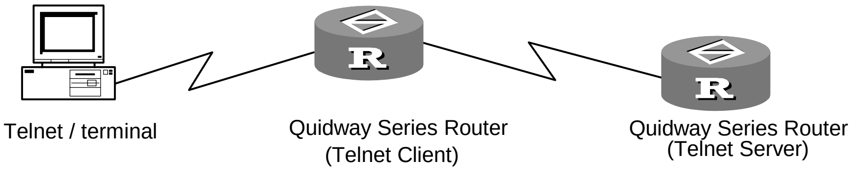


Figure 11-3 Provide the Telnet Client services

Refer to the following table for the Telnet service characteristics of the system.

Table 11-3 Telnet service characteristics

Service	Characteristics
Input mode	Character mode
Echo mode	Without local echo
Terminal type	VT100

III. Redirecting Telnet

To use terminal redirecting function, you need to log into the router from a designated port via Telnet client program, and then to establish connection with the serial port devices connected with the asynchronous interface of the router. The typical application is that 8/16 asynchronous interfaces of the router directly connect multiple devices for remote configuration and maintenance.

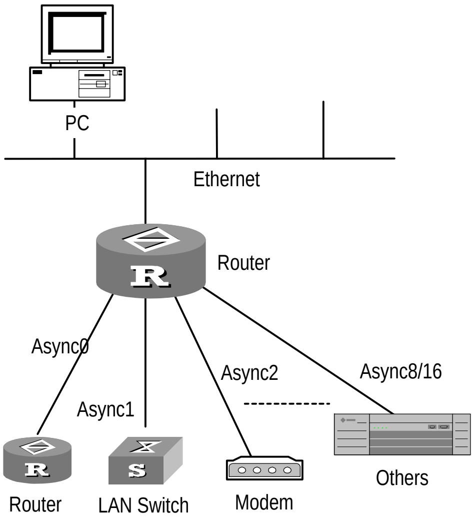


Figure 11-4 Provide Telnet redirection services

11.4.2 Establishing Telnet Connection

I. Establishing a Telnet connection

Perform the following configuration in user view.

Table 11-4 Establish Telnet connection

Operation	Command
Telnet to another router for management	**telnet** [**vpn-instance** *vpn-instance-name*] *host-ip-address* [*service-port*]

For example, a PC is connected to the console port on the router 3Com1. You may then use the following command to telnet to the router 3Com2 at 129.102.0.1.

```
<3Com1> telnet 129.102.0.1
Trying  129.102.0.1 ...
Connected to 129.102.0.1 ...
<3Com2>
```

II. Configuring idle timeout for a Telnet connection

Perform the following configuration in user interface view.

Table 11-5 Configure idle timeout for the Telnet connection

Operation	Command
Configure the idle timeout for the Telnet connection	**idle-timeout** *minutes* [*seconds*]
Restore the default idle timeout	**undo idle-timeout**

The idle timeout for the Telnet connection defaults to 10 minutes.

III. Configuring source interface/address in a telnet

Perform the following configuration in user view or system view.

Table 11-6 Configure source interface/address in a telnet

Operation	Command
Telnet from the main IP address of the specified interface to the destination IP address.	**telnet** *ip-address* [*port*] **source-interface** *interface-type interface-number*
Telnet from the specified IP address to the destination IP address.	**telnet** *ip-address* [*port*] **source-ip** *source-address*

When both source interface and source IP address are configured, the latter takes effect.

Usually this command is used in conjunction with ACL. For example, if a loopback interface is specified as the source interface at the telnet client, the source IP in the Telnet connection is the main IP address of the loopback interface. Thus, the access control policy configured at the Telnet server only involves one IP address.

11.4.3 Establishing Redirected Telnet Connection

In implementing Telnet redirect, you need to configure the router as follows:

- Configure the asynchronous interface to work in flow mode
- Enable Telnet redirect
- Disable terminal services on the user interface.
- Configure the options related to the user interface
- Disconnect the redirected Telnet connection

I. Configuring the asynchronous interface to work in flow mode

Table 11-7 Configure the asynchronous serial interface to work in flow mode

Operation	Command
Configure the asynchronous serial interface to work in flow mode (in asynchronous interface view)	**async mode flow**
Enable/disable DSR/DTR signal detect (in asynchronous interface view)	**detect dsr-dtr** **undo detect dsr-dtr**
Set the flow control on the TTY interface to none (in the user interface view of a TTY user)	**flow-control none**

By default, the mode of the asynchronous interface is protocol, DSR/DTR signal detect is enabled, and flow control is set to none.

Note that the asynchronous interfaces available with the 3Com Series Routers use seven wires and allow DSR/DTR signal detect. You must configure the **undo detect dsr-dtr** command on your router however, if the connected device, an NE router for example, uses three-wire asynchronous interfaces, which do not transmit DSR/DTR signals. This is to ensure that the serial interface can go up without detecting DSR/DTR signals.

II. Enabling Telnet redirect

Execute the **undo shell** command in interface view and the **redirect enable** command in user interface view.

Table 11-8 Establish Telnet redirect connection

Operation	Command
Disable terminal services on the user interface to allow telnet redirect to be enabled	**undo shell**
Enable Telnet redirect (only available with AUX and TTY interfaces	**redirect enable**
Disable Telnet redirect on the asynchronous serial interface	**undo redirect enable**

📖 **Note:**

To enable Telnet redirect on a port successfully after inputting the **undo redirect enable** command, you must wait a while to have the system close all the sockets using that port number. Otherwise, the system may fail to set up a listening socket.
You may use the **display tcp status** command to check the status of sockets, making sure that none of them are in the time_wait state.

III. Configuring a listening port

Perform the following configuration in user interface view.

Table 11-9 Configure a port to listen for redirected Telnet connections

Operation	Command
Configure a port to listen for redirected Telnet connections	**redirect listen-port** *port-number*
Restore the default listening port	**undo redirect listen-port** *port-number*

The default listening port number is TTY number plus 2000.

IV. Configuring other related parameters on the user interface

Perform the following configuration in user interface view.

Table 11-10 Configure the options related to the user interface

Operation	Command
Set the idle timeout for the redirected telnet connection	**redirect timeout** *minutes*
Configure the system to maintain an always-on redirected Telnet connection	**undo redirect timeout**
Enable the router that redirects telnet connections to process the carriage returns received from the Telnet client	**redirect return-deal from-telnet**
Disable the router that redirects Telnet connections to process the carriage returns received from the Telnet client	**undo redirect return-deal from-telnet**
Enable the router that redirects telnet connections to process the carriage returns received from terminals	**redirect return-deal from-terminal**
Disable the router that redirects Telnet connections to process the carriage returns received from terminals	**undo redirect return-deal from-terminal**

Operation	Command
Disable Telnet option negotiation during setup of redirected Telnet connection	**redirect refuse-negotiation**
Enable Telnet option negotiation during setup of redirected Telnet connection	**undo redirect refuse-negotiation**

By default, a Telnet connection can be idle for 360 seconds before it times out, carriage returns are not touched, and Telnet option negotiation is enabled.

V. Disconnecting the redirected Telnet connection

Perform the following configuration in user interface view.

Table 11-11 Disconnect the redirected Telnet connection

Operation	Command
Disconnect the redirected Telnet connection.	**redirect disconnect**

Terminate the redirected connection by pressing <Ctrl+]>.

Note:

- The interfaces of devices connected with the asynchronous interface of the router must also work in async flow mode.
- Telnet port number in establishing the redirect connection is numbered as follows: Telnet port number is equal to TTY number plus 2000. Various user interfaces and their numbers can be displayed using the **display user-interface** command. Moreover, TTY user interface number is one-to-one with each async interface of the router. See the section “Numbering User Interfaces”.

# Communicate with the external device on the seventh async serial interface of the router (IP address of the router is 10.110.164.44, and assume that the router and its external device have been configured).

```
<3Com> telnet 10.110.164.44 2007
Trying  10.110.164.44 ...
Connected to 10.110.164.44
```

After establishing Telnet redirect connection, you can send commands to communicate with the connected device on the asynchronous interface. If the connected one is a modem, you can detect its status or configure it by using the **AT** command.

For example:

```
at
OK
```

You may terminate the redirected connection by pressing <Ctrl+]>.

11.4.4 Specifying a Source Interface/IP Address for the Telnet Server

Perform the following configuration in system view.

Table 11-12 Specify a source interface or source IP address for the Telnet server

Operation	Command
Specify a source interface for the Telnet server	**telnet-server source-interface** *interface-type interface-number*
Delete the source interface specified for the Telnet server	**undo telnet-server source-interface**
Specify a source IP address for the packets sent by the Telnet server	**telnet-server source-ip** *ip-address*
Delete the source IP address for the packets sent by the Telnet server	**undo telnet-server source-ip**

By default, the source IP address in each packet sent by the Telnet server is the IP address of the interface where the packet is sent out.

Note:

You may specify a source IP address for the packets sent by the Telnet server with the **telnet-server source-interface** command or with the **telnet-server source-ip** command. If both commands are configured, the one configured later overrides the previous one.

11.4.5 Binding a User Interface with a VPN Instance

Perform the following configuration in user interface view.

Table 11-13 Bind a user interface with a VPN instance

Operation	Command
Bind a user interface with a VPN instance	**redirect bind vpn-instance**
Remove the VPN instance binding of the user interface	**undo redirect bind vpn-instance**

By default, the user interface is not bound with any VPN instance.

11.4.6 Displaying and Debugging

After completing the above configuration, execute the **display** commands in any view to view information on Telnet and to verify the configuration.

Execute the **debugging** command in user view to debug Telnet.

Table 11-14 Display and debug information on Telnet connections

Operation	Command
Display the connection status of the current LINE	**display users**
Display the connection status of each LINE	**display users all**
Display all current established TCP connections	**display tcp status**
Display the current source IP address set for the packets sent by the Telnet server	**display telnet-server source-ip**
Enable Telnet connection debugging	**debugging telnet**
Disable Telnet connection debugging	**undo debugging telnet**

The **display users** command can only be used to display which interface the Telnet user in connection with the router has to pass. To check the IP address of the Telnet server in connection with the router, execute the **display tcp status** command. All TCP connections with the port number as 23 belong to Telnet connection, which include the connection between the Telnet client and the Telnet server.

During Telnet connection, shortcut can be used to interrupt the connection. As displayed in the following figure, the terminal runs Telnet client program to log into RTA, and then telnet to RTB, then telnet to RTC. In this way, a multileveled connection structure is formed. In this case, RTA is the client of RTB and RTB is the client of RTC. The structure simply illustrates the usage of shortcuts.

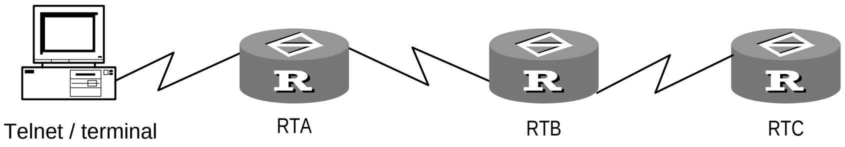


Figure 11-5 Use Telnet shortcuts

II. Shortcut <Ctrl+]>

When the network connection is normal, to press <Ctrl+]> is to notify Telnet server to interrupt the current Telnet login. Its effect is the same as the **Quit** command, that is, the server interrupts the connection initiatively. If the network is disconnected for some reason, the instruction of the shortcut cannot be sent to the server, and the input is invalid.

```
<RTC> (Press <Ctrl+]> and return to the prompt of RTB.)
<RTB> (Press <Ctrl+]> and return to the prompt of RTA.)
<RTA> (Press <Ctrl+]> and return to Telnet connection.)
```

III. Shortcut <Ctrl+K>

In the event that the server fails but the client cannot tell this, you will be unable to receive any reply from the server for instructions that you input. You may however, press <Ctrl+K> to disconnect and quit the Telnet connection:

```
<RTC> (Press <Ctrl+k> and interrupt the connection directly and return to
Telnet connection.
```

11.4.7 Telnet Redirect Configuration Example I

I. Networking requirements

Router A is connected to the PC at 201.1.1.2 through the interface Ethernet 0/0/0 at 201.1.1.1 and to the console interface on Router B through the interface async 1/0/0. The user interface that corresponds to async1/0/0 is tty 1.

II. Networking diagram

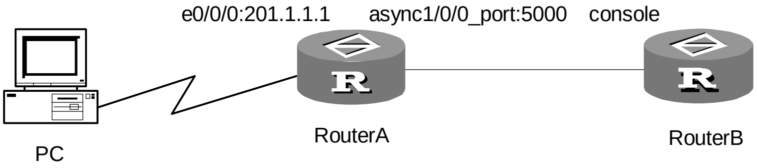


Figure 11-6 Network diagram for Telnet redirect configuration I

III. Configuration procedure

On Router A:

# Configure Ethernet 0/0/0.

```
[Router] interface Ethernet0/0/0
[Router-Ethernet0/0/0] ip address 201.1.1.1 255.255.255.0
[Router-Ethernet0/0/0] quit
```

# Configure async 1/0/0.

```
[Router] interface async1/0/0
```

```
[Router-async1/0/0]] async mode flow
[Router-async1/0/0] quit
```

# Enable Telnet redirect and configure the related parameters on the user interface.

```
[Router] user-interface tty 1
[Router-ui-tty1] undo shell
[Router-ui-tty1] redirect enable
[Router-ui-tty1] undo redirect timeout
[Router-ui-tty1] redirect listen-port 5000
[Router-ui-tty1] undo redirect refuse-negotiation
[Router-ui-tty1] flow-control none
```

After you complete the configurations, you can telnet from the PC using the **telnet 201.1.1.1 5000** command to the console interface on Router B to control and manage the device. This connection is permanent and no telnet option negotiation is allowed. After the connection is set up, Router A transparently transmits data between the PC (the telnet client) and Router B.

If you enter a carriage return at the PC, the string 0x0d 0x0a is sent and two redundant messages may be returned. To resolve the problem, you can configure this command on user interface tty 1:

```
[Router -ui-tty1] redirect return-deal from-telnet
```

11.4.8 Telnet Redirect Configuration Example II

I. Networking requirements

Router A is connected to the PC at 201.1.1.2 through the interface Ethernet0/0/0 at 201.1.1.1, to the console port on Router B through the interface async1/0/0, and to the console port on Router C through the interface async1/1/0. The user interfaces that correspond to async1/0/0 and async1/1/0 are respectively tty 1 and tty 2.

II. Networking diagram

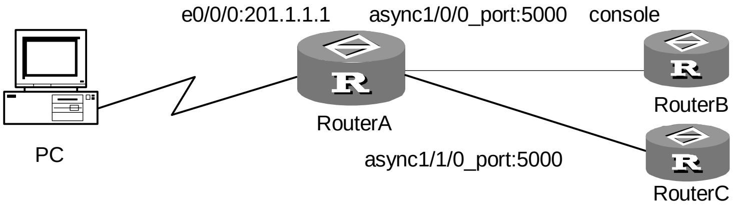


Figure 11-7 Configure Telnet redirect example II

III. Configuration procedure

On Router A:

# Configure Ethernet 0/0/0.

```
[Router] interface Ethernet0/0/0
[Router-Ethernet0/0/0] ip address 201.1.1.1 255.255.255.0
[Router-Ethernet0/0/0] quit
```

# Configure async1/0/0 and async1/1/0.

```
[Router] interface async1/0/0
[Router-async1/0/0] async mode flow
[Router-async1/0/0] flow-control none
[Router-async1/0/0] interface async1/1/0
[Router-async1/1/0] async mode flow
[Router-async1/1/0] quit
```

# Enable Telnet redirect and configure the related parameters on the user interfaces.

```
[Router] user-interface tty 1 2
[Router-ui-tty1-2] undo shell
[Router-ui-tty1-2] redirect enable
[Router-ui-tty1-2] undo redirect timeout
[Router-ui-tty1-2] redirect listen-port 5000
[Router-ui-tty1-2] undo redirect refuse-negotiation
[Router-ui-tty1-2] redirect return-deal from-telnet
[Router-ui-tty1-2] flow-control none
```

After you complete the configurations, you can telnet from the PC using the **telnet 201.1.1.1 5000** command to the console interface on Router B to control and manage the device. If you execute the command again, you can telnet to the console port on Router C to control and manage the device. When a device provides two console terminals, this can save port numbers and facilitate management.

11.5 PAD Terminal Services

There are two types of user terminals: packet terminals and non-packet terminals. Packet terminals (e.g., computers or intelligent terminals) receive and send regulated packets and can be directly connected with the packet switched network according to X.25 protocol. The user data generated by non-packet terminals (e.g., character terminals) are not packets but a string of characters (bytes). Non-packet terminals can only access the packet switched network though Packet Assembler/Disassembler (PAD) rather than directly connect with it.

The main function of PAD is to assemble a string of characters generated in the non-packet terminal to packets in the sending side, so as to send them to the packet switched network. And it will disassemble the packets received in the receiving side to characters for the non-packet terminal to receive.

V 2.41 supports X.25 PAD function which acts as a bridge to make non-X.25 terminals access the X.25 network. You can add a device called PAD between the X.25 network and terminals that do not support X.25 procedures to enable the latter to communicate with other terminals through the X.25 network. Therefore, X.25 PAD devices actually serve as a procedure translator or network server, providing services to different terminals to help them access the X.25 network.

For details about PAD terminal services, refer to “LAPB and X.25 Configuration” section in “Link Layer Protocol” of this manual.

11.6 SSH Configuration

11.6.1 Introduction to SSH

When routers are connected by remote users across insecure networks, secure shell (SSH) can provide them authentication and security fencing off IP spoofing, plain-text password interception and other attacks.

Your router can work as an SSH server or/and an SSH client. As an SSH server, it may accept connections from multiple SSH clients; as an SSH client, it can establish SSH connections with the routers and UNIX hosts working as SSH servers.

Currently, SSH 2.0 is supported.

Figure 11-8 and Figure 11-9 illustrate two methods for establishing an SSH channel between a client and a server:

- Connect through a LAN
- Connect through a WAN

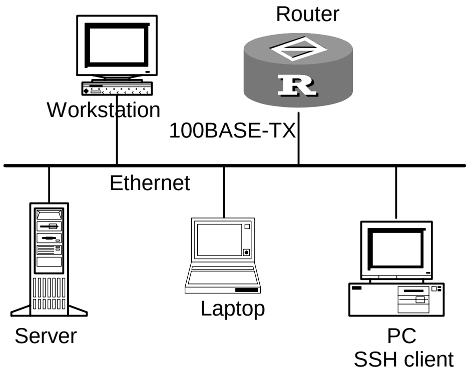


Figure 11-8 Establish an SSH channel in a LAN

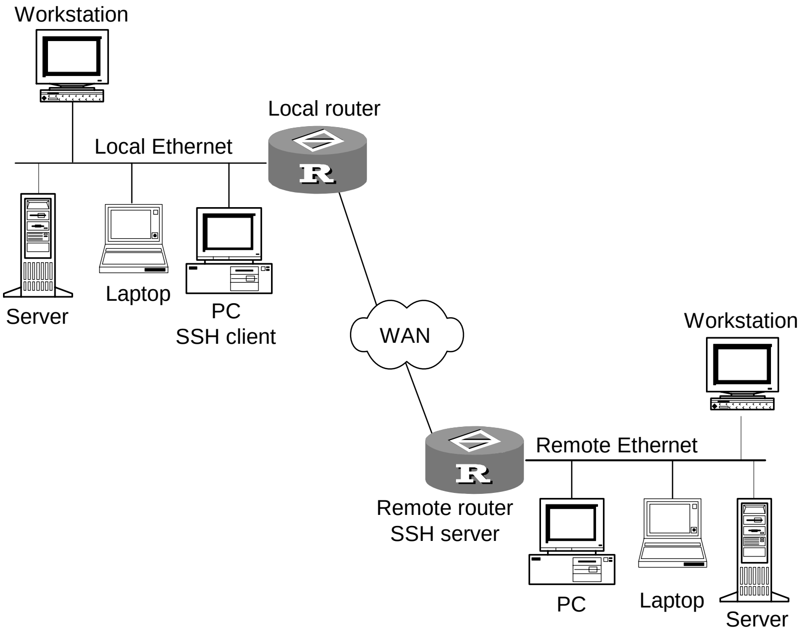


Figure 11-9 Establish an SSH channel through a WAN

To establish an SSH connection, the server and the client must go through the following five phases:

1) Version number negotiation

- The client starts a TCP connection to the server.
- After the TCP connection is established, the server and the client negotiate a version number.
- If the negotiation succeeds, the key algorithm negotiation phase starts; otherwise, the server tears down the TCP connection.

2) Key algorithm negotiation

- The server generates an RSA key pair and an 8-byte random number, and sends the portion of the public key and the random number to the client.
- Both the server and the client use the public key of the server and the 8-byte number as parameters to calculate a 16-byte session ID with the same algorithm.
- The client uses the public key from the server and a random number generated locally as parameters to calculate a session key.
- Using the public key from the server, the client encrypts the random number generated locally for session key calculation and sends the result to the server.
- Using the local private key, the server decrypts the data sent by the client and obtains the random number generated by the client.
- Using the local public key and the random number sent by the client as parameters, the server calculates the session key with the same algorithm used by the client.

Thus, the server and the client obtain the same session key. During the session, both ends use the same session key to perform encryption and decryption, thereby guaranteeing the security of data transfer.

3) Authentication mode negotiation

- The client sends its username information to the server.
- The server initiates a process to authenticate the user. If the user needs no authentication, the server proceeds to session request phase directly.
- The client adopts an authentication mode to authenticate the server till the authentication succeeds or the server tears down the connection because of timeout.

Note:

SSH provides two authentication modes: password and RSA.

1) Password authentication procedure

- The client sends the username and password to the server.
- The server compares the received username and password with the local configuration. If it finds an exact match, the authentication succeeds.

2) RSA authentication procedure

- The server configures the RSA public key of the client.
- The client sends its RSA public key member modulo to the server.
- The server verifies the member modulo. If the member modulo is valid, the server generates a random number, encrypts it using the RSA public key from the client, and sends the encrypted information back to the client.
- The server and the client use the random number and the session ID as parameters to calculate authentication data.
- The client sends the authentication data it generated to the server.
- The server compares the received authentication data with that locally calculated. If they match, the authentication succeeds.

4) Session request: If the authentication succeeds, the client sends a session request to the server. When the server has successfully processed the request, SSH enters the interactive session phase.

5) Interactive session: The client and the server exchange data till the session is over.

11.6.2 SSH Configuration

SSH configuration includes:

I. Configuring the SSH server

- Set the protocols supported on the current user interface
- Create a local RSA key pair
- Configure authentication mode for SSH user
- Create SSH users
- Set an interval for updating the server key (optional)
- Set the timeout time of SSH authentication (optional)
- Set maximum number of SSH authentication retries
- Enter public key view
- Enter public key edit view
- Exit public key edit view
- Assign public key for SSH user
- Configure a service type for an SSH user
- Set SSH version compatibility (optional)

II. Configuring the SSH client

- Enable the SSH client
- Configure public key to server associations
- Configure SSH server first-time authentication

11.6.3 Configuring the SSH Server

I. Setting the protocols supported on user interface

This configuration is used to specify the protocols supported by the system in user interface view. By default, the system supports Telnet and SSH. If SSH is enabled but the local RSA key is not configured, the user cannot login through SSH. The configuration will take effect in next login.

Perform the following operation in User interface view of VTY type.

Table 11-15 Set the protocols supported by system in user interface

Operation	Command
Set the protocols supported by system in user interface	**protocol inbound** { **all** | **pad** | **ssh** | **telnet** }

⚠ **Caution:**

If the protocol supported by the user interface is set to SSH, you must set the authentication mode to **authentication-mode scheme** to ensure a successful login; if you use **authentication-mode password** or **authentication-mode none**, the configuration of the **protocol inbound ssh** command fails. Likewise, an SSH-enabled user interface does not allow the configuration of **authentication-mode password** or **authentication-mode none**.

II. Creating/destroying a local RSA key pair

This configuration is used to generate the local server and host key pair. If there has been RSA now, the system will ask whether to replace the former key. The naming modes of generated key pairs go as follows respectively: router name +server and router name +host. The server key differs in 128 digits at least from host key. The minimum length of server and host key is 512 bits and the maximum length is 2048 bits.

Perform the following operation in system view.

Table 11-16 Configure and destroy a local RSA key pair

Operation	Command
Create a local RSA key pair	**rsa local-key-pair create**
Destroy a local RSA key pair	**rsa local-key-pair destroy**

⚠ **Caution:**

The primary operation to accomplish SSH login is to configure and generate local RSA key pair. Before performing other SSH configurations, you must accomplish the configuration of the **rsa local-key-pair create** command to generate local key pair. It is unnecessary to execute this command again after the router restarts up.

III. Configuring an authentication mode for SSH users

This configuration is used to specify an authentication mode for SSH users. The newly configured authentication mode takes effect at next login.

Perform the following configuration in system view.

Table 11-17 Configure authentication mode for SSH user

Operation	Command
Specify an authentication mode for an SSH user	**ssh user** *username* **authentication-type** { **password** | **rsa** | **all** }
Restore the default, where login is always denied	**undo ssh user** *username* **authentication-type**
Specify a default authentication mode for SSH users	**ssh authentication-type default** { **password** | **rsa** | **all** | **password-publickey** }
Delete the specified default authentication mode for SSH users	**undo ssh authentication-type default**

The authentication mode specified using the **ssh user** *username* **authentication-type** command is only for an SSH user while the one specified using the **ssh authentication-type default** command is the default authentication mode for all SSH users. For an SSH user, the authentication mode configured using the **ssh user** *username* **authentication-type** command is always preferred to the one configured using the **ssh authentication-type default** command.

Note:

If password authentication is adopted, the user name specified in the **ssh user authentication-type** command must be consistent with the user name defined in AAA. If RSA authentication is adopted, the value of this argument is a local SSH user name and needs not to be defined in AAA.

IV. Creating SSH users

All SSH users need authentication. Before creating an SSH user with the **ssh user** command, you must specify a default authentication mode with the **ssh authentication-type default** command.

Perform the following configuration in system view.

Table 11-18 Create an SSH user

Operation	Command
Create an SSH user	**ssh user** *username*
Delete an SSH user	**undo ssh user** *username*

📖 **Note:**

If password authentication is adopted, the user name specified in the **ssh user** command must be consistent with the user name defined in AAA. If RSA authentication is adopted, the value of this argument is a local SSH user name and needs not to be defined in AAA.

If the default authentication mode for SSH users is password and local AAA authentication is adopted, you are not necessarily use the **ssh user** command to create an SSH user. Instead, you can use the **local-user** command to create a user name and its password and then specify the service type for the user to SSH.

V. Setting an interval for updating the server key

To ensure security of the connections to the SSH server, update its key regularly.

Perform the following configuration in system view.

Table 11-19 Set an interval for updating the SSH server key

Operation	Command
Set an interval for updating the SSH server key	**ssh server rekey-interval** *hours*
Restore the default update interval	**undo ssh server rekey-interval**

By default, the server key is not updated.

VI. Setting the timeout time of SSH authentication

This configuration is used to set the time-out time of SSH authentication.

Perform the following configuration in system view.

Table 11-20 Set the timeout time of SSH authentication

Operation	Command
Set the timeout time of SSH authentication	**ssh server timeout** *seconds*
Restore the default time-out time of SSH authentication	**undo ssh server timeout**

By default, the time-out time is 60 seconds.

VII. Setting maximum number of SSH authentication retries

To prevent malicious behaviors such as malicious guess, limit the number of SSH authentication retries.

Perform the following configuration in system view.

Table 11-21 Set maximum number of SSH authentication retries

Operation	Command
Set maximum number of SSH authentication retries	**ssh server authentication-retries** *times*
Restore default maximum number of SSH authentication retries	**undo ssh server authentication-retries**

Maximum number of SSH authentication retries defaults to 3.

For password-public authentication, maximum number of SSH authentication retries must be greater than two, one of which is for sending the public key. Otherwise, the SSH client cannot log into the SSH server.

VIII. Configuring client public key

Two ways of configuring client public keys are available.

1) Manual configuration

Enter public key view with the **rsa peer-public-key** command. With **public-key-code begin** and **public-key-code end** commands, you can input or copy client public key manually.

Table 11-22 Configuring a client public key manually

<table>
<tr><th colspan="2">Operation</th><th>Command</th></tr>
<tr><td colspan="2">At the SSH 1.0/2/0 client, generate a random RSA key pair</td><td>—</td></tr>
<tr><td colspan="2">Convert the public key part to PKCS code with software called SSHKEY.EXE</td><td>—</td></tr>
<tr><td rowspan="4">Configure the client public key on the router</td><td>Enter public key view (in system view)</td><td><b>rsa peer-public-key</b> <i>key-name</i></td></tr>
<tr><td>Enter public key edit view to copy the public key converted by SSHKEY.EXE (in public key view)</td><td><b>public-key-code begin</b></td></tr>
<tr><td>Exit to public key view, with the public key being saved automatically (in public key edit view)</td><td><b>public-key-code end</b></td></tr>
<tr><td>Exit to system view (in public key view)</td><td><b>peer-public-key end</b></td></tr>
</table>

The client public key is a hexadecimal character string generated through PKCS coding of SSHKEY.EXE software. The following shows configuration details.

```
[3Com] rsa peer-public-key 3Com002
[3Com-rsa-public-key] public-key-code begin
[3Com-rsa-key-code] 308186028180739A291ABDA704F5D93DC8FDF84C427463
[3Com-rsa-key-code] 1991C164B0DF178C55FA833591C7D47D5381D09CE82913
[3Com-rsa-key-code] D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE4
[3Com-rsa-key-code] 0861B74A0E135523CCD74CAC61F8E58C452B2F3F2DA0DC
[3Com-rsa-key-code] C48E3306367FE187BDD944018B3B69F3CBB0A573202C16
[3Com-rsa-key-code] BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125
[3Com-rsa-key-code] public-key-code end
[3Com-rsa-public-key] peer-public-key end
```

2) With the **rsa peer-public-key** *key-name* **import sshkey** *filename* command

Table 11-23 Configure a client public key with the **rsa peer-public-key** *key-name* **import sshkey** *filename* command

Operation		Command
At the SSH 1.5/2.0 client, generate a random RSA key pair and save the key file		—
Configure the client public key on the router	Send the public key file to the Flash on the router through FTP/TFTP	Refer to section 5.3 "System Management Overview" and section 5.4 "System Management Overview".
	Perform public key format conversion and configuration	**rsa peer-public-key** *key-name* **import sshkey** *filename*

This way is more convenient and recommended.

Note:

The *filename* argument must take the name of the public key file saved on the Flash.

IX. Assigning an SSH user a public key

Perform the following configuration in system view to assign a public key to an SSH user.

Table 11-24 Assign an SSH user a public key

Operation	Command
Assign a public key to an SSH user	**ssh user** *username* **assign rsa-key** *keyname*

Remove the association of a public key to an SSH user	**undo ssh user** *username* **assign rsa-key**

X. Configuring a service type for an SSH user

Perform the following configuration in system view to configure a service type for an SSH user.

Table 11-25 Configure a service type for an SSH user

Operation	Command
Configure a service type for an SSH user	**ssh user** *username* **service-type** { **stelnet** | **sftp** | **all** }
Restore the default service type for an SSH user	**undo ssh user** *username* **service-type**

The default service type for an SSH user is **stelnet**.

XI. Setting SSH version compatibility

Perform the following configuration in system view to enable/disable the SSH server to work with SSH1.X clients.

Table 11-26 Enable/disable the SSH server to work with SSH1.X clients

Operation	Command
Enable the SSH server to work with SSH1.X clients	**ssh server compatible_ssh1x enable**
Disable the SSH server to work with SSH1.X clients	**undo ssh server compatible_ssh1x**

By default, the SSH server works with SSH1.X clients.

XII. Specifying a source interface/IP address for the SSH server

Perform the following configuration in system view.

Table 11-27 Specify a source interface or source IP address for the SSH server

Operation	Command
Specify a source interface for the SSH server	**ssh-server source-interface** *interface-type interface-number*
Delete the source interface specified for the SSH server	**undo ssh-server source-interface**
Specify a source IP address for the packets sent by the SSH server	**ssh-server source-ip** *ip-address*

Operation	Command
Delete the source IP address for the packets sent by the SSH server	**undo ssh-server source-ip**

By default, the source IP address in each packet sent by the SSH server is the IP address of the interface where the packet is sent out.

Note:

You may specify a source IP address for the packets sent by the Telnet server with the **ssh-server source-interface** command or with the **ssh-server source-ip** command. If both commands are configured, the one configured later overrides the previous one.

11.6.4 Configuring the SSH Client

I. Enabling the SSH client

When enabling the SSH client to SSH to the server, you need to specify the preferred key exchange algorithm, encryption algorithm and HMAC algorithm between the client and the server.

Perform the following configuration in system view.

Table 11-28 Enable the SSH client

Operation	Command
Enable the SSH client	**ssh2** { *host-ip* | *host-name* } [*port-num*] [**prefer_kex** { **dh_group1** | **dh_exchange_group** }] [**prefer_ctos_cipher** { **des** | **3des** | **aes128** }] [**prefer_stoc_cipher** { **des** | **3des** | **aes128** }] [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]

II. Configuring public key to server associations

You need to associate an SSH server with the name assigned to its public key. When connecting to this server, the client verifies its trustworthiness based on this association.

Perform the following configuration in system view.

Table 11-29 Associate an SSH server with a public key

Operation	Command
Associate an SSH server with its public key	**ssh client** *server* **assign rsa-key** *keyname*
Remove an SSH server to public key association	**undo ssh client** *server* **assign rsa-key** *keyname*

III. Configuring SSH server first-time authentication

The configuration of first-time authentication decides the action taken by the SSH client when it accesses a server in the absence of the server's public key:

- With first-time authentication enabled, the SSH client can attempt to access the server and get the server's public key through negotiation. Then this public key could be saved on the client for next access.
- With first-time authentication disabled, the SSH client rejects to access a server. To access the server, you must save its public key on the SSH client beforehand.

Perform the following configuration in system view.

Table 11-30 Configure first-time authentication

Operation	Command
Enable SSH server first-time authentication	**ssh client first-time enable**
Disable SSH server first-time authentication	**undo ssh client first-time**

By default, first-time authentication is enabled on the SSH client.

IV. Specifying a source interface/IP address for the SSH client

Perform the following configuration in system view.

Table 11-31 Specify a source interface or source IP address for the SSH client

Operation	Command
Specify a source interface for the SSH client server	**ssh2 source-interface** *interface-type interface-number*
Delete the source interface specified for the SSH client	**undo ssh2 source-interface**
Specify a source IP address for the packets sent by the SSH client	**ssh2 source-ip** *ip-address*
Delete the source IP address for the packets sent by the SSH client	**undo ssh2 source-ip**

By default, the source IP address in each packet sent by the SSH client is the IP address of the interface where the packet is sent out.

Note:

You may specify a source IP address for the packets sent by the Telnet server with the **ssh2 source-interface** command or with the **ssh2 source-ip** command. If both commands are configured, the one configured later overrides the previous one.

11.6.5 Displaying and Debugging

After the above configuration, execute display command in any view to display the running of the SSH configuration, and to verify the configuration.

The task of displaying and debugging SSH is used to view the configuration of various SSH users to utilize the system resource better and accomplish the secure information connection.

Table 11-32 View relevant information about SSH

Operation	Command
View the pubic key of host and server key pair	**display rsa local-key-pair public**
Display the RSA public key of client	**display rsa peer-public-key** [**brief** | **name** *keyname*]
Display SSH status information and session information	**display ssh server** { **status** | **session** }
Display SSH user information	**display ssh user-information** [*username*]
Display the current source IP address setting of the SSH server	**display ssh-server source-ip**
Display the current source IP address setting of the SSH client	**display ssh2 source-ip**

Executing the **debugging** command in user view.

Table 11-33 Debug information on SSH

Operation	Command
Enable SSH debug	**debugging ssh server** { **vty** *index* | **all** }

Operation	Command
Disable SSH debug	**undo debugging ssh server** { **vty** *index* | **all** }
Enable RSA debugging	**debugging rsa**
Disable RSA debugging	**undo debugging rsa**

11.6.6 SSH Configuration Example

I. Network requirements

As shown in Figure 11-10, the console terminal (the SSH client) is directly connected to the router through an Ethernet interface. Run SSH2.0 client software on the terminal for securely logging onto the router for configuration and management. The username of the SSH client is client001@169.254.0.1 and the password is 3Com.

II. Network diagram

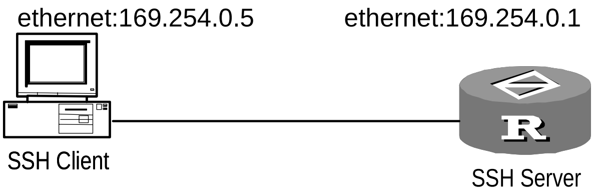


Figure 11-10 Network diagram for SSH server configuration

III. Configuration procedure

1) Configure the SSH server (the router)

Configuration procedure varies with login authentication mode. However, all procedures must start with creating local RSA key pairs using the following command:

```
[3Com] rsa local-key-pair create
```

Note:

If local key pairs exist, skip this step.

- Set the authentication method for the SSH user to password.

```
[3Com] user-interface vty 0 4
[3Com-ui-vty0-4] authentication-mode scheme
[3Com-ui-vty0-4] protocol inbound ssh
[3Com-ui-vty0-4] quit
```

```
[3Com] local-user client001
[3Com-luser-client001] password simple 3Com
[3Com-luser-client001] service-type ssh
[3Com-luser-client001] quit
[3Com] ssh user client001 authentication-type password
[3Com] domain 169.254.0.1
[3Com-isp-169.254.0.1] scheme local
[3Com-isp-169.254.0.1] quit
```

The default value for authentication time-out time, retry times and update time of server key of SSH can be adopted. After these configurations, you can run SSH2.0 on a terminal connected to the router. Then, you can access the router with username client001 and password 3Com.

- Set the authentication method for SSH user to RSA.

```
[3Com] user-interface vty 0 4
[3Com-ui-vty0-4] authentication-mode scheme
[3Com-ui-vty0-4] protocol inbound ssh
[3Com-ui-vty0-4] quit
[3Com] ssh user client002 authentication-type RSA
```

Then, use the SSH2.0 client software to randomly generate the RSA key pairs (including public and private keys) and synchronize the public key to the specified rsa peer-public-key on the SSH server. The RSA public key discussed here is a hexadecimal string coded using the software SSHKEY.EXE provided by our company according to the PKCS standard.

```
[3Com] rsa peer-public-key 3Com002
[3Com-rsa-public] public-key-code begin
[3Com-key-code] 308186028180739A291ABDA704F5D93DC8FDF84C427463
[3Com-key-code] 1991C164B0DF178C55FA833591C7D47D5381D09CE82913
[3Com-key-code] D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE4
[3Com-key-code] 0861B74A0E135523CCD74CAC61F8E58C452B2F3F2DA0DC
[3Com-key-code] C48E3306367FE187BDD944018B3B69F3CBB0A573202C16
[3Com-key-code] BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125
[3Com-key-code] public-key-code end
[3Com-rsa-public] public-key-code end
[3Com] ssh user client002 assign rsa-key 3Com002
```

2) Configure the SSH client

- When password authentication applies, you need to configure at the client the IP address of a reachable interface on the SSH server or the router, 169.254.0.1 in this example, set the protocol type to SSH, use SSH version 2. After opening the SSH connection, enter the user name and password to access the router configuration interface.

```
login as: client001
```

```
Sent username "client001"
client001@169.254.0.1's password:
*********************************************************
*          All rights reserved (1997-2004)              *
*      Without the owner's prior written consent,       *
*no decompiling or reverse-engineering shall be allowed.*
*********************************************************

<Router>
```

- When RSA authentication applies, you must specify an RSA private key file, which is generated randomly by the client software in addition to the configuration tasks done with password authentication. After opening the SSH connection, enter the user name to access the router configuration interface.

```
login as: client002
Sent username "client002"
Trying public key authentication.
No passphrase required.

*********************************************************
*          All rights reserved (1997-2004)              *
*      Without the owner's prior written consent,       *
*no decompiling or reverse-engineering shall be allowed.*
*********************************************************

<Router>
```

Caution:

To set up an SSH connection, make sure that the user name provided at login must be the same as the one configured on the router with the **ssh user** *username* command.

11.6.7 SSH Client Configuration Example

I. Network requirements

Router B is working as the SSH client with user name client003.

Router A is working as the SSH server with IP address 10.165.87.136.

II. Network diagram

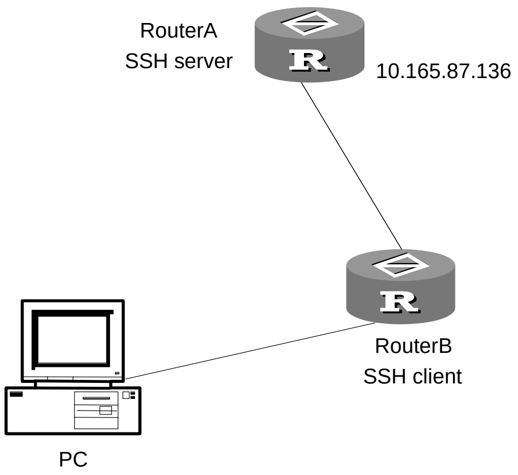


Figure 11-11 Network diagram for SSH client configuration

III. Configuration procedure

1) Configure the SSH server (Router A)

Refer to the configuration procedure in section 11.6.6 “SSH Configuration Example”.

2) Configure the SSH client (Router B)

# Enable SSH server first-time authentication.

```
[3Com] ssh client first-time enable
```

Caution:

Before you can access the SSH server, you must configure the server’s public key and associate the key with the server on the client (except for the software Putty and Openssh).

# Configure the server’s public key.

```
[3Com] rsa peer-public-key 10.165.87.136
[3Com-rsa-public-key] public-key-code begin
[3Com-rsa-key-code] 308186028180739A291ABDA704F5D93DC8FDF84C427463
[3Com-rsa-key-code] 1991C164B0DF178C55FA833591C7D47D5381D09CE82913
[3Com-rsa-key-code] D7EDF9C08511D83CA4ED2B30B809808EB0D1F52D045DE4
[3Com-rsa-key-code] 0861B74A0E135523CCD74CAC61F8E58C452B2F3F2DA0DC
[3Com-rsa-key-code] C48E3306367FE187BDD944018B3B69F3CBB0A573202C16
[3Com-rsa-key-code] BB2FC1ACF3EC8F828D55A36F1CDDC4BB45504F020125
[3Com-rsa-key-code] public-key-code end
```

```
[3Com-rsa-public-key] peer-public-key end
[3Com] ssh client 10.165.87.136 assign rsa-key 10.165.87.136
```

# Enable the SSH client.

The configuration varies depending on the adopted authentication mode.

- When password authentication and the default algorithms are adopted, do the following:

```
[3Com] ssh2 10.165.87.136
Please input the username: client003
Trying 10.165.87.136
Press CTRL+K to abort
Connected to 10.165.87.136...
The Server is not authenticated.Do you continue access it?(Y/N):y
Do you want to save the server's public key?(Y/N):y
Enter password:
*********************************************************
*          All rights reserved (1997-2004)              *
*      Without the owner's prior written consent,       *
*no decompiling or reverse-engineering shall be allowed.*
*********************************************************

<3Com>
```

- When RSA authentication is adopted, do the following:

```
[3Com] ssh2 10.165.87.136 22 perfer_kex dh_group1 perfer_ctos_cipher des
perfer_stoc_cipher 3des perfer_ctos_hmac md5 perfer_stoc_hmac md5
Please input the username: client003
Trying 10.165.87.136...
Press CTRL+K to abort
Connected to 10.165.87.136...
The Server is not authenticated.Do you continue access it?(Y/N):y
Do you want to save the server's public key?(Y/N):y
*********************************************************
*          All rights reserved (1997-2004)              *
*      Without the owner's prior written consent,       *
*no decompiling or reverse-engineering shall be allowed.*
*********************************************************

<3Com>
```

11.7 SFTP Service

11.7.1 Introduction to SFTP

Secure FTP (SFTP) is a new feature introduced in SSH 2.0.

SFTP is established on SSH connections to provide secured data transfer.

Your router may work as both SFTP server and client. As an SFTP server, it allows a remote user to securely log into it to manage and transfer files for example, when upgrading the system. As an SFTP client, it allows you to securely log into another device to transfer files.

11.7.2 Configuring the SFTP Server

The following table describes the SFTP server configuration tasks:

Table 11-34 Configure the SFTP server

No.	To do…	Use the command…	View	Remarks
1	Configure a service type for an SSH user	**ssh user service-type**	System view	Optional
2	Enable the SFTP server	**sftp server enable**	System view	Required

I. Configuring a service type for a user

Perform the following configuration in system view to set a service type for an SSH user.

Table 11-35 Set a service type for an SSH user

Operation	Command
Set a service type for an SSH user	**ssh user** *username* **service-type** { **stelnet** | **sftp** | **all** }
Restore the default service type	**undo ssh user** *username* **service-type** { **stelnet** | **sftp** | **all** }

The default service type for an SSH user is stelnet.

II. Enabling the SFTP server

Perform the following configuration in system view.

Table 11-36 Enable the SFTP server

Operation	Command
Enable the SFTP server	**sftp server enable**
Disable the SFTP server	**undo sftp server**

By default, the SFTP server is disabled.

11.7.3 Configuring the SFTP Client

The following table describes the SFTP client configuration tasks:

Table 11-37 Configure the SFTP client

No.	To do…		Use the command…	In… view	Remarks
1	Enable the SFTP client		**sftp**	SFTP client view	Required
2	Disable the SFTP client		**bye**	System view	Optional
			exit		
			quit		
3	Directory-related operations with SFTP	Change the current directory	**cd**	SFTP client view	Optional
		Exit to the upper directory	**cdup**		
		Display the current directory	**pwd**		
		Display the list of the files in a directory	**dir**		
			ls		
		Create a new directory	**mkdir**		
		Delete a directory	**rmdir**		

No.	To do…		Use the command…	In… view	Remarks
4	File-related operations with SFTP	Rename a file on the SFTP server	**rename**	SFTP client view	Optional
		Download a file from the remote SFTP server	**get**		
		Upload a file from the remote SFTP server	**put**		
		Display the list of the files in a directory	**dir**		
			ls		
		Delete a file from the SFTP server	**delete**		
			remove		
5	Get help information about SFTP client commands		**help**	SFTP client view	Optional

I. Enabling the SFTP client

To log into and operate on an SFTP server, enable the SFTP client and enter SFTP client view.

Perform the following configuration in system view.

Table 11-38 Enable the SFTP client

Operation	Command
Enable the SFTP client	**sftp** { *host-ip* | *host-name* } [*port-num*] [**prefer_kex** { **dh_group1** | **dh_exchange_group** }] [**prefer_ctos_cipher** { **des** | **3des** | **aes128** }] [**prefer_stoc_cipher** { **des** | **3des** | **aes128** }] [**prefer_ctos_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }] [**prefer_stoc_hmac** { **sha1** | **sha1_96** | **md5** | **md5_96** }]

II. Disabling the SFTP client

Execute the following command in SFTP view to disable the SFTP client.

Table 11-39 Disable the SFTP client

Operation	Command
Disable the SFTP client	**bye**
	exit
	quit

III. Operating with SFTP directories

Execute the following command in SFTP client view.

Table 11-40 Operate with SFTP directories

Operation	Command
Change the current directory	**cd** *remote-path*
Exit to the upper directory	**cdup**
Display the current directory	**pwd**
Display the list of the files in a directory	**dir** [*remote-path*]
	ls [*remote-path*]
Create a directory on the SFTP server	**mkdir** *remote-path*
Delete a directory from the SFTP server	**rmdir** *remote-path*

IV. Operating with files

Execute the following command in SFTP client view.

Table 11-41 Operate with SFTP files

Operation	Command
Change the name of a file on the remote SFTP server	**rename** *old-name new-name*
Download a file from the remote SFTP server	**get** *remote-file* [*local-file*]
Upload a file to the remote SFTP server	**put** *local-file* [*remote-file*]
Display the list of the files in a directory	**dir** [*remote-path*]
	ls [*remote-path*]

Operation	Command
Delete a file from the SFTP server	**delete** *remote-file*
	remove *remote-file*

V. Specifying a source interface/IP address for the SFTP client

Perform the following configuration in system view.

Table 11-42 Specify a source interface or source IP address for the SFTP client

Operation	Command
Specify a source interface for the SFTP client	**sftp source-interface** *interface-type interface-number*
Delete the source interface specified for the SFTP client	**undo sftp source-interface**
Specify a source IP address for the packets sent by the SFTP client	**sftp source-ip** *ip-address*
Delete the source IP address for the packets sent by the SFTP client	**undo sftp source-ip**

By default, the source IP address in each packet sent by the SFTP client is the IP address of the interface where the packet is sent out.

📖 **Note:**

You may specify a source IP address for the packets sent by the Telnet server with the **sftp source-interface** command or with the **sftp source-ip** command. If both commands are configured, the one configured later overrides.

VI. Displaying help information

Execute the following command in SFTP client view to get help information about SFTP client commands.

Table 11-43 Display help information about SFTP client commands

Operation	Command
Display help information about SFTP client commands	**help** [*command-name*]

11.7.4 SFTP Configuration Example

I. Network requirements

As shown in Figure 11-12,

- An SSH connection is present between Router A and Router B.
- Use Router A as an SFTP server with IP address 10.111.27.91.
- Use Router B as an SFTP client.
- Create an SSH user account 8040 with password 3Com.

II. Network diagram

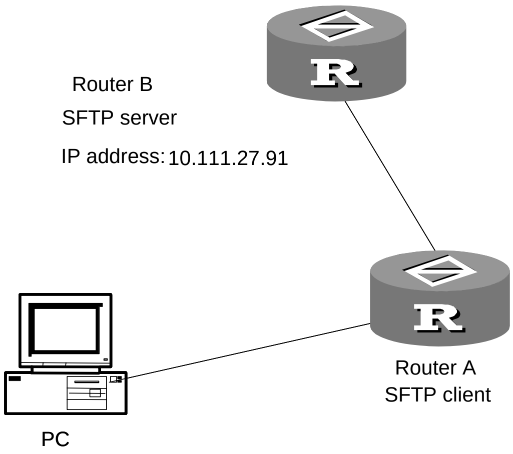


Figure 11-12 Network diagram for SFTP

III. Configuration procedure

1) Configure Router B (the SFTP server)

# Enable the SFTP server.

```
[3Com] sftp server enable
```

# Specify SFTP service for SSH user 8040.

```
[3Com] ssh user 8040 service-type sftp
```

2) Configure Router A (the SFTP client)

# Establish a connection to the SFTP server and enter SFTP client view.

```
[3Com] sftp 10.111.27.91
```

# Display the current directory on the SFTP server, delete file z and verify the operation.

```
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 v 2.41cfg.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
```

```
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
-rwxrwxrwx   1 noone    nogroup         0 Sep 01 08:00 z
sftp-client> delete z
Remove this File?(Y/N)
flash:/zy
File successfully Removed
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 v 2.41cfg.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
```

# Create directory new1 and verify the operation.

```
sftp-client> mkdir new1
New path created
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 v 2.41cfg.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:30 new1
```

# Change the name of directory new1 to new2 and verify the operation.

```
sftp-client> rename new1 new2
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 v 2.41cfg.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
-rwxrwxrwx   1 noone    nogroup       225 Sep 01 06:55 pub
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:33 new2
```

# Download file pubkey2 and rename it to pu.

```
sftp-client> get pubkey2 pu
Downloading file successfully ended
```

# Upload file pu to the SFTP server and rename it to puk. Verify the operations.

```
sftp-client> put pu puk
Uploading file successfully ended
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 v 2.41cfg.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
```

```
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
drwxrwxrwx   1 noone    nogroup         0 Sep 01 06:22 new
drwxrwxrwx   1 noone    nogroup         0 Sep 02 06:33 new2
-rwxrwxrwx   1 noone    nogroup       283 Sep 02 06:35 pu
-rwxrwxrwx   1 noone    nogroup       283 Sep 02 06:36 puk
sftp-client>
```

# Disconnect from the SFTP server.

```
sftp-client> quit
Bye
<3Com>
```

11.8 Dumb Terminal Service

11.8.1 Description on Dumb Terminal Functions

When the async interface (e.g. sync/async interface, AUX port or 8-async interface) of the router works in flow mode, you can directly connect it with the serial interface of the computer (or terminal) to enter the command-line interface and to configure the router, this mode is called dumb terminal working mode. You can establish other applications based on dumb terminal, for example, executing the Telnet to log in to other devices.

A user can log in to and manage the router by running the super-terminal on his/her PC to connect with any async interface on a router, as shown in Figure 11-13.

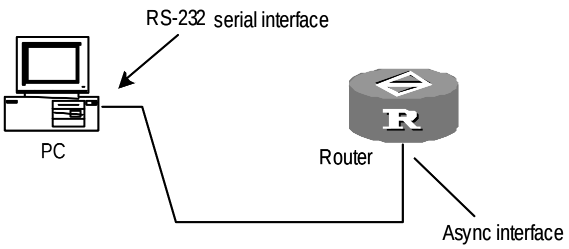


Figure 11-13 Dumb terminal connection mode

11.8.2 Dumb Terminal Service Features

See Table 11-2. They are consistent with those of remote terminal service.

11.8.3 Typical Application of Dumb Terminal

Typical applications:

- In flow mode, the async interface is connected via the dedicated line to directly enter the command-line interface of a router. This application provides another terminal service except Console port and Telnet.

- In flow mode, the async interface directly logs in to the command-line interface of a router via the async dedicated line, and then boots Telnet Client program to log in to other remote systems.

11.8.4 Configuring Dumb Terminal Service

The following table shows the configuration commands related to dumb terminal. Perform the configurations of the **async mode** command in interface view, and of the **auto-execute command** command in user interface view.

Table 11-44 Related commands for establishing dumb terminal connection

Operation	Command
Set the async interface to work in flow mode	**async mode flow**
Disable the async interface to work in flow mode	**async mode protocol**
Auto-execute the configuration command on the async interface	**auto-execute command** *command*
Disable to auto-execute the configuration command on the async interface	**undo auto-execute command**

I. Dumb terminal configuration

# Configure the async interface connected with the terminal.

Configure the sync/async interface as follows:

```
[3Com-serial1/0/0] physical-mode async
[3Com-serial1/0/0] async mode flow
```

Configure 8-/16-async interface as follows:

```
[3Com-ui-tty1] undo modem
[3Com-async1/0/0] async mode flow
```

Configure AUX port as follows:

```
[3Com-ui-aux0] undo modem
[3Com-Aux0] async mode flow
```

After the above operations, press two carriage returns on the external terminal of the async interface to enter the configuration interface of the router. During the configuration, if you execute **quit** to exit from the command-line interface and want to enter again, you must press two carriage enters.

🕮 **Note:**

Set the async interface to disable Modem dial-in in the relevant user interface view. For more details, see the *User Interface Configuration* chapter.

II. auto-execute command configuration

If the async interface of the router is configured with the **auto-execute command** command, and a user presses two carriage enters on its external terminal, the router will automatically execute some commands to directly enter the operating state.

There are some restrictions in using the **auto-execute command** command.

- If the router has only one Console port or AUX port (Console port and AUX port share one port), the port will not support the **auto-execute command** command.
- If the router has one Console port and one AUX port (two ports), the former will not support the **auto-execute command** command, while the latter will support it.
- No restriction on other types of interfaces.

The system will automatically execute a certain command configured by the **auto-execute command** command on the terminal at login, and disconnect user connection after the command terminates. In practice, Telnet is configured by the **auto-execute command** command on the terminal to enable a user to automatically connect to the specified host. Using the command will result in disabling the terminal to configure the system. Be cautious in use.

⚠ **Caution:**

Before configuring the **auto-execute command** command and saving its configuration (execute **save**), make sure that you can log in to the system to change this configuration back by other means.

The most typical application of the **auto-execute command** command is that after a user establishes connection with the router via dumb terminal mode, he/she can remotely log in to other routers via the Telnet specified by the **auto-execute command**. In this way, the router is transparent to the end user, as shown in the following figure:

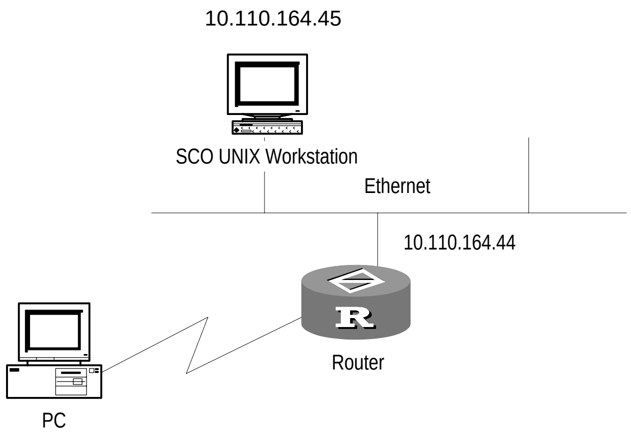


Figure 11-14 auto-execute command configuration diagram

Configuration procedure is as follows:

# Configure the async interface (e.g. serial1/0/0) to work in dumb terminal mode, see the configuration in the preceding section.

# Configure the **auto-execute command** command.

In user interface view, enter:

```
[3Com-ui-vty0] auto-execute command telnet 10.110.164.45
```

After configuration, press two carriage enters on the terminal connected with the async interface of the router to log in to the destination host. If you want to log in again after exiting, re-press two carriage enters.

Note:

To cancel the **auto-execute command** function, execute the **undo auto-execute command** command in the relevant user interface view.

11.8.5 Timely Disconnecting Dumb Terminals

Perform the following configuration in user interface view.

Table 11-45 Timely disconnect the dumb terminal

Operation	Command
Enable timely disconnecting dumb terminal connection	**idle-timeout** *minutes* [*seconds*]
Restore its default value	**undo idle-timeout**

If a user has set the **idle-timeout** and does not receive the entry from a dumb terminal user within this time, the system will disconnect this connection to prevent the illegal intrusion of unauthorized users after 10 minutes. If a user executes the **idle-timeout** 0 command to disable this function in the relevant user interface view, dumb terminal users will not be disconnected all the time.

# Disable timely disconnecting dumb terminal connection.

```
[3Com-ui-vty0] idle-timeout 0
```

11.9 Remote Shell Service

11.9.1 Introduction to Remote Shell

Remote shell (RSH) is originally a Berkeley/UNIX network command. It allows you to execute some particular commands on the RSH-supported remote hosts that run the RSH daemon for the communications with the RSH client.

A 3Com series router can work as the RSH client where you can use the **rsh** command to execute commands on the server host remotely, as shown in the following figure.

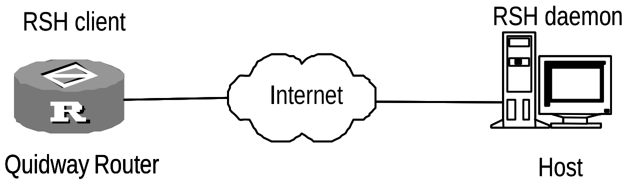


Figure 11-15 Typical network that runs RSH

With the RSH daemon, you can execute commands remotely if trusted-host and privilege port authentication is passed. You can start or close the service using the service component in Windows NT/2000/XP/2003.

Note:

Neither Windows NT/2000/XP/2003 system nor the 3Com Series Routers provide the RSH daemon program, so you need install one yourself to have the service.

11.9.2 Operating on the RSH Client Side

Execute the following command on the router that runs the RSH client.

Perform the following operation in user view.

Table 11-46 Operate on the RSH client

Operation	Command
Execute a command remotely.	**rsh** *host* [**user** *username*] **command** *remote-command*

11.9.3 Debugging RSH

To verify the effect after you execute the **rsh** command, use the **debugging rsh** command.

Perform the following operation in user view.

Table 11-47 Debug RSH

Operation	Command
Enable RSH debugging.	**debugging rsh**
Disable RSH debugging.	**undo debugging rsh**

11.9.4 Example of Rsh Client Operation

On a network reside a router that acts as the RSH client and a remote host that uses Windows 2000 and has the RSH daemon service enabled.

You can set the time of the host remotely on the router.

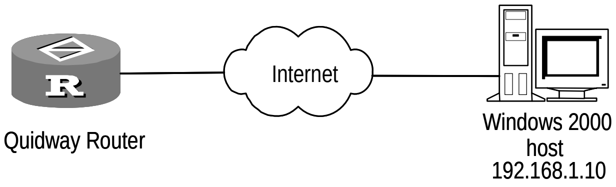


Figure 11-16 Networking for an RSH application

Note:

This example assumes that at least a route exists between the router and the host.

I. Checking that the RSH daemon has been installed and started in Windows NT/2000/XP/2003

1) Enter [Start/Settings/Control Panel/Administrative Tools]. (For Windows XP, when you use the classification view of the Control Panel window, select Administrative Tools from Performance and Maintenance.)

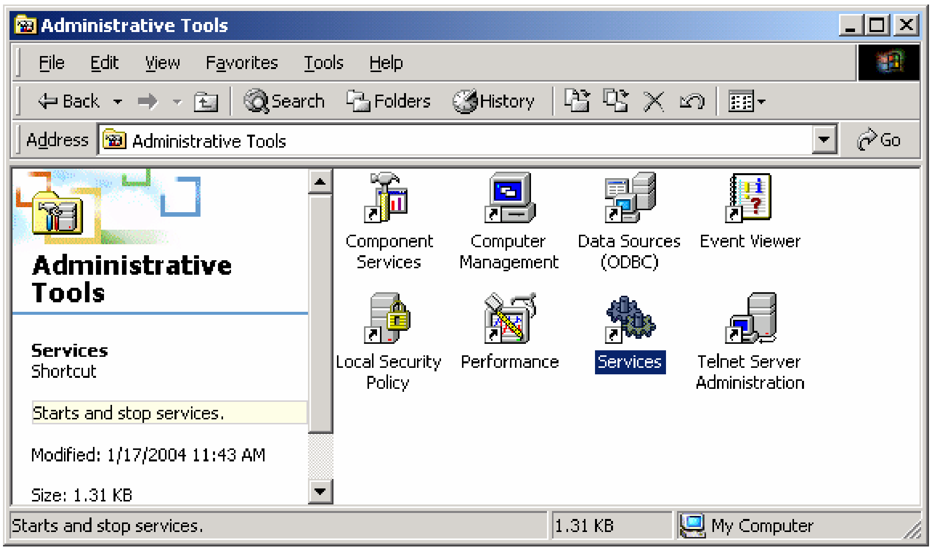
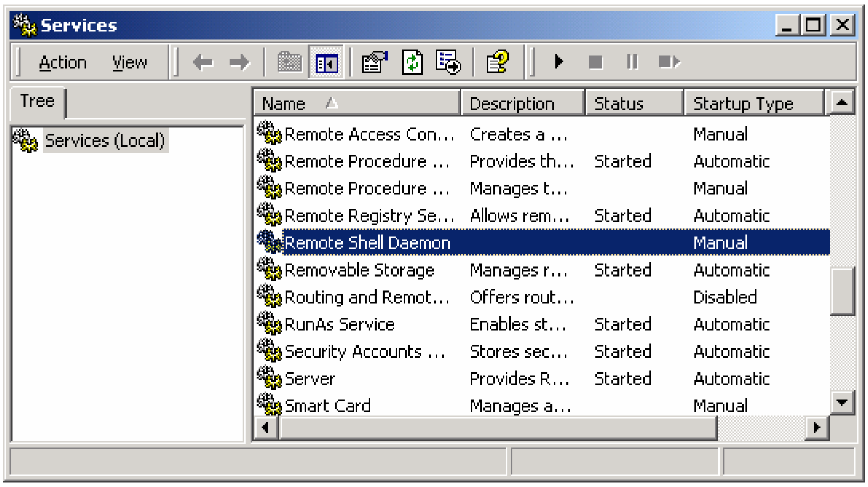


Figure 11-17 Administrative Tools folder of Windows

2) Double-click on the Services icon to enter the Services window.



Name	Description	Status	Startup Type
Remote Access Con…	Creates a …		Manual
Remote Procedure …	Provides th…	Started	Automatic
Remote Procedure …	Manages t…		Manual
Remote Registry Se…	Allows rem…	Started	Automatic
Remote Shell Daemon			Manual
Removable Storage	Manages r…	Started	Automatic
Routing and Remot…	Offers rout…		Disabled
RunAs Service	Enables st…	Started	Automatic
Security Accounts …	Stores sec…	Started	Automatic
Server	Provides R…	Started	Automatic
Smart Card	Manages a…		Manual

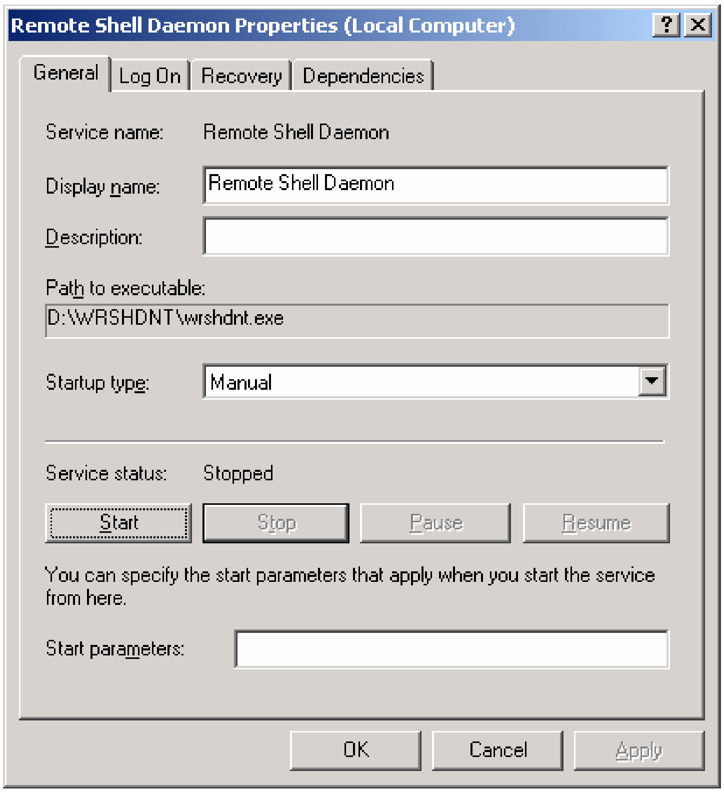
Figure 11-18 Services window

3) Check for the Remote Shell Daemon. If it does not exist, install it first.

4) Look at the Status column to check whether the Remote Shell Daemon service is started.

In this example, the service is not started yet.

5) Double-click on the service row, and in the popup Remote Shell Daemon Properties window, click <Start> to start the service, as shown in the following figure.



Service name: Remote Shell Daemon

Display name: Remote Shell Daemon

Description:

Path to executable:
D:\WRSHDNT\wrshdnt.exe

Startup type: Manual

Service status: Stopped

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Figure 11-19 Remote Shell Daemon Properties window

II. Executing the following commands in user view on the router

```
<3Com>rsh 192.168.1.10 command time
Trying 192.168.1.10 ...
Press CTRL+K to abort
The current time is:  6:56:42.57
Enter the new time: 12:00
12:00
```

11.10 Rlogin Terminal Service Connectivity

11.10.1 Introduction

Remote login (rlogin) was a remote login service first developed for Berkeley Unix. Compared with Telnet, it provides tighter output control and suppression but is easier to implement and use. Rlogin clients and servers are connected using TCP, allowing multiple logins to one Unix host.

On the router, V 2.41 delivers the rlogin client service similar to a multi-port serial interface card, allowing the logging user terminals (digital or analog) to rlogin to a remote Unix host.

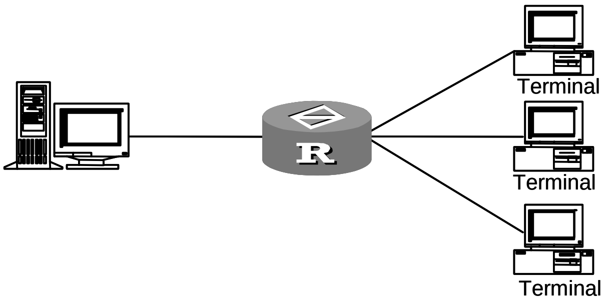


Figure 11-20 Connect terminals to a Unix server through the router

The rlogin client service provided by the router supports:

- Terminal type of VT100
- Transmission rate of 38,400 bps
- Multiple terminal types, such as Console, TTY, and VTY
- Multiple rlogin sessions initiated by one terminal

11.10.2 Rlogin Configurations

Perform the following configurations in user view.

Table 11-48 Establish an rlogin connection

Operation	Command
Establish an rlogin connection	**rlogin** *remote-host username*

11.10.3 Displaying and Debugging Rlogin

Perform the following operations in user view.

Table 11-49 Display and debug Rlogin

Operation	Command
Enable rlogin debugging	**debugging rlogin**
Disable rlogin debugging	**undo debugging rlogin**

11.10.4 Rlogin Configuration Example

I. Network requirements

Rlogin onto a UNIX server with the IP address of 192.168.0.200 as the user zhb, and abort the local session by pressing <Ctrl+K> or by entering a tilde (~) plus a dot (.), a local terminal escape sequence.

II. Network diagram

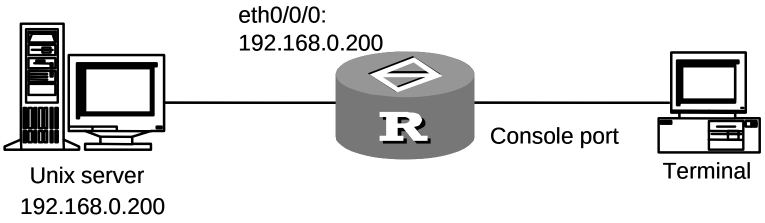


Figure 11-21 Network diagram for rlogin

III. Configuration procedure

1) Configure the Unix server

Add a user account zhb (skipped).

2) Configure the router

# Establish an rlogin connection.

```
<3Com> rlogin 192.168.0.200 zhb
Trying 192.168.0.200 ...
Press CTRL+K to abort

Connected to 192.168.0.200 ...
Password:
Password:
Last login: Thu Oct 28 17:30:23 from 192.168.0.5
bash: Path: command not found
[root@localhost zhb] #
```

# Disconnect the connection.

```
[root@localhost zhb] #
```

Enter a tilde (~) followed by a dot (.), or press <Ctrl+K>. The following is displayed:

```
The connection was closed by the local terminal!
```

Interface Operation

Table of Contents

Chapter 1 Interface Configuration Overview

1.1 Interface Overview

Router interface refers to the part through which a router system exchanges data and interacts with other devices on the network. It functions to accomplish the data exchange between the router and other network devices.

V 2.41 supports physical and logical interfaces on routers.

Physical interfaces are those that physically exist and have the supported components. Ethernet interfaces and synchronous/asynchronous serial interfaces are such examples. Physical interfaces include the LAN interface and the WAN interface. LAN interface mainly refers to the Ethernet interface through which a router exchanges data with other network devices on the local LAN. WAN interface mainly refers to the interface through which the router exchanges data with the network devices on an external network. WAN interfaces include synchronous/asynchronous serial interface, asynchronous serial interface, AUX interface, AM interface, CE1/PRI interface, and ISDN BRI interface. Through the WAN interfaces, the router can exchange data with external network devices.

Logical interface refers to the interface that can implement data exchange but does not physically exist and needs to be set up through configuration. It can be a dialer interface, subinterface, backup center logic-channel or virtual-template.

1.2 Interface Configuration

1.2.1 Interface View

Interface view is designed in the V 2.41 software for the convenience of configuration and maintenance. All the commands related to an interface can become valid only when they are used in the view of the interface.

I. Entering interface view

Perform the following configuration in system view to enter the specified interface view.

Table 1-1 Enter the specified interface view

Operation	Command
Enter specified interface view	**interface** *type number*

Note:

In V 2.41, the command used for entering the E1/T1 interface view is **controller** { **e1 | t1** }, which is different from those for entering other interface views.

II. Exiting interface view

Return to system view by executing the **quit** command in interface view.

1.2.2 Configuring Interface Description

In V 2.41, there is an interface description configuration entry for each physical interface on routers for identifying the function of the interface.

Perform the following configuration in interface view.

Table 1-2 Configure interface description

Operation	Command
Configure interface description	**description** *interface-description*
Restore the interface description to default	**undo description**

1.2.3 Configuring an Average Interface Rate Measurement Period

Perform the following configuration in system view to configure the interval for measuring the average rage of the interfaces.

Table 1-3 Configure an average interface rate measurement period

Operation	Command
Configure an average interface rate measurement period.	**flow-interval** *seconds*
Restore the default average interface rate measurement period.	**undo flow-interval** *seconds*

The default interval is 300 seconds.

1.2.4 Enabling/Disabling an Interface to Send UPDOWN Traps

Perform the following configuration in interface view.

Table 1-4 Enable/disable the interface to send UPDOWN traps

Operation	Command
Enable the interface to send UPDOWN traps	**enable snmp trap updown**
Disable the interface to send UPDOWN traps	**undo enable snmp trap updown**

By default, the interface can send UPDOWN traps.

1.2.5 Testing Interface/Line Loops

Loop test is available only on synchronous serial interfaces (including those formed on E1/T1/E1-F/T1-F interfaces) using SD701 chips.

Perform the following configuration in any view.

Table 1-5 Perform a loop test on an interface/line

Operation	Command
Perform a loop test on an interface/line	**looptest** [**-c** *count* | **-p** { *pattern* | **special** { **ascending** | **descending** | **random** } } | **-s** *packetsize* | **-t** *timeout*] * **interface** *type number*

By default, test packets are sent five times; test pattern is 0x55 interleaved with 0xAA; test packet size is 52 bytes with the 12-byte header excluded; and timeout waiting for receiving a sent test packet is 2000 milliseconds.

For a line with a low transmission speed, increase the timeout waiting for receiving a sent test packet.

1.2.6 Configuring Other Interface Parameters

Before configuring an interface, you should make sure that you have fully understood the networking requirements and the networking diagram. Configuring an interface includes the following tasks:

- If the interface is a physical one, you should specify its connection state, operating mode, and the relevant operating parameters.
- If the interface is a WAN interface, you should configure the link layer protocol agreed by the connected remote interface as well as the operating parameters.
- Assign a network protocol (such as IP) address to the interface
- Configure the static routing of the destination network reachable through the interface, or configure the working parameters of the dynamic routing protocol on the interface.

- If the interface supports dial-up, you should also configure parameters in Dial Control Center (DCC) operation and modem management.
- If the interface is working as a master interface or standby interface in the backup center, you should configure the relevant backup center operating parameters.
- If you want to set up a firewall on the interface, you should configure the parameters in packet filtering, address translation and so on.

Many parameters need to be configured in interface view. This part mainly introduces some specific parameter configurations of physical interfaces and makes a simple introduction to logical interfaces. For the sake of simplicity and clarity, this part will not cover the configuration in link layer and network layer protocols, their relevant parameters, and some special functions (such as dial, backup center, and firewall) that have been discussed in other parts of the manual.

1.3 Displaying and Debugging Interfaces

Table 1-6 Display and debug interfaces

Operation	Command
Display the current operating state and statistics of interfaces in any view	**display interface** [*type number*]
Display brief information on specified or all interfaces in any view	**display brief interface** [*type* [*number*]] [**|** { **begin** | **include** | **exclude**} *text*]
Display the major configuration information of interfaces in any view	**display ip interface** [*type number*]
Display state of an interface in any view	**display status interface** *interface-type interface-number*
Clear the interface statistic information in any view	**reset counters interface** [*type number*]
Shut down an interface in interface view	**shutdown**
Re-enable the interface in interface view	**undo shutdown**
Reset the interface in interface view.	**restart**
Enable debugging on the specified interface.	**debugging physical** { **all** | **error** | **event** | **packet** } [**interface** *interface-type interface-number*]
Disable debugging on the specified interface.	**undo debugging physical** { **all** | **error** | **event** | **packet** } **interface** *interface-type interface-number*

📖 **Note:**

When a physical interface on the router has no cable connection, shut down it with the **shutdown** command to prevent anomalies caused by interferences.

Chapter 2 LAN Interface Configuration

The local area network (LAN) mainly includes Ethernet and Token-Ring network. Currently, Ethernet has become the most important LAN networking technology thanks to its high flexibility, relative simplicity and easy implementation.

So far, LAN interfaces supported by V 2.41 are Ethernet interfaces which include the traditional Ethernet interface and the FE interface.

2.1 Ethernet Interface

2.1.1 Introduction to Ethernet Interface

I. Ethernet interface types

Fast Ethernet (FE) interfaces supported by 3Com Routers include electrical and optical interfaces, complying with 100Base-TX and 100Base-FX physical layer criteria respectively. The supported Gigabit Ethernet (GE) interfaces also include electrical and optical interfaces. GE electrical interfaces comply with 1000Base-T criterion, and GE optical interfaces comply with 1000Base-LX and 1000Base-SX criteria.

II. Operating speed and mode

FE electrical interfaces can work at the speeds of 10Mbps and 100Mbps; GE electrical interfaces can work at the speeds of 10Mbps, 100Mbps, and 1000Mbps.

In terms of operating modes, both FE and GE electrical interfaces support half and full duplex modes.

To simplify system configuration and management, both FE and GE electrical interfaces support auto-negotiation, allowing them to negotiate with other network devices for the optimum working modes and rates.

Optical interfaces can only work in full duplex modes and their speeds cannot be changed. FE optical interfaces can only work at the speed of 100Mbps and GE optical interfaces can only work at 1000Mbps.

III. Supported frame formats

Both FE and GE interfaces support the Ethernet frames in Ethernet_II or Ethernet_SNAP format, and can automatically identify their formats. They send frames in Ethernet_II format.

2.1.2 Ethernet Interface Configuration

Ethernet Interface configuration includes:

- Enter specified Ethernet interface view
- Set the network protocol address
- Configure Maximum Transmission Unit (MTU)
- Select the operating speed of Ethernet interface
- Select the operating mode of Ethernet interface
- Enable or disable loopback
- Configure flow-control mode of GE interface
- Configure the operating mode of GE interface
- Configure the operating mode of Ethernet interface

The specified Ethernet interface cannot be configured unless you enter its interface view. It is necessary to configure IP address. You are recommended not to enable other configuration tasks of Ethernet interface, as their default settings are enough for the normal operation of the system in most circumstances.

I. Entering specified Ethernet interface view

Perform the following configuration in system view.

Table 2-1 Enter the specified Ethernet interface view

Operation	Command
Enter the specified Ethernet interface view	**interface ethernet** *number*
Enter GE interface view	**interface gigabitethernet** *interface-number*

II. Setting network protocol address

Perform the following configuration in Ethernet interface view.

Table 2-2 Assign an IP address to the interface

Operation	Command
Assign an IP address to the interface	**ip address** *ip-address mask* [**sub**]
Remove the IP address of the interface	**undo ip address** [*ip-address mask*] [**sub**]

When an Ethernet interface is configured with two or more IP addresses, use the keyword "**sub**" to identify the second one and those behind it (that is, the secondary IP addresses).

III. Configuring MTU

The configuration of MTU can affect the fragment and reassembly of IP packets.

Perform the following configuration in Ethernet interface view.

Table 2-3 Configure MTU

Operation	Command
Configure MTU	**mtu** *size*
Restore MTU to default	**undo mtu**

The frame format defaults to Ethernet_II and MTU size is in the range 46 to 1500 bytes. The default MTU size is 1500 bytes.

📖 **Note:**

MTU only affects IP packet assembly/disassembly. MTU can reach 1500 bytes in the Ethernet_II format.

Since QoS queue length is limited, too small MTU and too big packet may result in many fragments and QoS queues discarding packets. To avoid this, you can increase QoS queue length. By default, the queue scheduling mechanism adopted on the interfaces of 3Com Routers is FIFO. You can use the **qos fifo queue-length** command to change the queue length. For detailed QoS queue configuration, see the section of QoS configuration in this manual.

IV. Selecting operating speed of Ethernet interface

Ethernet interfaces support multiple speeds. FE electrical interfaces support 10Mbps and 100Mbps. FE optical interfaces only support 100Mbps. GE electrical interfaces support 10Mbps, 100Mbps, and 1000Mbps. GE optical interfaces can only work at 1000Mbps. Thus, you only need to configure Ethernet electrical interfaces while do not need to configure optical interfaces.

Perform the following configuration in Ethernet interface view.

Table 2-4 Select an operating speed for an Ethernet interface

Operation	Command
Select an operating speed for the FE interface	**speed** { **10** | **100** | **negotiation** }
Configure the operating speed for a GE electrical interface	**speed** { **10** | **100** | **1000** | **negotiation** }
Restore the default operating speed	**undo speed**

By default, **negotiation** is selected, i.e., the system automatically chooses an optimum operating speed.

📖 **Note:**

- By default, both operating speeds and modes of FE and GE electrical interfaces are **negotiation**. You can force to change the operating speeds and modes, but should keep the speed and mode the same as those of the peer end.
- If you force to execute the **duplex negotiation** or **speed negotiation** command, the Ethernet electrical interfaces are set to the **negotiation** mode, and negotiate speed and duplex mode.
- In terms of GE electrical interfaces, the operating speed 1000Mbps and half-duplex mode are mutually exclusive. Thus, you cannot set these two values at the same time.

V. Selecting an operating mode for an Ethernet interface

As mentioned earlier, an Ethernet interface can work at both full-duplex mode and half-duplex mode. Connected to a hub, the Ethernet interface on a router must be specified to work in half-duplex mode. Connected to a LAN Switch, however, it must be specified to work in full-duplex mode. Both FE and GE electrical interfaces support these two modes, whereas FE and GE optical interfaces can only work in full-duplex mode.

Perform the following configuration in Ethernet interface view to select an operating mode.

Table 2-5 Select an operating mode for the FE interface

Operation	Command
Select an operating mode for the FE interface	**duplex** { **negotiation | full | half** }

By default, **negotiation** is set on both FE and GE electrical interfaces. That is, the system automatically negotiates an optimum operating mode.

📖 **Note:**

In terms of GE electrical interfaces, the operating speed 1000Mbps and half-duplex mode are mutually exclusive. Thus, you cannot set these two values at the same time.

VI. Enabling or disabling loopback

Sometimes, you need to enable local loop on an interface for testing some special functions. Perform the following configuration in Ethernet interface view to enable an interface to make local loopback.

Table 2-6 Enable or disable local loopback

Operation	Command
Enable local loopback	**loopback**
Disable local loopback	**undo loopback**

By default, local loop is disabled.

🕮 **Note:**

- Ethernet interfaces will work in full-duplex mode when loopback is enabled.
- If the operating speed is 1000Mbps or **negotiation**, the system will force to convert it to 100Mbps when loopback is enabled. In addition, it will restore the original setting when loopback is disabled.
- When loopback is enabled, you can change the GE operating speed to 10Mbps or 100Mbps. If the new speed is different from the current speed, it starts loopback in the new speed and saves the new configuration. In other cases (GE operating speed is changed to 1000Mbps or negotiation, or operating mode is changed to half-duplex mode), the new configuration is saved. It disables loopback and starts to work in the new mode.

VII. Configuring Flow Control on an Ethernet Interface

Perform the following configuration in Ethernet interface view.

Table 2-7 Configure flow control on the Ethernet interface

Operation	Command
Enable flow control on the Ethernet interface.	**flow-control**
Restore the default.	**undo flow-control**

By default, flow control is disabled. Flow control can take effective only when it is enabled at both ends.

When flow control is enabled, the system cannot enter normal UP state if negotiation fails. If flow control is enabled on the local interface, you are recommended to execute the **shutdown** command and then the **undo shutdown** command to restart the interface when the configuration of the peer end changes, to keep the flow control mode the same on both ends.

VIII. Configuring the operating mode of a GE interface

GE optical interfaces provide two operating modes: negotiation and force. In negotiation mode, the interface chip checks negotiation code, negotiating the format of the PAUSE frame and the peer state (that is, whether it is faulty). In force mode, no negotiation stream is present on the line. The interface chip decides whether an interface can be brought up depending on how much light intensity it reads.

You must set the two ends to work in the same operating mode. Any inconsistency can prevent the interface adopting negotiation mode from going up.

Perform the following configuration in GE interface view.

Table 2-8 Configure the operating mode of the GE interface

Operation	Command
Configure the GE interface to operate in force mode.	**force-link**
Restore the default.	**undo force-link**

The default operating mode is negotiation.

IX. Configuring the operating mode of an Ethernet interface

Perform the following configuration in Ethernet interface.

Table 2-9 Configure the operating mode of the Ethernet interface

Operation	Command
Set the operating mode of the Ethernet interface to promiscuous.	**promiscuous**
Disable the Ethernet interface to operate in promiscuous mode.	**undo promiscuous**

By default, the Ethernet interface is operating in non-promiscuous mode.

When the Ethernet interface is operating in promiscuous mode, it receives all correct Ethernet packets without checking their MAC addresses, This mode is configured when network listening applies.

After you enable the bridging function on an Ethernet interface and adds it to a bridge-set, the interface enters promiscuous mode automatically. After removed from the bridge-set, the interface enters non-promiscuous mode automatically.

2.1.3 Displaying and Debugging Ethernet Interface

Perform the following configuration in any view.

Table 2-10 Display the state of a specified Ethernet interface

Operation	Command
Display the state of a specified Ethernet interface	**display interface** { **ethernet** | **gigabitethernet** } [*interface-number*]

2.1.4 Ethernet Configuration Example

I. Networking requirements

As shown in the following figure, the Ethernet interface on Router A is connected to the IP network 192.168.0.0. The computers on the LAN are connected to the Internet via Router A. Set the MTU on the Ethernet interface to 1492 bytes.

II. Networking diagram

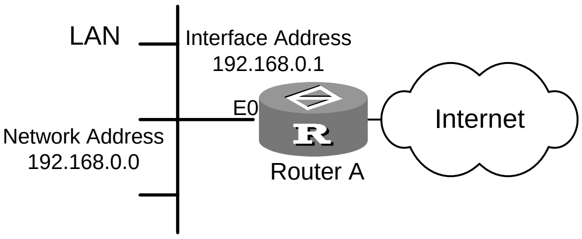


Figure 2-1 Networking diagram of Ethernet configuration example

III. Configuration procedure

# Assign the IP address 192.168.0.1 to Ethernet 0/0/0, given the mask is 255.255.0.0.

```
[3Com] interface ethernet 0/0/0
[3Com-Ethernet0/0/0] ip address 192.168.0.1 255.255.0.0
```

# Set the MTU on the interface to 1492 bytes.

```
[3Com-Ethernet0/0/0] mtu 1492
```

2.1.5 Troubleshooting

You can perform the following operations to determine the correctness of the Ethernet interface.

- Ping the Ethernet interface on the router from a host locating on the same LAN, anticipating that all the packets can be correctly returned.
- Look up the statistics of the connected two parties (router and switch for example), anticipating that the received error frames have not rapidly increased.

If the test result of either item is incompliance with the anticipation, you can conclude that the Ethernet interface or its connection is not properly working.

After confirming the existence of a fault, you can isolate it following these steps:

Step: Check that the LAN connection between the host and the router is correct.

If the Ethernet is connected to a hub or LAN Switch, check the ON/OFF status of the LEDs for the link to the hub or LAN Switch. ON LEDs mean that the Ethernet interface between the host and the router and the network cable are physically normal. Otherwise, please replace such physical devices as the network adapter, network cable, router or the relevant interface module.

If the Ethernet is connected using Unshielded Twisted Pair (UTP) and if at least one of the connection parties supports 100Base-TX, rate matching must be taken into consideration. An operating rate mismatch between the two parties, i.e., one is working at 100 Mbps and the other at 10 Mbps, will cause faults. From the perspective of the one working at 100 Mbps, no connection can be set up. From the perspective of the one working at 10 Mbps, the connection can be set up but the physical layer activity LED (ACTIVE) will keep blinking quickly and data transmission and receipt cannot be carried out properly.

When looking for the connection problems of FE interface on 3Com Series Routers, there are two prompt messages that are very helpful. These two messages are displayed on the Console screen upon your operation of selecting speed or connecting network.

```
Ethernet 0/0/0: Warning--the link partner do not support 100M mode
Ethernet 0/0/0: Warning--the link partner may not support 10M mode
```

The first prompt message indicates that the Ethernet interface on the 3Com Series Router has detected that the remote end does not support 100Mbps operating speed, but the local end is forced to work at 100Mbps. In this case, you should ensure the remote end to make the same configuration so that it can work at 100 Mbps. The second prompt message indicates that the Ethernet interface on the 3Com Series Router has detected that the remote end does not support 10Mbps operating speed, but the local end is forced to work at 10 Mbps. In this case, the user should ensure that the remote end could work at 10 Mbps. However, when the FE interface on 3Com Series Routers is connected to the 10/100 Mbps adaptive port of the hub, this information does not mean setting is incorrect.

Step 2: View whether IP addresses of the Ethernet interfaces of the host and router are in the same subnet. In other words, they must use the same network address but different host addresses. If they are not in the same subnet, please set a new IP address.

Step 3: Check that the operating mode of the Ethernet interface is correct. When the Ethernet is connected using UTP or fiber, 10Base-T/100Base-TX/100Base-FX standard provisions two operating modes, that is, full duplex and half duplex. When a hub is used for connecting the Ethernet, the interface should work in half-duplex mode. When a LAN Switch working in half duplex mode is used, the Ethernet interface of the router must also work in half duplex mode. If the LAN Switch is working in full duplex mode, the Ethernet interface of the router must also work in full duplex mode. If the operating mode is incorrect, i.e. one party of the connection is working in full duplex mode while the other party in half duplex mode, fault will occur. That is, when the network traffic increases, the party operating in half duplex mode shows frequent network collisions. For example, if Hub is connected, all the other devices in the whole network segment will have serious network collisions. The party operating in full duplex mode will receive a large amount of error messages, accompanied with serious message losses at both parties. In this case, use **display interface ethernet** command to view the error ratio of transmitting and receiving messages on the Ethernet interface. Usually, the collision can be observed through the state LEDs of the Ethernet interface.

Step 4: Check that flow-control mode of Ethernet interface is correct.

By default, negotiation flow-control is adopted in Ethernet interface. If forced flow-control mode is used at the peer end, the interface might not be able to go up. In this case, please keep the flow-control mode the same at both ends. Restart the interface using the **shutdown** and **undo shutdown** commands.

Contact our technical support engineers if you still cannot locate the problem by using the above methods.

Chapter 3 Layer 2 Ethernet Port Configuration

3.1 Introduction to Layer 2 Ethernet Ports

The legacy routers are only operating at layer 3. Now, the use of switching chips on routers allows the AR 18-22-24 and the AR 28/46, through an 8-/16-port layer 2 switching interface module/card (8LS/16LS or FIC-8LS/FIC-16LS), to implement layer 2 switching, providing more 10/100 Base-Tx Ethernet ports. They are nice and cost effective switching-routing integrated devices on an enterprise network for providing connectivity between the PCs and network devices on the network.

The layer 2 Ethernet ports support:

- Layer 2 forwarding
- Broadcast storm suppression
- MAC address aging
- Port-based VLAN (802.1Q)

These layer 2 Ethernet ports however do not support:

- STP/MSTP/RSTP (Loop prevention must be considered at the time of networking.)
- Link aggregation
- RMON statistics

Ethernet is a medium sharing data network communications technology based on the access method of carrier sense multiple access/collision detect (CSMA/CD). On a small local area network (LAN), it can work well. On a large LAN, however, the likelihood exists that the network be overwhelmed by collisions and broadcasts. The worst case is the paralysis of the entire network. Using switches to provide LAN interconnectivity eliminates collisions, but the problem of broadcast storms still exists. Virtual LAN (VLAN) technology was thus developed. It divides a LAN into smaller logical LANs called VLANs, each being a broadcast domain. The hosts on a VLAN can communicate with each other as they would on a LAN but they cannot communicate with the hosts on other VLANs. Thus, broadcasts are restricted to a VLAN, as shown in the following figure:

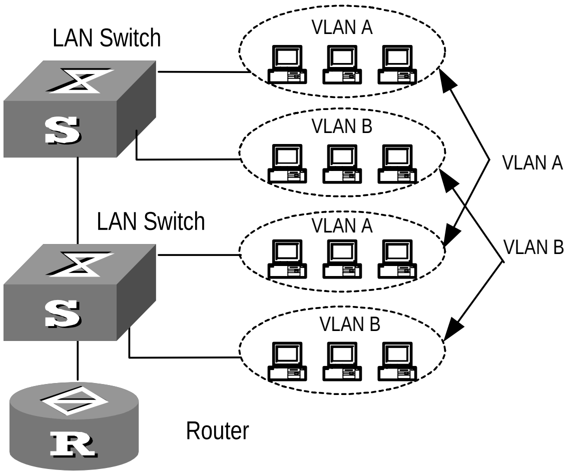


Figure 3-1 VLAN

VLANs can be port-based, MAC-based, protocol-based, IP map-based, multicast-based, or policy-based.

Currently, the routers support port-based VLAN on their layer 2 Ethernet ports. Given the AR 18-22-24, port-based VLAN is implemented within the scope of the 24 layer 2 switching ports; given the AR 28/46, port-based VLAN is implemented within the scope of the 8/16 layer 2 switching ports.

The benefits of VLANs include:

- Suppressing broadcast storms, saving bandwidth resources, and improving the processing capability of the network
- Enhancing communication security on LANs, because the interconnectivity of VLANs is provided at layer 3 by routers or switches.

3.2 Configuring Ethernet Ports

The Ethernet port configuration tasks are described in the following sections:

- Entering Ethernet Port View
- Enabling/Shutting Down the Ethernet Port
- Configuring Ethernet Port Description
- Setting the Duplex Mode of the Ethernet Port
- Setting the Speed of the Ethernet Port
- Enabling/Disabling Flow Control on the Ethernet Port
- Setting the Link Type of the Ethernet Port
- Setting the MAC Address Aging Timer
- Configuring a Broadcast Suppression Ratio on the Ethernet Port
- Enabling/disabling Loopback on the Ethernet Port
- Assigning the Ethernet Port to a VLAN
- Assigning a Default VLAN ID to the Ethernet Port

3.2.1 Entering Ethernet Port View

Before you can configure an Ethernet port, you must enter its view first.

Perform the following configuration in system view.

Table 3-1 Enter Ethernet port view

Operation	Command
Enter Ethernet port view	**interface** { *interface_type* *interface_num* | *interface_name* }

📖 **Note:**

The following are the interface numbering conventions for the AR 18-22-24 Router and the 8LS/16LS interface module:

- Given the AR 18-22-24, Ethernet *slot*/1 through Ethernet *slot*/24 are Layer 2 Ethernet ports. Ethernet *slot*/0 is a layer 3 virtual interface; you can assign an IP address to it and configure subinterfaces on it. The *slot* argument must be set to 3.
- Given the 8LS/16LS or FIC-8LS/FIC-16LS on the AR 28/46, Ethernet *slot*/0/0 through Ethernet *slot*/0/7 or through Ethernet *slot*/0/5 are Layer 2 Ethernet ports. Ethernet *slot*/0/8 or Ethernet *slot*/0/16 is a layer 3 virtual interface; you can assign an IP address to it and configure subinterfaces on it. The *slot* argument is the number of the actual slot that holds the interface module/card.
- The **vlan-type dot1q vid 1** command is not available on the subinterfaces on layer 3 virtual interfaces. Thus, these subinterfaces cannot forward packets for VLAN 1.

3.2.2 Enabling/Shutting Down the Ethernet Port

After you finish the configuration of a port, you may use the **undo shutdown** command to enable it. If you want to disable the port to forward data, you may shut it down using the **shutdown** command.

Perform the following configuration in Ethernet port view.

Table 3-2 Enable/shut down the Ethernet port

Operation	Command
Shut down the Ethernet port	**shutdown**
Enable the Ethernet port	**undo shutdown**

By default, the port is enabled.

3.2.3 Configuring Ethernet Port Description

To distinguish a port from others, you may configure a port description for it.

Perform the following configuration in Ethernet port view.

Table 3-3 Configure port description

Operation	Command
Configure port description.	**description** *text*
Restore the defaut port description.	**undo description**

The default port description is port name plus interface.

3.2.4 Setting the Duplex Mode of the Ethernet Port

To have a port receive packets while sending packets, set its duplex mode to full. To have the port only receive or send packets at a time, set its duplex mode to half. To allow the port to negotiate duplex mode with the connected port, set its duplex mode to negotiation.

Perform the following configuration in Ethernet port view.

Table 3-4 Set the duplex mode of the Ethernet port

Operation	Command
Set the duplex mode of the Ethernet port	**duplex** { **full | half | negotiation** }
Restore the default duplex mode of the Ethernet port	**undo duplex**

3.2.5 Setting the Speed of the Ethernet Port

You may set the speed of an Ethernet port. In auto-negotiation mode, the port negotiates its speed automatically with the connected port.

Perform the following configuration in Ethernet port view.

Table 3-5 Set the speed of the Ethernet port

Operation	Command
Set the speed of the Ethernet port	**speed** { **10 | 100 | negotiation** }
Restore the defaut speed of the Ethernet port	**undo speed**

The default port speed setting is **negotiation**.

3.2.6 Enabling/Disabling Flow Control on the Ethernet Port

To prevent packet loss, you may enable flow control. When congestion occurs to one of the two connected routers enabled with flow control, it sends a message asking the peer to stop packet sending. As requested, the peer pauses until it is allowed to send packets again.

Perform the following configuration in Ethernet port view.

Table 3-6 Enable/disable flow control

Operation	Command
Enable flow control on the Ethernet port	**flow-control**
Disable flow control on the Ethernet port	**undo flow-control**

By default, flow control is disabled on the port.

3.2.7 Setting the Link Type of the Ethernet Port

The link type of an Ethernet port can be access, hybrid, or trunk.

Access ports are intended for connecting PCs and they can be assigned to one VLAN only.

Trunk ports are intended for connecting routers and they can be assigned to multiple VLANs.

Hybrid ports can connect both routers and PCs and they can be assigned to multiple VLANs.

The last two types of ports are different in that a hybrid port allows the packets from multiple VLANs to be sent untagged, but a trunk port only allows the packets from the default VLAN to be sent untagged.

Perform the following configuration in Ethernet port view.

Table 3-7 Set the link type of the Ethernet port

Operation	Command
Set the link type of the port to access.	**port link-type access**
Set the link type of the port to hybrid.	**port link-type hybrid**
Set the link type of the port to trunk.	**port link-type trunk**
Restore the default link type of the port, that is, access.	**undo port link-type**

The default link type of the port is access.

3.2.8 Setting the MAC Address Aging Timer

An appropriately configured aging timer can effectively implement the function of MAC address aging.

An inappropriate aging timer, however, either too long or too short, may cause the router to broadcast packets with unknown destination MAC addresses, degrading the performance. If the aging time is too long, the MAC address table on the router may become filled up with out-of-date entries, failing to accommodate to the changes on the network. If the aging time is too short, the router may delete valid entries.

Normally, you are recommended to use the default MAC address aging time, that is, 300 seconds.

Perform the following configuration in Ethernet port view.

Table 3-8 Set the MAC address aging timer

Operation	Command
Set the MAC address aging time	**mac-address timer aging** {*age-time* | **no-age**}
Restore the default MAC address aging timer setting.	**undo mac-address timer aging**

The default MAC address aging timer is set to 300 seconds.

3.2.9 Configuring a Broadcast Suppression Ratio on the Ethernet Port

To suppress broadcast storms and avoid congestion, you may configure the permitted broadcast traffic size on a port. Once broadcast traffic exceeds the specified value, the system starts discarding broadcast packets until the broadcast traffic decreases to the acceptable degree.

In the **broadcast-suppression** *pct* command, how much broadcast traffic can pass through depends on the specified maximum wire speed ratio of the broadcast traffic on the port. As this ratio is decreasing, the permitted broadcast traffic size decreases. When the ratio is set to 100, all broadcast traffic can pass through without suppression.

Perform the following configuration in Ethernet port view.

Table 3-9 Configure a broadcast suppression ratio on the Ethernet port

Operation	Command
Configure a broadcast suppression ratio on the Ethernet port	**broadcast-suppression** *pct*
Restore the default broadcast suppression ratio on the Ethernet port	**undo broadcast-suppression**

By default, all broadcast traffic can pass through without suppression.

3.2.10 Enabling/disabling Loopback on the Ethernet Port

You may enable loopback on an Ethernet port to test whether the port is operating normally.

Perform the following configuration in Ethernet port view.

Table 3-10 Enable/disable loopback on the Ethernet port

Operation	Command
Enable loopbck on the port.	**loopback**
Disable loopback on the port.	**undo loopback**

By default, loopback is disabled on the port.

You need enable loopback on a port only for some special tests.

3.2.11 Assigning the Ethernet Port to a VLAN

You may assign an Ethernet port to a VLAN. When doing this, note that while you may assign a hybrid or trunk port to multiple VLANs, you may assign an access port to one VLAN only.

Perform the following configuration in Ethernet port view.

Table 3-11 Assigning the port to the specified VLAN or VLANs

Operation	Command
Assign the access port to the specified VLAN.	**port access vlan** *vlan_id*
Assign the hybrid port to the specified VLAN or VLANs.	**port hybrid vlan** *vlan_id_list* { **tagged** | **untagged** }
Assign the trunk port to the specified VLAN or VLANs.	**port trunk permit vlan** { *vlan_id_list* **|** **all** }
Remove the access port from the specified VLAN.	**undo port access vlan**
Remove the hybrid port from the specified VLAN or VLANs.	**undo port hybrid vlan** *vlan_id_list*
Remove the trunk port from the specified VLAN or VLANs.	**undo port trunk permit vlan** { *vlan_id_list* **|** **all** }

Note that you cannot assign an access port to VLAN 1.

After assigned to a VLAN, the Ethernet port can forward the packets from the VLAN. If the port is hybrid or trunk, you may assign it to multiple VLANs, allowing each VLAN to communicate with its counterpart on the connected router or switch. You may configure a hybrid port to tag a packet or not to tag it depending on from which VLAN it comes. This allows the router to handle packets on a per-VLAN basis.

3.2.12 Assigning a Default VLAN ID to the Ethernet Port

As an access port can be assigned to one VLAN only, its default VLAN is the VLAN to which it is assigned. For a hybrid or trunk port which may belong to multiple VLANs however, you need to assign a default VLAN ID. When the port receives an untagged packet, it forwards the packet to the port assigned to the default VLAN. When the port receives a packet with the assigned default VLAN ID, it forwards the packet with the tag removed.

Perform the following configuration in Ethernet port view.

Table 3-12 Assign a default VLAN ID to the Ethernet port

Operation	Command
Assign a default VLAN ID to the hybrid port.	**port hybrid pvid vlan** *vlan_id*
Assign a default VLAN ID to the trunk port.	**port trunk pvid vlan** *vlan_id*
Restore the default of the default VLAN ID of the hybrid port.	**undo port hybrid pvid**
Restore the default of the default VLAN ID of the trunk port.	**undo port trunk pvid**

To ensure the correct transmission of packets, you must ensure that the default VLAN ID assigned to this hybrid or trunk port must be the same as the one assigned to the connected hybrid or trunk port.

The default VLAN to which the hybrid or trunk port is assigned defaults to VLAN 1. The default VLAN for the access port is the VLAN to which it belongs.

3.3 Displaying and Debugging Ethernet Ports

After completing the configuration tasks, execute the **display** command in any view to display the running state about the Ethernet ports for effect verification.

Execute the **reset** command in user view to clear the statistics about Ethernet ports.

Table 3-13 Display and debug Ethernet ports

Operation	Command
Display all information about the specified Ethernet port.	**display interface** { **ethernet** | **gigabitethernet** } [*interface-number*]

Operation	Command
Display hybrid or trunk ports.	**display port** { **hybrid** | **trunk** }
Clear the statistics about the specified Ethernet port or all ports.	**reset counters interface** [*interface-type* [*interface-number*]]

🕮 **Note:**

The **display vlan** command displays information about VLANs for Ethernet subinterfaces but not for layer 2 Ethernet ports.

3.4 Ethernet Port Configuration Example

3.4.1 VLANs Involving One Network Segment

I. Network requirements

As shown in the following diagram, the ports on the AR 18-22-24 Router are configured with VLAN properties. PCs 1 through 4 are on the same network segment. PC 1 and PC 2 are connected to ports Ethernet3/0/1 and Ethernet3/0/2; they belong to VLAN 10. PC 3 and PC 4 are connected to ports Ethernet 3/0/3 and Ethernet 3/0/4; they belong to VLAN 20. The two VLANs on the same network segment cannot communicate with each other.

Do the following:

- Assign an IP address to interface Ethernet3/0/0, ensuring that this address is on the same segment to which the host is connected.
- Allow PC 1 and PC 2 to communicate with each other, so do PC 3 and PC 4.
- Forbid PC 1 and PC 2 to communicate with PC 3 and PC 4.

II. Network diagram

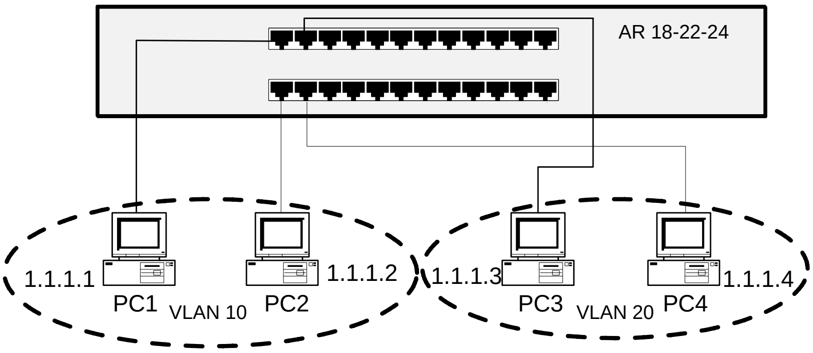


Figure 3-2 VLANs involving one network segment

III. Configuration procedure

Enter the view of each involved Ethernet port, specify its link type, and assign the port to the specified VLAN. If the link type of the port is already access, you can omit the **port link-type access** command.

# Configure Ethernet 3/0/1.

```
[3Com] interface ethernet 3/0/1
[3Com-Ethernet3/0/1] port link-type access
[3Com-Ethernet3/0/1] port access vlan 10
```

# Configure Ethernet 3/0/2.

```
[3Com] interface ethernet 3/0/2
[3Com-Ethernet3/0/2] port link-type access
[3Com-Ethernet3/0/2] port access vlan 10
```

# Configure Ethernet 3/0/3.

```
[3Com] interface ethernet 3/0/3
[3Com-Ethernet3/0/3] port link-type access
[3Com-Ethernet3/0/3] port access vlan 20
```

# Configure Ethernet 3/0/4.

```
[3Com] interface ethernet 3/0/4
[3Com-Ethernet3/0/4] port link-type access
[3Com-Ethernet3/0/4] port access vlan 20
```

# Configure virtual Ethernet interface Ethernet 3/0/0.

```
[3Com] interface Ethernet 3/0/0
[3Com-Ethernet3/0/0.1] ip address 1.1.1.5  255.255.255.0
```

3.4.2 VLANs Involving Multiple Network Segments

I. Network requirements

As shown in the following diagram, the ports on the router are configured with VLAN properties. PC 1 and PC 2 are connected to ports Ethernet 3/0/1 and Ethernet 3/0/2; they belong to VLAN 10. PC 3 and PC 4 are connected to ports Ethernet 3/0/3 and Ethernet 3/0/4; they belong to VLAN 20. The two VLANs are located on different network segments and cannot communicate with each other.

Do the following:

- Assign an IP address to interface Ethernet 3/0/0, ensuring that this address is on the same segment to which the host is connected.
- Allow PC 1 and PC 2 to communicate with each other, so do PC 3 and PC 4.
- Allow the four PCs to communicate with each other.

II. Network diagram

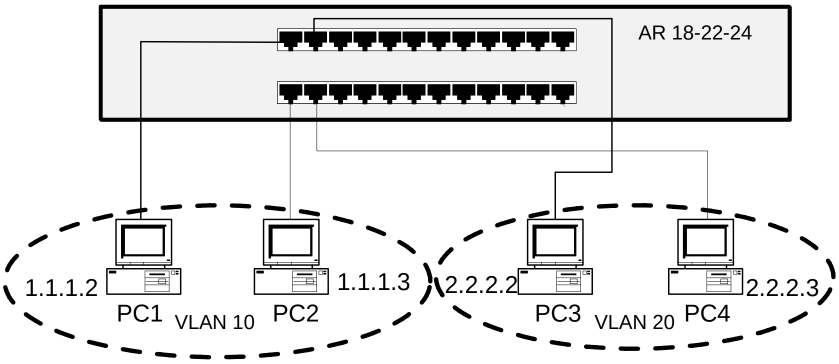


Figure 3-3 VLANs involving multiple network segments

III. Configuration procedure

Enter the view of each involved Ethernet port, specify its link type, and assign the port to the specified VLAN.

# Configure Ethernet3/0/1

```
[3Com] interface ethernet 3/0/1
[3Com-Ethernet3/0/1] port link-type access
[3Com-Ethernet3/0/1] port access vlan 10
```

# Configure Ethernet 3/0/2

```
[3Com] interface ethernet 3/0/2
[3Com-Ethernet3/0/2] port link-type access
[3Com-Ethernet3/0/2] port access vlan 10
```

# Configure Ethernet 3/0/3

```
[3Com] interface ethernet 3/0/3
[3Com-Ethernet3/0/3] port link-type access
[3Com-Ethernet3/0/3] port access vlan 20
```

# Configure Ethernet 3/0/4

```
[3Com] interface ethernet 3/0/4
[3Com-Ethernet3/0/4] port link-type access
[3Com-Ethernet3/0/4] port access vlan 20
```

To have VLAN 10 and VLAN 20 communicate with each other, you must configure Ethernet subinterfaces for them for routing purpose. For each VLAN, create a subinterface and enter its view, run the protocol to be used, associate the VLAN ID to the subinterface, and assign an IP address and mask.

Do the following:

# Configure Ethernet 3/0/0.1

```
[3Com] interface Ethernet 3/0/0.1
[3Com-Ethernet3/0/0.1] vlan-type dot1q vid 10
[3Com-Ethernet3/0/0.1] ip address 1.1.1.1 255.255.255.0
```

# Configure Ethernet3/0/0.2

```
[3Com] interface Ethernet 3/0/0.2
[3Com-Ethernet3/0/0.2] vlan-type dot1q vid 20
[3Com-Ethernet3/0/0.2] ip address 2.2.2.1 255.255.255.0
```

3.4.3 VLANs Involving Multiple Devices

I. Network requirements

As shown in the following diagram, the router is connected to a switch that supports 802.1Q-compliant VLAN. Configure the router and the switch each with a trunk carrying multiple VLANs.

PC 1 and PC 2 are connected to port Ethernet 3/0/1 and port Ethernet 3/0/2 on the router; they belong to VLAN 10 and VLAN 20 respectively.

PC 3 and PC 4 are connected to port Ethernet 0/0/1 and port Ethernet 0/0/2 on the switch; they belong to VLAN 10 and VLAN 20 respectively.

Port Ethernet 3/0/22 on the router is connected to port Ethernet0/0/3 on the switch using a network cable. Set the link type to trunk on them.

Do the following:

- Allow PC 1 and PC 3 to communicate with each other, so do PC 2 and PC 4.
- Forbid PC 1 and PC 3 to communicate with PC 2 and PC 4.

II. Network diagram

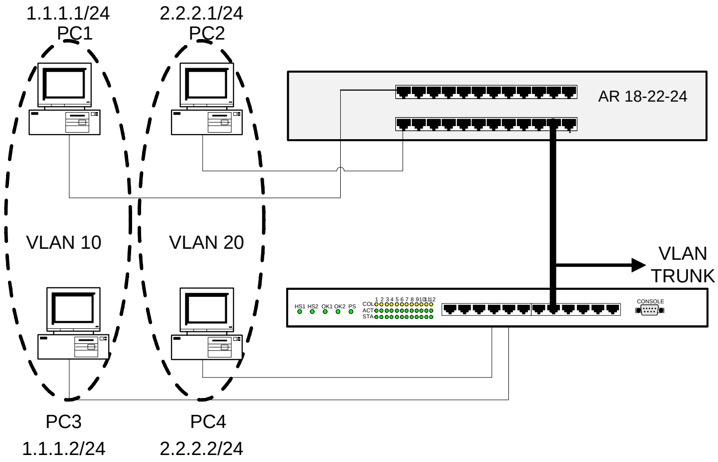


Figure 3-4 VLANs involving multiple devices

III. Configuration procedure

- Configure the router

# Configure Ethernet 3/0/1

```
[3Com] interface Ethernet 3/0/1
[3Com-Ethernet3/0/1] port link-type access
[3Com-Ethernet3/0/1] port access vlan 10
```

# Configure Ethernet 3/0/2

```
[3Com] interface Ethernet 3/0/2
[3Com-Ethernet3/0/2] port link-type access
[3Com-Ethernet3/0/2] port access vlan 20
```

# Configure a trunk on the router.

```
[3Com] interface Ethernet 3/0/22
[3Com-Ethernet3/0/22] port link-type trunk
[3Com-Ethernet3/0/22] port trunk permit vlan 10 20
```

- Configure the switch

# Configure Ethernet 0/0/1

```
[3Com] interface Ethernet 0/0/1
[3Com-Ethernet0/1] port link-type access
[3Com-Ethernet0/1] port access vlan 10
```

# Configure Ethernet 0/0/2

```
[3Com] interface Ethernet 0/0/2
[3Com-Ethernet0/2] port link-type access
[3Com-Ethernet0/2] port access vlan 20
```

# Configure a trunk on the switch

```
[3Com] interface Ethernet 0/0/3
[3Com-Ethernet0/0/3] port link-type trunk
[3Com-Ethernet0/0/3] port trunk permit vlan 10 20
```

3.5 Troubleshooting Ethernet Ports

Symptom:

Failed to assign a default VLAN ID to a port.

Solution:

Check that the link type of the port is hybrid or trunk by using the **display interface** command or the **display port** command.

Assign a default VLAN ID to the port.

Chapter 4 Logical Interface Configuration

Logical interfaces are virtual interfaces that can be created to exchange data, such as dialer, subinterface, loopback, NULL, MP-group, MFR, virtual template, and backup center logical channel.

4.1 Dialer Interface

4.1.1 Introduction to Dialer Interface

As the name implies, a Dialer interface is used for the dialing purpose. The dial-supported interfaces available for 3Com Series Routers include synchronous serial interface, asynchronous serial interface, ISDN BRI interface, and ISDN PRI interface. V 2.41 has implemented the DCC (Dialup Control Center) function. In addition, V 2.41 provides the users with two DCC configuration approaches, specifically, Circular DCC (C-DCC) and Resource-Shared DCC (RS-DCC), so that the users can make full use of the DCC function and various Dialer interfaces.

See Dialup Configuration module of this manual for details about configuring polling DCC and shared DCC, displaying and debugging, configuration example, troubleshooting.

4.2 Loopback Interface

4.2.1 Introduction to Loopback Interface

The TCP/IP suite provisions that the addresses in the 127.0.0.0 segment are loopback addresses. The interfaces at such addresses are called loopback interfaces. As far as a 3Com Series Router is concerned, the interface Loopback0 is the loopback interface for receiving all the packets sent to the local routers.

In some applications (such as configuring local peers in an SNA), there is often the need to assign a fixed IP address to a local interface without affecting the physical interface configuration. To save the scarce IP address resources, this IP address must be an address of 32-bit mask and must be advertised through a routing protocol. The Loopback interface is introduced for satisfying such a need.

4.2.2 Configuring a Loopback Interface

Perform the following tasks to configure a loopback interface:

- Create a loopback interface
- Configure the operating parameters of the interface

I. Creating a loopback interface

Table 4-1 Create/delete a loopback interface

Operation	Command
Create a loopback interface and enter the loopback interface view	**interface loopback** *number*
Delete the specified loopback interface	**undo interface loopback** *number*

II. Configuring the operating parameters of the interface

You can configure the parameters like IP address and IP routing for a loopback interface. For details, refer to *V 2.41 Operation Manual - Network Protocol*.

⚠ **Caution:**

You can configure a 32-bit subnet mask for a loopback interface. that is, the subnet mask can be 255.255.255.255. In addition, the IP address with the 32-bit mask can be advertised through a routing protocol.
You are recommended to assign a host address of 32-bit mask to a loopback interface. In this way, you can not only save the address resources but also use the interface as an unnumbered interface.
You can use the shutdown command to disable the loopback interface.

4.3 Null Interface

4.3.1 Introduction to Null Interface

3Com Series Routers support the Null interface. Such an interface is always UP but cannot forward packets. In addition, no IP address or other link layer protocols can be configured on it.

Null interface is the logical interface of pure software property. Therefore, all the network specific packets sent to the interface will be dropped.

4.3.2 Configuring a Null Interface

Perform the following configuration in system view to create the interface Null 0 on a 3Com router.

Table 4-2 Create/delete a Null interface

Operation	Command
Create a Null interface and enter the Null interface view	**interface null 0**
Delete the Null interface	**undo interface null 0**

As a Null interface drops all the packets reaching it, it provides you with a means of packet filtering. You can simply make the configuration to send all the undesired network traffic to the interface Null0 rather than bothering yourself with the complex work of configuring ACL (Access Control List).

For example, you can drop all the packets destined to the segment 192.101.0.0 by configuring the static routing command **ip route-static 192.101.0.0 255.255.0.0 null 0**.

4.4 Subinterface

4.4.1 Introduction to Subinterface

Introducing the concept of subinterface into V 2.41 allows the users of 3Com Series Routers of high flexibility as the users can configure multiple subinterfaces on a single physical interface in this case.

Subinterfaces are the logical virtual interfaces configured on a physical interface. They share the physical layer parameters of the physical interface and can be separately configured with the link layer and network layer parameters. As they can be associated with a physical interface, they are often called “subinterfaces”.

On 3Com Series Routers, the subinterface-supported physical interfaces include:

- Ethernet interface. Without VLAN ID, an Ethernet subinterface can only support IPX. Assigned with a VLAN ID, the subinterface can support both IPX and IP.
- WAN interface encapsulated with FR. The subinterfaces of such a WAN interface can support both IP and IPX.
- WAN interface encapsulated with X.25. The subinterfaces of such a WAN interface can support both IP and IPX.
- IP-supported ATM subinterface

4.4.2 Configuring an Ethernet Subinterface

Perform the following tasks to configure an Ethernet subinterface:

- Create an Ethernet subinterface
- Configure encapsulation and VLAN ID on the subinterface
- Configure the maximum number of packets processed per second for a VLAN (optional)

I. Creating an Ethernet subinterface

Perform the following configuration in system view.

Table 4-3 Create/delete an Ethernet subinterface

Operation	Command
Create an Ethernet subinterface and enter the Ethernet subinterface view	**interface ethernet** *number.sub-number*
Delete the specified Ethernet subinterface	**undo interface ethernet** *number.sub-number*

If the Ethernet subinterface (the same as *sub-number*) that you intend to create has existed, the system will directly enter the view of the subinterface. Otherwise, the system will create the Ethernet subinterface assigned with *sub-number* before entering its view.

II. Configuring the VLAN-related parameters

Perform the following configuration in system view or Ethernet subinterface view.

Table 4-4 Configure the VLAN-related parameters

Operation	Command
Set the encapsulation type of an Ethernet subinterface or a gigabit Ethernet subinterface and the associated VLAN ID (in interface view)	**vlan-type dot1q vid** *vid*
Set the maximum number of packets processed by a VLAN per second (in system view)	**max-packet-process** *count vid*
Restore the default maximum number of packets processed for a VLAN per second (in system view)	**undo max-packet-process** *vid*

By default, the Ethernet subinterface is not configured with any encapsulation or associated with any VLAN ID. In addition, the maximum number of processed packets is not limited.

After you configure encapsulation on the Ethernet subinterface, it allows VLAN trunk.

📖 **Note:**

Given the AR 18-22-24, do not set the VLAN ID of a subinterface to VLAN1. Otherwise, it is regarded an invalid interface.

III. Configuring other operating parameters

As an Ethernet subinterface that has not been assigned with VLAN ID can only support IPX, you can only assign an IPX address to such an Ethernet subinterface and configure the IPX operating parameters. But the configuration procedure is similar to that for configuring an Ethernet interface. An Ethernet subinterface that has been assigned with VLAN ID can support both IP and IPX. For the related configurations, refer to *V 2.41 Operation Manual – Network Protocol*.

IV. Displaying/debugging Ethernet subinterfaces

After completing the above configurations, execute the **display** commands in any view to verify how the Ethernet subinterface is operating after it is associated with a VLAN ID.

Execute the **reset** command in user view to clear information about the subinterface.

Table 4-5 Display and debug Ethernet

Operation	Command
Display information about the specified VLAN	**display vlan vid**
Display the maximum number of processed packets configured on a specified VLAN	**display vlan max-packet-process** *vid*
Display the packet statistics of the specified VLAN, including the received and sent packet numbers	**display vlan statistics vid** *vid*
Display the VLAN configuration information on an interface	**display vlan interface** *interface-type interface-num*
Clear the packet statistics of specified VLAN	**reset vlan statistics vid** *vid*

4.4.3 Configuring a WAN Subinterface

I. Configuring subinterfaces on a WAN interface running frame relay

1) Create/delete a subinterface from a serial interface

Perform the following configuration in system view.

Table 4-6 Create/delete a subinterface from a serial interface

Operation	Command
Create a subinterface on the serial interface and enter its view	**interface serial** *number.sub-number* [**p2mp** | **p2p**]

Operation	Command
Delete the specified subinterface from the serial interface.	**undo interface serial** *number.sub-number*

If the serial subinterface (the same as *sub-number*) that you intend to create has existed, the system will directly enter its view. Otherwise, the system will create the serial subinterface assigned with *sub-number* before entering its view.

2) Configure the relevant operating parameters

You can make the following configurations for a subinterface on a WAN interface encapsulated with FR.

FR address map different from that of the WAN interface (also called the main interface) to which the subinterface belongs

- IP address beyond the segment on which the main interface is located
- IPX network number and other IPX parameters different from the main interface
- VCs belonging to the subinterface

For more information about the configurations, refer to *V 2.41 Operation Manual - Link Layer Protocol* and *V 2.41 Operation Manual – Network Protocol*.

II. Configuring a subinterface on a WAN interface encapsulated with X.25

1) Create/delete a WAN subinterface

You can use the same commands described in Table 4-6 to create/delete a WAN subinterface.

2) Configure the relevant operating parameters

You can make the following configurations for a subinterface on a WAN interface encapsulated with X.25.

- X.25 address map different from that of the WAN interface (also called the main interface) to which the subinterface belongs
- IP address beyond the segment on which the main interface is located
- IPX network number and other IPX parameters different from the main interface
- VC belonging to the subinterface

For more information about the configurations, refer to *V 2.41 Operation Manual - Link Layer Protocol* and *V 2.41 Operation Manual – Network Protocol*.

III. Configuring an ATM subinterface

1) Create/delete an ATM subinterface

Perform the following configuration in system view.

Table 4-7 Create/delete an ATM subinterface

Operation	Command
Create an ATM subinterface and enter its view	**interface atm** *number.sub-number* [**p2mp** | **p2p**]
Delete the specified ATM subinterface	**undo interface atm** *number.sub-number*

2) Configure other operating parameters

On an ATM subinterface, you can configure:

- An IP address located on a segment different than the WAN interface to which the subinterface belongs
- PVCs

For configuration details, refer to the "Link Layer Protocol" and "Network Protocol" parts of this manual.

4.4.4 Ethernet Subinterface Configuration Example

I. Network requirements

As shown in the following figure, the encapsulation type is set to **dot1q** on the ports on Switch 1 and Switch 2; the attached workstations A and C belong to VLAN 10 and the attached workstations B and D belong to VLAN 20. The following are required:

- The addresses of Ethernet subinterfaces 3/0/0.1, Ethernet3/0/0.2, Ethernet4/0/0.1, and Ethernet4/0/0.2 are 1.0.0.1, 2.0.0.1, 3.0.0.1, and 4.0.0.1.
- Communication is feasible between workstation A and B as well as between C and D, i.e. through the same Switch, workstations in different VLANs can communicate with each other.
- Communication is feasible between workstation A and C, as well as between B and D, i.e. through different Switches, workstations in the same VLAN can communicate with each other.
- Communications can be carried out between workstations A and D, and between B and C, i.e. different switches and different VLANs can communicate with each other.

II. Network diagram

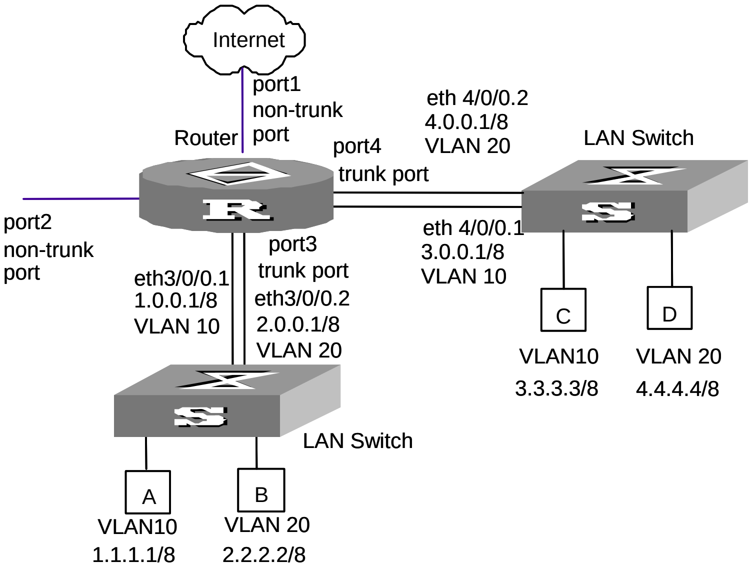


Figure 4-1 Network diagram for Ethernet subinterface configuration

III. Configuration procedure

Configure the router:

# Create Ethernet subinterfaces (Ethernet 3/0/0.1, Ethernet 3/0/0.2, Ethernet 4/0/0.1, and Ethernet 4/0/0.2 as shown in the figure) and enter their views to configure their IP addresses. Set the encapsulation type of each subinterface (The encapsulation type of the Ethernet subinterface must keep consistent with that configured on the switch port) and the associated VLAN ID.

```
<3Com> system-view
[3Com] interface ethernet 3/0/0.1
[3Com-Ethernet3/0/0.1] ip address 1.0.0.1 255.0.0.0
[3Com-Ethernet3/0/0.1] vlan-type dot1q vid 10
[3Com-Ethernet3/0/0.1] interface ethernet 3/0/0.2
[3Com-Ethernet3/0/0.2] ip address 2.0.0.1 255.0.0.0
[3Com-Ethernet3/0/0.2] vlan-type dot1q vid 20
[3Com-Ethernet3/0/0.2] interface ethernet 4/0/0.1
[3Com-Ethernet4/0/0.1] ip address 3.0.0.1 255.0.0.0
[3Com-Ethernet4/0/0.1] vlan-type dot1q vid 10
[3Com-Ethernet4/0/0.1] interface ethernet 4/0/0.2
[3Com-Ethernet4/0/0.2] ip address 4.0.0.1 255.0.0.0
[3Com-Ethernet4/0/0.2] vlan-type dot1q vid 20
[3Com-Ethernet4/0/0.2] quit
```

# Set the maximum number of packet that VLAN10 can process per second to 100000 and VLAN20 can process per second to 200000.

```
[3Com] max-packet-process 100000 10
[3Com] max-packet-process 200000 20
```

4.4.5 WAN Subinterface Configuration Example

I. Network requirements

As shown in the following figure, the WAN interface Serial0/0/0 on Router A is connected to Router B and Router C via a public FR network. By configuring subinterfaces on Serial0/0/0 on Router A, you can make LAN 1 to access LAN 2 and LAN 3 simultaneously through Serial0/0/0.

II. Network diagram

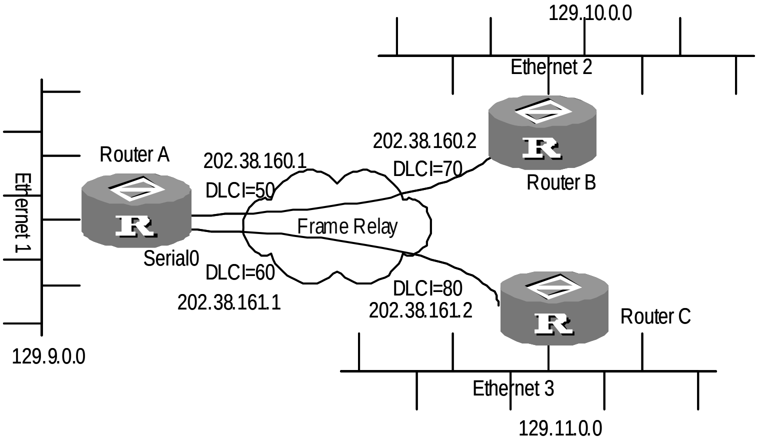


Figure 4-2 Network diagram for the WAN subinterface configuration

III. Configuration procedure

# Enter the view of Serial0/0/0 on Router A.

```
[3Com] interface serial 0/0/0
```

# Encapsulate the interface with FR.

```
[3Com-Serial0/0/0] link-protocol fr
```

# Specify the interface to work as DTE in FR.

```
[3Com-Serial0/0/0] fr interface-type dte
```

# Create the subinterface Serial 0/0/0.1 on Serial0/0/0 on Router A, specify it work in point-to-point mode, and enter the view of the subinterface.

```
[3Com] interface serial 0/0/0.1 p2p
```

# Assign the IP address 202.38.160.1 to the subinterface, given the mask is 255.255.255.0.

```
[3Com-Serial0/0/0.1] ip address 202.38.160.1 255.255.255.0
```

# Assign the VC assigned with DLCI 50 to the subinterface.

```
[3Com-Serial0/0/0.1] fr dlci 50
```

# Create the subinterface Serial 0/0/0.2 on Serial0/0/0 on Router A, specify it to work in point-to-point mode, and enter its view.

```
[3Com-Serial0/0/0.1] interface serial 0/0/0.2 p2p
```

# Assign the IP address 202.38.161.1 to the subinterface, given the mask is 255.255.255.0.

```
[3Com-Serial0/0/0.2] ip address 202.38.161.1 255.255.255.0
```

# Assign the VC assigned with DLCI 60 to the subinterface.

```
[3Com-Serial0/0/0.2] fr dlci 60
[3Com-Serial0/0/0.2] quit
```

# Configure the static routes from Router A to LAN2 and LAN3.

```
[3Com] ip route-static 129.10.0.0 255.255.0.0 202.38.160.2
[3Com] ip route-static 129.11.0.0 255.255.0.0 202.38.161.2
```

The configurations of Router B and Router C are omitted.

4.5 MP-Group and MFR

Refer to the “Link Layer Protocol” part of this manual.

4.6 Logical Channel of Backup Center

4.6.1 Introduction to Logical Channel of Backup Center

In addition to providing the backup between interfaces, the backup center allows an X.25 or FR VC to work as the master interface or standby interface of the backup center. For more information about the backup center, refer to *V 2.41 Operation Manual - Reliability*.

To make the configuration easier, you can specify a logical channel for the VC discussed above, and then configure the operating parameters of the backup center on the logical channel.

4.6.2 Configuring a Backup Center Logical Channel

Refer to the “Reliability” part of this manual.

4.7 Virtual-Template and Virtual Interface

4.7.1 Introduction to Virtual-Template and Virtual Interface

Virtual-Template is a template for configuring a virtual interface. It is primarily applied in the application environments like VPN and MP.

After setting up a VPN session, the system needs to create a virtual interface for exchanging data with the remote end. For this purpose, the system will choose a virtual-template according to the user's configuration, and dynamically create a virtual interface based on the configuration parameters of the template. For VPN configuration details, refer to the related sections of VPN Configuration in this manual..

Likewise, after bundling multiple PPP links into an MP, the system also needs to create a virtual interface for exchanging data with the remote end. In this case, you can select a virtual-template for the purpose of dynamic creation of virtual interface.

4.7.2 Configuring a Virtual-Template

In VPN and MP application environments, the system automatically creates and deletes virtual interfaces, which is completely transparent to the user. The user only needs to configure VPN or MP on the involved physical interface, creates and configures a virtual-template, and finally associates the virtual-template with the physical interface.

Perform the following tasks to configure a virtual-template:

- Create/Delete a virtual-template
- Set operating parameters of virtual-template
- Associate the virtual-template with the involved physical interface

I. Creating/Deleting a virtual-template

Perform the following configuration in system view.

Table 4-8 Create/delete a virtual-template

Operation	Command
Create a virtual-template and enter the virtual-template view	**interface virtual-template** *number*
Delete the virtual-template	**undo interface virtual-template** *number*

If the virtual-template that you intend to create by using the **interface virtual-template** command has existed, the system will directly enter the view of the virtual-template. Otherwise, the system will create the virtual-template assigned with specified *number* before entering its view.

In deleting a virtual-template, make sure that all of its derived virtual interfaces have been removed and this virtual-template is not in use any more.

II. Setting operating parameters of virtual-template

Compared with a regular physical interface, virtual-templates only support PPP in terms of link layer protocol and IP and IPX in terms of network protocol. accordingly, you can perform the following tasks to set the following operating parameters:

- Set PPP operating parameters
- Assign an IP address to the virtual interface
- Set the IP address (or IP address pool) assigned to the PPP peer

Setting these parameters on a virtual-template is the same as setting them on a regular interface.

III. Associating the virtual-template with the involved physical interface

You are required to associate an L2TP group with the virtual-template in a VPN environment and MP user with the virtual-template in an MP environment.

For details, refer to *V 2.41 Operation Manual - VPN*.

4.7.3 Displaying and Debugging Virtual-Template and Virtual Interface

When needed, the system can automatically create a virtual interface and operate it with the parameters of the associated virtual-template. Therefore, manual creation and configuration are not needed. A virtual interface can be deleted due to the disconnection of the bottom layer link or the interruption of the user.

Execute the following command in any view to display the state of a specified virtual-template.

Table 4-9 Display the state about the specified virtual-template

Operation	Command
Display the state about the specified virtual-template	**display interfaces virtual-template** *number*
Display the state about the specified or all virtual access interfaces.	**display virtual-access** { **dialer** [*number*] | **vt** [*vt-number*] | **user** *user-name* | **peer** *peer-address* | *va-number* }*

4.7.4 Troubleshooting

Before isolating the faults of a virtual-template, you must make sure the application environment, specifically, whether the virtual-template is used for creating a VPN virtual interface or for creating an MP virtual interface.

Fault 1: The system failed to create a virtual interface.

Problem solving: Such a problem may arise because:

- The virtual-template had not been assigned with an IP address. Therefore, the virtual interface failed to pass the PPP negotiation and hence could not go up.
- The virtual-template had not been configured with the IP address (or IP address pool) intended for the peer. Therefore, if it is necessary to allocate address for the peer, the associated virtual interface could not satisfy the requirements of the peer and hence could not go up.
- PPP authentication parameters were incorrectly set. When the peer was not a user defined on the router, PPP negotiation would also fail.

4.8 Virtual Ethernet Interface

4.8.1 Introduction to Virtual Ethernet Interface

Virtual Ethernet interface (VE) is a logical interface that is implemented on the interface card. It is primarily application to Point to point Protocol over Ethernet over ATM (PPPoEoA).

PPPoEoA adopts a three-layer architecture, with the top layer encapsulated with PPP, the mid-layer with PPPoE (PPP over Ethernet), and the bottom layer with PPPoE over ATM.

Typically, PPPoE is applied to the community broadband access and to the application in which multiple hosts share a front-end bridging access device. The PPP parameters carried over the Ethernet are implemented on the interface card of the access device via Virtual Ethernet interface. For accessing a remote access server (for the purpose of accessing an external network) via this device, the ATM PVC must be adopted due to the long distance involved. In this case, the ATM port on the server is required to carry the Ethernet packets, which is called PPPoEoA.

For details, refer to *Operation Manual - Link Layer Protocol*.

4.8.2 Virtual Ethernet Interface Configuration

Perform the following tasks to configure a Virtual Ethernet interface:

- Create/Delete a Virtual Ethernet interface
- Configure Virtual Ethernet interface parameters

I. Creating/Deleting a Virtual Ethernet Interface

Perform the following configuration in system view.

Table 4-10 Create/delete a Virtual Ethernet interface

Operation	Command
Create a Virtual Ethernet interface	**interface virtual-ethernet** *number*
Delete the Virtual Ethernet interface	**undo interface virtual-ethernet** *number*

The user may establish as many as 1024 Virtual Ethernet interfaces.

When configuring a PVC to carry PPPoEoA, you must associate a VE interface with the PVC. If the specified VE interface has not been created yet, the configuration will fail and the system will return. A VE interface can only be associated with a PVC carrying PPPoEoA. The efforts of deleting a VE interface will fail if the VE interface has been associated with a PVC carrying PPPoEoA.

II. Configuring Virtual Ethernet Interface parameters

You can set the VE interface parameters in the same way of setting Ethernet interface parameters. For details, refer to Ethernet Interface in this manual.

As the debug and display operations of VE interface and Ethernet interface are the same, this section will not cover the details for the sake of simplicity.

For the typical PPPoEoA configuration example, refer to *Operation Manual – Link Layer Protocol*.

Link Layer Protocol

Table of Contents

Chapter 1 PPP and MP Configuration

1.1 Introduction to PPP and MP

1.1.1 PPP

Point-to-point protocol (PPP) is a link layer protocol that carries network layer packets over point-to-point links. It has found wide application because it can provide user authentication, support synchronous/asynchronous communication, and can be extended easily.

PPP defines a whole set of protocols, covering link control protocol (LCP), network control protocol (NCP), and authentication protocols including password authentication protocol (PAP) and challenge handshake authentication protocol (CHAP). Where,

- LCP is responsible for establishing, removing and monitoring data links.
- NCP is used to negotiate the format and type of the packets over data links.
- Authentication protocol suite used for network security

I. PPP authentication

1) PAP authentication

PAP is a two-way handshake authentication protocol operating as follows:

- The requester sends its username and password to the authenticating party.
- The authenticator will check if the username and password are correct according to local user list and then return different responses (Acknowledge or Not Acknowledge).

2) CHAP authentication

Challenge-handshake authentication protocol (CHAP) is a three-way handshake authentication protocol operating as follows:

- The authenticator actively initiates an authentication request by sending a randomly generated packet (Challenge) carrying its own username to the authenticatee.
- When the authenticatee receives the authentication request, it looks for the password according to the username in the packet. If the **ppp chap password** command is configured on the receiving interface, the authenticatee uses the password set by the command. If not, it looks up its local user database for a match. After finding a match, the authenticatee encrypts this packet with packet ID, password and the MD5 algorithm; and then sends back a Response carrying the generated ciphertext and its own username.

- After receiving the Response, the authenticator looks up its local user database for a match according to the username of the authenticatee in the Response. When a match is found, it encrypts the original randomly generated packet with the authenticatee password and the MD5 algorithm, compares the encryption result with the received ciphertext, and returns an Acknowledge or Not Acknowledge packet depending on the comparison result.

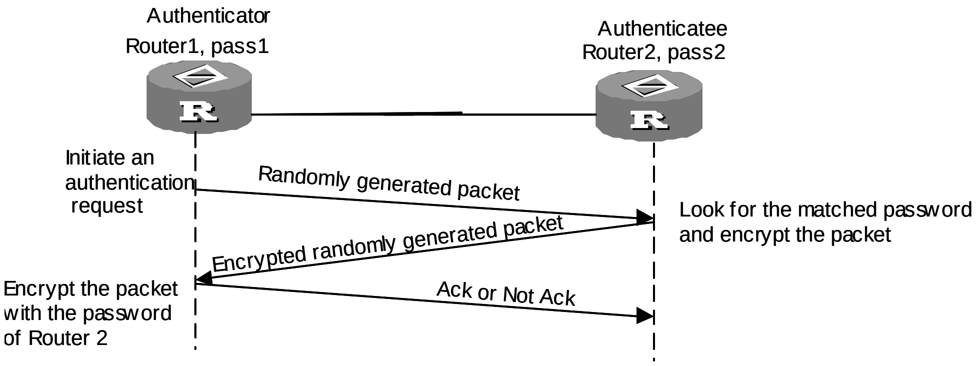

Authenticator
Router1, pass1
Authenticatee
Router2, pass2
Initiate an authentication request
Randomly generated packet
Look for the matched password and encrypt the packet
Encrypted randomly generated packet
Encrypt the packet with the password of Router 2
Ack or Not Ack

Figure 1-1 CHAP Authentication

II. Operating mechanism of PPP

Following is how PPP operates:

1) Before setting up a PPP link, enter the Establish phase.
2) Carry out LCP negotiation in the Establish phase, which includes the negotiation in operating mode (SP or MP), authentication mode and maximum receive unit (MRU). If the negotiation is successful, LCP will enter the Opened status, indicating the setup of the bottom layer link.
3) If the authentication (the remote verifies the local or the local verifies the remote) is configured, it enters the Authenticate phase and starts the CHAP/PAP authentication
4) If the authentication fails, it will enter the Terminate phase to remove the link and the LCP will go down. If the authentication succeeds, it will proceed to start the network negotiation (NCP). In this case, the LCP state is still Opened, while the state of IP control protocol (IPCP) is changed from Initial to Request.
5) NCP negotiation supports the negotiation of IPCP, which primarily refers to the negotiation of the IP addresses of the two parties. NCP negotiation is conducted for the purpose of selecting and configuring a network layer protocol. Only the network layer protocol that has been agreed upon by the two parties in the NCP negotiation can send packets over the PPP link.
6) The PPP link will remain for communications until an explicit LCP or NCP frame close it or some external events take place (for example, the intervention of the user).

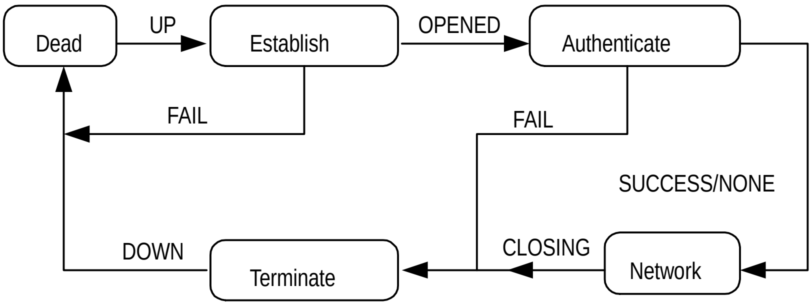


Figure 1-2 PPP operation flow chart

For the details of PPP, refer to RFC1661.

1.1.2 Introduction to MP

Multilink PPP (MP) provides an approach to increasing bandwidth. It allows multiple PPP links to form an MP bundle. After receiving a packet, MP segments (in case the packet is large) and distributes it over multiple PPP links in a bundle on a segment by segment basis. The receiving MP then assembles these segments and passes the resulted packet to the network layer.

MP functions to:

- Increase bandwidth, or dynamically increase/reduce bandwidth in combination with DCC
- Load sharing
- Backup
- Decrease transmission delay due to the use of fragmentation

MP can work on any physical or virtual interfaces with PPP encapsulation, such as serial, ISDN BRI/PRI, and PPPoX (PPPoE, PPPoA, or PPPoFR). However, a multilink bundle is preferred to include only one type of interface.

1.2 Configuring PPP

Fundamental PPP configuration tasks include:

- Configure the data link protocol encapsulated on the interface to be PPP
- Configure the polling interval
- Configure PPP authentication mode, user name and user password

Advanced PPP configuration tasks include:

- Configure PPP negotiation parameters
- Configure PPP link quality control (LQC)

The fundamental configuration is the parameter setting that must be performed for running PPP on the router, whereas the advanced configurations are the options that can be configured as needed.

1.2.1 Configuring PPP Encapsulation on the Interface

Perform the following configuration in interface view.

Table 1-1 Configure PPP encapsulation on the interface

Operation	Command
Configure PPP encapsulation on the interface.	**link-protocol ppp**

The link layer protocol encapsulated on the interface defaults to PPP.

1.2.2 Configuring the Polling Interval

Data link protocols such as PPP, MP and HDLC use a timer to monitor the status of the link periodically. You are recommended to set the same polling interval at the two ends of the link.

Perform the following configuration in interface view.

Table 1-2 Configure polling interval on the interface

Operation	Command
Set the polling interval.	**timer hold** *seconds*
Reset polling interval	**undo timer hold**

The polling interval defaults to 10 seconds. The cyclic polling operation will be closed if the polling interval is set to 0.

Elongate this time to prevent net fluctuation for long-delay and high-congestion network.

1.2.3 Configuring PPP Authentication Mode and Username and User Password

The local and the peer support both CHAP and PAP authentication approaches between them. The configuration procedures in both approaches will be described in the following subsections. This chapter only discusses local authentication. For information about the remote AAA authentication, refer to the part relating to security in this manual.

I. Configuring the local router to authenticate the peer using PAP

Table 1-3 Configure the local router to authenticate the peer with the PAP approach

Operation	Command
Configure the local to authenticate the peer in PAP mode (in interface view).	**ppp authentication-mode pap** [**domain** *isp-name*]
Disable the configured PPP authentication mode, i.e. performing no PPP authentication (in interface view).	**undo ppp authentication-mode**
Create a local user and enter the corresponding view (in system view)	**local-user** *username*
Configure the password for the local user (in local user view)	**password** { **simple** | **cipher** } *password*
Cancel the password of the local user (in local user view)	**undo password**
Set the callback and caller number attributes of the PPP user (in local user view)	**service-type ppp** [**callback-nocheck** | **callback-number** *callback-number* | **call-number** *call-number* [**:***subcall-number*]]
Restore the default callback and caller number attributes of the PPP user (in local user view)	**undo service-type ppp** [**callback-nocheck** | **callback-number** | **call-number**]
Create an ISP domain or enter the view of a created domain (in system view)	**domain** { *isp-name* | **default** { **disable** | **enable** *isp-name* } }
Configure the user in the domain to use the local authentication scheme (in domain view)	**scheme local**

By default, PPP authentication is disabled.

If you configure the **ppp authentication-mode** { **pap** | **chap** } command without specifying a domain, the system-default domain named system applies by default, using local authentication and the address pool you configured for this domain for address allocation. If a domain is specified, you must configure an address pool in the specified domain.

If a received username includes a domain name, this domain name is used for authentication (if the name does not exist, authentication is denied). Otherwise, the domain name configured for PPP authentication applies.

If the username does not include a domain name, and the domain name configured for PPP authentication does not exist, authentication is denied.

For authentication on a dial interface, you are recommended to configure authentication on both the physical interface and the dialer interface. When the physical interface receives a DCC call request, it first initiates PPP negotiation and authenticates the dial-in user, and then passes the call to the upper layer protocol.

II. Configuring the local router to authenticate the peer using CHAP

Table 1-4 Configure the local router to authenticate the peer with the CHAP approach

Operation	Command
Configure the local to authenticate the peer in CHAP mode (in interface view)	**ppp authentication-mode chap** [**domain** *isp-name*]
Disable the configured PPP authentication, i.e. performing no PPP authentication (in interface view)	**undo ppp authentication-mode**
Configure the local username (in interface view)	**ppp chap user** *username*
Delete the configured local username (in interface view)	**undo ppp chap user**
Create a local user and enter the corresponding view (in system view)	**local-user** *username*
Configure the password for the local user (in local user view)	**password** { **simple | cipher** } *password*
Cancel the password of the local user (in local user view)	**undo password**
Set the callback and caller number attributes of the PPP user (in local user view)	**service-type ppp** [**callback-nocheck | callback-number** *callback-number* | **call-number** *call-number* [*:subcall-number*]]
Restore the default callback and caller number attributes of the PPP user (in local user view)	**undo service-type ppp** [**callback-nocheck | callback-number | call-number**]
Create an ISP domain or enter the view of a created domain (in system view)	**domain** { *isp-name* **| default** { **disable | enable** *isp-name* } }
Configure the user in the domain to use the local authentication scheme (in domain view)	**scheme local**

By default, PPP authentication is disabled.

For authentication on a dial interface, you are recommended to configure authentication on both the physical interface and the dialer interface. When the physical interface receives a DCC call request, it first initiates PPP negotiation and authenticates the dial-in user, and then passes the call to the upper layer protocol.

III. Configuring the local to be authenticated by the peer using PAP

Table 1-5 Configure the local to be authenticated by the peer with the PAP approach

Operation	Command
Configure PAP username and password that the local will send when authenticated by the peer in PAP mode	**ppp pap local-user** *username* **password** { **simple** | **cipher** } *password*
Delete the PAP username and password that the local will send when authenticated by the peer in PAP mode	**undo ppp pap local-user**

By default, when the local router is authenticated by the peer in PAP mode, both username and password sent by the local router are null.

IV. Configuring the local to be authenticated by the peer using CHAP

Table 1-6 Configure the local to be authenticated by the peer with the CHAP approach

Operation	Command
In system view create a local user and enter its view	**local-user** *username*
In local user view set a password for the local user	**password** { **simple** | **cipher** } *password*
In local user view remove the password of the local user	**undo password**
Configure the name of the local end	**ppp chap user** *username*
Delete the configured name of the local	**undo ppp chap user**
Configure a CHAP authentication password.	**ppp chap password** { **simple** | **cipher** } *password*
Delete the CHAP authentication password	**undo ppp chap password**

In the above table, **simple** means to send password in plain text and **cipher** in ciphertext.

By default, when the local router is authenticated by the peer in CHAP mode, both username and password sent by the local router are null.

When configuring PPP CHAP, note the following:

- At the authenticator end, create a local user entry for the authenticatee. Only the password configured in local user view can be used for encryption.

- At the authenticatee end, the password for CHAP authentication could be one set by the **ppp chap password** command or one set in local user view, with the former taking priority over the latter for encryption.
- With bidirectional authentication enabled, the authenticatee can use either the password set by the **ppp chap password** command or the password set in local user view if the same password is used for authentication; but if different passwords are used, it can only use the one set by the **ppp chap password** command.

1.2.4 Configuring PPP Negotiation Timeout Interval

During PPP negotiation, if the response message of the peer is not received within this time interval, PPP will retransmit the message. The timeout interval ranges from 1 to 10 seconds.

Perform the following configuration in interface view.

Table 1-7 Configure the time interval of PPP negotiation timeout

Operation	Command
Configure the time interval of negotiation timeout	**ppp timer negotiate** *seconds*
Restore the default value of time interval of negotiation timeout	**undo ppp timer negotiate**

The timeout interval defaults to 3 seconds.

1.2.5 Negotiating IP address using PPP

I. Configuring client

Suppose PPP has been encapsulated on local and remote interfaces. If the local interface has no IP address while the remote interface has one, you may configure the local interface to allow it to negotiate an IP address using PPP and accept the IP address thus assigned by the remote interface. When accessing the Internet via an ISP, you may make this configuration to get an IP address from the ISP.

Perform the following configuration in interface view.

Table 1-8 Configure an interface to negotiate IP address using PPP

Operation	Command
Configure an interface to negotiate IP address using PPP.	**ip address ppp-negotiate**
Disable PPP negotiation.	**undo ip address ppp-negotiate**

By default, the IP address of interface is not negotiable.

⚠ **Caution:**

- You may configure an interface to obtain an IP address through negotiation only when the interface is encapsulated with PPP. When PPP goes down, the IP address obtained through PPP negotiation is deleted.
- After you configure IP address negotiation on an interface that has been assigned an IP address or configured with IP address negotiation, the original IP address is deleted, whether it is manually assigned or obtained through PPP negotiation.
- After you configure IP address negotiation on an interface, the interface can obtain IP address automatically and you need not to assign it an IP address.
- Once the IP address that an interface obtained through PPP negotiation is removed, the interface will have no IP address.

II. Configuring server

When the router is functioning as the server to assign an IP address to a PPP user, three IP address assignment methods are available.

1) Method 1: Assign an IP address to the PPP user directly on the interface. This method does not require the configuration of address pool.

Table 1-9 Assign an IP address to a PPP user on the interface

Operation	Command
Assign an IP address to the PPP user	**remote address** *ip-address*
Disable the interface to assign IP addresses to PPP users	**undo remote address**

By default, the interface does not assign IP address to its peer.

2) Method 2: Assign an IP address picked from a global address pool

In this approach, you need to do the following:

- Create a global address pool in system view.
- Assign the address pool (only one is allowed) to the interface by executing the **remote address pool** command in interface view.

Table 1-10 Assign IP addresses picked from a global address pool

Operation	Command
Configure a global IP address pool	**ip pool** *pool-number* *low-ip-address* [*high-ip-address*]
Remove the global IP address pool	**undo ip pool** *pool-number*
Assign the global address pool to an interface for address assignment to PPP users	**remote address pool** [*pool-number*]
Disable the interface to assign IP addresses to PPP users	**undo remote address**

By default, the interface does not assign IP address to the remote end. If the *pool-numbe*r argument is not specified in the **remote address pool** command, the default global address pool, pool 0, is used.

Note:

The above two methods are used where PPP authentication is not required, and the third method to be described is used where PPP authentication is required.

3) Method 3: Assign an IP address picked from a domain address pool

In this approach, you need to do the following:

- Create a domain address pool in domain view.
- Assign the domain address pool to the interface by executing the **remote address pool** command in interface view. If this command is not configured, the system looks up the address pools of the domain in turn to pick an address for the peer during the authentication negotiation with the peer.

Table 1-11 Use domain address pools for address assignment

Operation	Command
Configure a domain IP address pool	**ip pool** *pool-number* *low-ip-address* [*high-ip-address*]
Remove the domain IP address pool	**undo ip pool** *pool-number*
Assign the domain address pool to an interface for address assignment to PPP users	**remote address pool** [*pool-number*]
Disable the interface to assign IP addresses to PPP users	**undo remote address**

By default, the interface does not assign IP address to the remote end.

🕮 **Note:**

When both the **remote address pool** [*pool-number*] command and the **remote address** *ip-address* command are configured, the system uses the address specified by the latter for assignment.

To sum up, the system assigns an IP address to a PPP user following these rules:

1) For a domain user (*userid* or *userid@isp-name*)

Address assignment depends on its authentication type, as shown in the following table.

Table 1-12 Assign an address to a domain user

Authentication/ Authorization type	Address assignment
RADIUS/TACACS	1) If the RADIUS or TACACS server issues an address, the router assigns this address to the domain user. 2) If the RADIUS or TACACS server issues a domain address pool instead of an address, the router picks an address from the pool. 3) If neither address nor domain address pool is issued, the router looks up the address pools of the domain in turn for an address.
Local	The router looks up the address pools of the domain in turn and picks an address.

2) For a non-authenticated user

The router assigns the address specified directly on the interface or an address picked from the global address pool assigned to the interface.

The PPP user, however, does not necessarily accept the assigned address. Instead, it may choose to use a self-configured IP address.

To force the PPP user to accept the assigned address, perform the following command in interface view at the server end.

Table 1-13 Enable/disable forced IP address assignment with PPP IPCP negotiation

Operation	Command
Forbid the peer to use a self-configured fix IP address in PPP IPCP negotiation.	**ppp ipcp remote-address forced**
Disable forced address assignment in PPP IPCP negotiation.	**undo ppp ipcp remote-address forced**

By default, the PPP user can use its self-configured IP address in PPP IPCP negotiation. If the PPP user explicitly requests an address, this end acts as requested; if the peer already has a self-configured IP address, this end does not assign one to the peer.

1.2.6 Negotiating an DNS Address through PPP

While negotiating PPP address, the router can negotiate DNS server address as a DNS server address provider or recipient, depending on the connected device.

When a PC connects to the router using PPP, through dialup for example, the router, as the server, should allocate a DNS server address to the PC so that the PC can use its domain name to access the Internet.

When connected using PPP to the network access server (NAS) of the service provider, the router, as the client, should be able to request the NAS for a DNS server address or accept the assigned DNS server address.

1) Configure the client end in DNS server address negotiation

Perform the following configuration in interface view.

Table 1-14 Configure the client end in DNS server address negotiation

Operation	Command
Enable the router to accept the unsolicited DNS server address	**ppp ipcp dns admit-any**
Disable the router to accept the unsolicited DNS server address	**undo ppp ipcp dns admit-any**
Enable the router to request for a DNS server address	**ppp ipcp dns request**
Disable the router to request for a DNS server address	**undo ppp ipcp dns request**

By default, DNS address negotiation is disabled.

2) Configure the server end in DNS server address negotiation

Perform the following configuration in interface view.

Table 1-15 Configure the server end in DNS server address negotiation

Operation	Command
Enable the router to allocate a DNS server address to the peer	**ppp ipcp dns** *primary-dns-address* [*secondary-dns-address*]
Disable the router to allocate a DNS server address to the peer	**undo ppp ipcp dns** [*primary-dns-address* [*secondary-dns-address*]]

By default, DNS address negotiation is disabled.

The command is intended for the use with PPP, PPPoE, and MP and the interface view in which the command is configured varies with the adopted protocol.

- At the client end, the command is configured in serial interface view for PPP, in virtual template interface view for MP, and in dialer interface view for PPPoE.
- At the server end, the command is configured in serial interface view for PPP, in virtual template interface view for both MP and PPPoE.

1.2.7 Configuring PPP Link Quality Control

You may use PPP link quality control (LQC) to monitor quality of PPP links including those in MP bundles. The system shuts down a link when its quality decreased below the forbidden-percentage and brings it up when its quality ameliorates exceeding the resumptive-percentage. When re-enabling the link, PPP LQC experiences a delay to avoid link flapping.

Perform the following configuration in interface view.

Table 1-16 Configure PPP link quality control

Operation	Command
Enable PPP LQC	**ppp lqc** *forbidden-percentage* [*resumptive-percentage*]
Disable PPP LQC	**undo ppp lqc**

By default, the arguments *resumptive-percentage* and *forbidden-percentage* are equal.

Note that before you enable LQC on the PPP interface, it sends keepalives to the peer regularly. After you enable LQC on the interface, it sends link quality reports (LQRs) instead for monitoring the link.

When the quality of the link is normal, the system calculates link quality based on each LQR and shuts down the link if the results of two consecutive calculations are below the forbidden-percentage. After shutting down the link, the system calculates link quality every ten L QRs, and brings the link up again if the results of three consecutive calculations are higher than the resumptive-percentage. That means a disabled link must experience 30 keepalive periods before it can go up again. If a large keepalive period is specified, it may take long time for the link to go up.

1.2.8 Configuring PPP LCP to Negotiate MRU

Perform the following configuration in interface view.

Table 1-17 Enable PPP LCP to negotiate MRU

Operation	Command
Configure PPP LCP to negotiate MRU	**ppp lcp mru consistent**
Restore the default	**undo ppp lcp mru consistent**

By default, PPP LCP does not negotiate MRU; the local end modifies MTU depending on the remote MRU.

After PPP LCP is enabled to negotiate MRU, the MRU value carried in the LCP CONREQ message received from the remote end cannot be less than the MTU value configured on the local interface. If a smaller MRU value is received, the local end sends a CONNAK message to the remote end. If the received MRU value is still smaller after the local end makes a specified number of CONNAK message sending attempts, the local end sends a CONREJ message to disable MRU negotiation. The MRU negotiation attempts made by the remote end after that will always fail.

Normally, after PPP LCP negotiation succeeds, the MTU at the local end does not change as the remote MRU changes.

1.3 Configuring MP

You can configure MP by configuring virtual templates or MP-group interfaces. They are different in that:

- Virtual templates can be used in combination with authentication. According to the remote use name, the router determines the associated virtual template interface and based on the configurations of the template creates a bundle equivalent to an MP link.
- From one virtual template interface can derive multiple bundles called VT channels, each being an MP link. From the perspective of the network layer, these links form a point to multipoint network topology. In this sense, virtual template interfaces are flexible than MP-group interfaces.
- To distinguish among multiple bundles derived from a virtual template interface, the **ppp mp binding-mode** command is provided in virtual template interface view to specify bundling mode. Three bundling modes are available: **authentication**, **both** (the default), and **descriptor**. The **a**uthentication mode is to bundle links according to remote user name, the descriptor mode is to bundle links according to the remote endpoint descriptor obtained from LCP negotiation, and the both mode is to bundle links according to both user name and descriptor.
- MP-group interfaces are intended only for MP. On an MP-group interface, only one bundle is allowed. Compared with virtual template interfaces, the configuration of MP-group interfaces is simpler and easier.

I. Configuring MP on a virtual template interface

Fundamental MP configuration tasks include:

- Create a virtual template interface
- Associate a remote username with the virtual template interface
- Enable the PPP interface to operate in MP mode
- Specify the bundling mode on the virtual template interface

Advanced MP configuration tasks include:

- Configure the maximum number of links allowed in an MP bundle
- Set minimum outgoing MP packet fragment size

II. Configuring MP on an MP-group interface

- Create/delete an MP-group interface
- Assign or remove interfaces to or from the MP-group

These two configuration tasks are order independent.

1.3.1 Configuring MP on a Virtual Template Interface

I. Creating a virtual template interface

Perform the following configuration in system view.

Table 1-18 Create/delete a virtual template interface

Operation	Command
Create an MP virtual template interface and enter its view	**interface virtual-template** *number*
Delete the specified MP virtual template interface	**undo interface virtual-template** *number*

II. Assigning physical interfaces to or associating a remote username with the virtual template interface

When configuring MP on the virtual template interface, you can do one of the following:

- Assign physical interfaces to the virtual template using the **ppp mp virtual-template** command. In this case, the configuration of authentication is optional. Without authentication, the system bundles links according to the remote endpoint descriptor. With authentication, the system bundles links according to both remote username and endpoint descriptor.
- Associate a username with the virtual template. When bundling links, the system searches for the associated virtual template interface according to the provided valid username and bundles links according to the username and the remote

endpoint descriptor. To ensure a successful link negotiation, you must configure the **ppp mp** command and two-way authentication (CHAP or PAP) on the bundled interfaces.

📖 **Note:**

- When the **ppp mp virtual-template** command is configured on an interface, the system does not look for a virtual template by username. Instead, it looks for the template configured by the command.
- You must configure the to-be-bundled interfaces in the same way.
- In practice, you may configure one-way authentication, where one end associates physical interfaces to a virtual template interface and the other end searches for the virtual template interface by username.
- A virtual template interface is preferred to provide only one service, such as MP, L2TP, or PPPoE.

1) Assign physical interfaces to the virtual template

Perform the following configuration in interface view.

Table 1-19 Assign the physical interface to the specified virtual template

Operation	Command
Assign the interface to the specified virtual template	**ppp mp virtual-template** *number*
Disable MP bundling on the interface	**undo ppp mp**

The configuration of PPP authentication on the physical interface is optional; it is irrelevant to MP connection setup.

2) Associate a username with the virtual template interface

Perform the following configuration in system view.

Table 1-20 Associate a username with the specified virtual template interface

Operation	Command
Associate an MP username with the specified virtual template interface	**ppp mp user** *username* **bind virtual-template** *number*
Remove the binding	**undo ppp mp user** *username*

In this approach to MP, the system searches for a virtual template interface by username. Therefore, to set up an MP connection, you must configure two-way PPP authentication on the involved physical interfaces. For more information about PPP authentication, refer to the section 1.2.3 "Configuring PPP Authentication Mode and Username and User Password".

In addition, perform the following configuration in interface view to have the interface operate in MP mode.

Table 1-21 Set the PPP-encapsulated interface to operate in MP mode

Operation	Command
Set the PPP-encapsulated interface to work in MP mode	**ppp mp**
Set the interface to work in a common PPP mode	**undo ppp mp**

By default, the PPP-encapsulated interface is operating in a common PPP mode.

III. Specifying the bundling mode on the virtual template interface

Username discussed here refers to the remote username received during PAP or CHAP authentication performed when setting up a PPP connection. An endpoint descriptor uniquely identifies a router; here, it refers to the remote endpoint descriptor received during LCP negotiation. The system distinguishes among the MP bundles on a virtual template interface by username and endpoint descriptor.

Perform the following configuration in VT view or Dialer view.

Table 1-22 Specify the bundling mode on the virtual template interface

Operation	Command
Bundle according to authenticated username	**ppp mp binding-mode authentication**
Bundle according to endpoint descriptor	**ppp mp binding-mode descriptor**
Bundle according to both username and endpoint descriptor	**ppp mp binding-mode both**
Restore the default bundle mode	**undo ppp mp binding-mode**

By default, the system performs bundle according to the authenticated username and terminal identifier simultaneously.

After the configurations above, the basic MP configuration is finished. The user can configure other MP optional parameters as needed.

📖 **Note:**

- If the **ppp mp binding-mode authentication** command is configured to enable the router to perform MP bundling according to authenticated username, you are recommended to configure PPP PAP or CHAP authentication on physical subchannels. Otherwise, all users are regarded anonymous and their corresponding subchannels are assigned to a default bundle. As this bundle has no name, its information is not available when the **display ppp mp** command is performed.
- After configuring the **ppp mp binding-mode** command on a virtual template interface, shut down all its physical subchannels and then undo the operation to have the command take effect.

IV. Configuring maximum/minimum number of mp bundled links (optional)

Execute the **ppp mp max-bind** command in virtual-template view or dialer interface view. Execute the **ppp mp min-bind** command in dialer interface view.

Table 1-23 Configure maximum/minimum number of MP bundled links

Operation	Command
Configure maximum number of MP bundled links	**ppp mp max-bind** *max-bind-num*
Restore the default configuration	**undo ppp mp max-bind**
Configure minimum number of MP bundled links	**ppp mp min-bind** *min-bind-num*
Restore the default configuration	**undo ppp mp min-bind**

By default, the maximum number of bundled links is 16 and the minimum number is 1.

min-bind-num must be less than *max-bind-num*.

🕮 **Note:**

- The upper limit on minimum/maximum number of bundled links is 128, a number set considering only the functionality of MP.
- The forwarding performance of MP is irrelevant to the number of bundled links. When configuring minimum/maximum number of bundled links, you need to consider interface type, interface bandwidth, and forwarding performance of the router.
- On dial PPP MP links, both the **ppp mp max-bind** command and the **ppp mp min-bind** command are available. On non-dial PPP MP links, however, only the **ppp mp max-bind** command is available. For the functions of these commands, refer to "DCC Configuration" in the "Dial-up" part of this manual.

V. Setting minimum outgoing mp packet fragment size (optional)

Perform the following configuration in virtual-template view.

Table 1-24 Set the minimum fragment size of the MP outgoing packets

Operation	Command
Set the minimum fragment size for fragmenting MP outgoing packets.	**ppp mp min-fragment** *size*
Restore the default setting.	**undo ppp mp min-fragment**

By default, the minimum packet size for MP packet to fragment is 128.

1.3.2 Configuring MP on an MP-Group Interface

I. Creating an MP-group interface

Perform the following configuration in system view.

Table 1-25 Create an MP-group interface

Operation	Command
Create an MP-group interface	**interface mp-group** *number*
Delete an MP-group interface	**undo interface mp-group** *number*

II. Assigning interfaces to the MP-group

Perform the following configuration in interface view.

Table 1-26 Assign the interface to the specified MP-group

Operation	Command
Assign the interface to the specified MP-group	**ppp mp mp-group** *number*
Remove the interface from the specified MP-group	**undo ppp mp mp-group** *number*

1.3.3 Configuring the Size of the MP Sort Window

When MP applies, packets may be received out of order. The sort window is thus used to re-order packets. The size of the sort window is a trade-off between re-ordering effect and delay: a large sort window brings good re-ordering effect but increased delay. For voice packets, transmission delay should be minimized.

Perform the following configuration in virtual template interface or MP-group interface view.

Table 1-27 Configure the size of the MP sort window

Operation	Command
Configure the size of the MP sort window	**ppp mp sort-buffer-size** *size*
Restore the default size of the MP sort window	**ppp mp sort-buffer-size** *size*

The default size of the MP sort window is 1, that is, only one packet is sorted.

1.4 Configuring PPP Link Efficiency Mechanism

Four mechanisms are available for improving transmission efficiency on PPP links. They are IP header compression (IPHC), Stac Lempel-Ziv standard (Stac LZS) compression on PPP packets, V. Jacobson Compressing TCP/IP Headers (VJ TCP header compression), and link fragmentation and interleaving (LFI).

I. IP header compression

IPHC is a host-to-host protocol that applies to transmit multimedia services such as voice and video over IP networks. To decrease the bandwidth consumed by headers, you may enable IP header compression on PPP links to compress RTP (including IP, UDP, and RTP) headers or TCP headers. The following describes how compression operates taking RTP header compression for example.

The real-time transport protocol (RTP) is virtually a UDP protocol using fixed port number and format. Since its publication as RFC 1889, there has been growing interest in using RTP as one step to achieve interoperability among different implementations of network audio/video applications. However, there is also concern that 40-byte IP/UDP/RTP header containing a 20-byte IP header, 8-byte UDP header and 12-byte RTP header, is too large an overhead for 20-byte or 160-byte payloads.

To reduce overhead, you can use IPHC to compress headers. In many cases, all three headers can be compressed to 2 to 5 bytes. The effect of the header compression proves considerable that a payload of 40 bytes can be compressed to 5 bytes through the process with the compression ratio as (40+40) / (40+5), about 1.78. The process of IPHC is illustrated in the following figure.

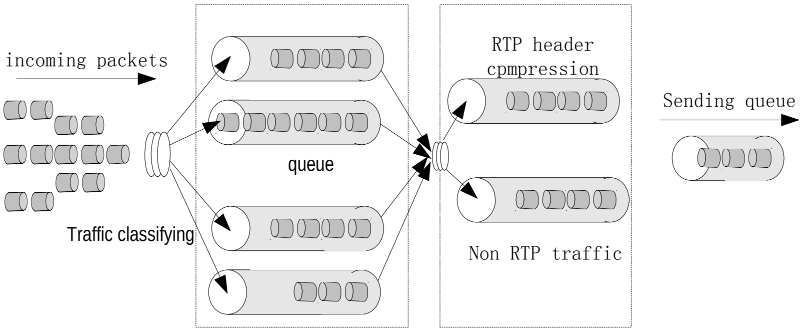


Figure 1-3 IP header compression

II. Stac LZS compression

Stac LZS compression is a link-layer data compression standard developed by Stac Electronics. Stac LZS is a Lempel-Ziv-based algorithm that compresses only packet payloads. It replaces a continuous data flow with binary code that can accommodate to the change of data. While allowing for more flexibility, this requires more CPU resources.

III. VJ TCP header compression

VJ TCP header compression was defined in RFC 1144 for use on low-speed links.

Each TCP/IP packet transmitted over a TCP connection contains a typical 40-byte TCP/IP header containing an IP header and a TCP header that are 20-byte long each. The information in some fields of these headers, however, is unchanged through the lifetime of the connection and needs sending only once, while the information in some other fields changes but regularly and within a definite range. Based on this idea, VJ TCP header compression may compress a 40-byte TCP/IP header to 3 to 5 bytes. It can significantly improve the transmission speed of some applications, such as FTP, on a low-speed serial link like PPP.

IV. Link Fragmentation and Interleaving

On the low speed serial link, real-time interactive communication (such as Telnet and VoIP) is performed, and block and delay may occur when large packets are transmitted. For example, if a voice packet arrives when large packets are being scheduled and waiting for being transmitted, it has to wait until all the large packets have been transmitted. As for the real-time applications, large packets can cause block and delay, consequently, the remote end cannot hear continuous speech. It is required by the interactive voice that the end-to-end delay cannot be larger than 100-150ms.

Dispatching a large packet of 1500 bytes through a 56-kbps line, perhaps will take 215 ms, this will exceed the delay point that one can tolerate. LFI is a method for fragmenting larger packets and adding both the smaller packets and fragments of the large packet to the queue. The fragmented datagrams are reassembled at the destination. LFI can reduce delay of real-time packets on relatively slow bandwidth links.

The following figure describes the process of link fragmentation and interleaving. When large packets and small voice packets arrives at an interface at the same time, the large packets are fragmented into small fragments. If the interface is configured with WFQ, the voice packets and these small fragments are interleaved together and put into the WFQ.

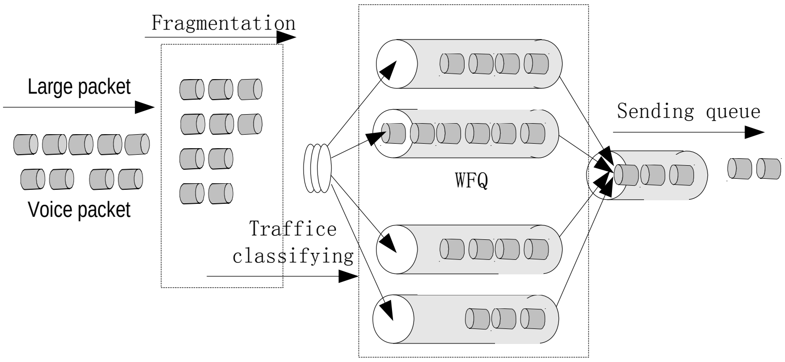


Figure 1-4 Link fragmentation and interleaving

1.4.1 Configuring IPHC

IPHC configuration tasks are described in the following sections:

- Enabling/disabling IPHC
- Configuring maximum number of compression-enabled TCP connections (optional)
- Configuring maximum number of compression-enabled RTP connections (optional)

I. Enabling/disabling IPHC

Executing the command in the following table can enable the IP header compression on some interface. Enabling IP header compression enables the system to compress the TCP packets for RTP session setup. Likewise, disabling IP header compression disables the system to compress the TCP packets for RTP session setup.

You must configure IP header compression at the endpoints of a link.

Perform the following configurations in interface view.

Table 1-28 Enable/disable IPHC

Operation	Command
Enable IPHC.	**ppp compression iphc** [**nonstandard**]
Disable IPHC.	**undo ppp compression iphc**

II. Configuring maximum number of compression-enabled TCP connections

You can configure maximum number of compression-enabled TCP connections.

Perform the following configuration in interface view.

Table 1-29 Configure maximum number of compression-enabled TCP connections

Operation	Command
Configure maximum number of compression-enabled TCP connections	**ppp compression iphc tcp-connections** *number*
Restore the default	**undo ppp compression iphc tcp-connections**

The parameter *number* indicates the maximum number of TCP compression connections on the interface. It is 16 by default.

III. Configuring maximum number of compression-enabled RTP connections

You can configure maximum number of compression-enabled RTP connections.

Perform the following configurations in interface view.

Table 1-30 Configure maximum number of compression-enabled RTP connections

Operation	Command
Configure maximum number of compression-enabled RTP connections	**ppp compression iphc rtp-connections** *number*
Restore the default	**undo ppp compression iphc rtp-connections**

The *number* argument specifies the maximum number of compression-enabled RTP connections (in the range 3 to 1000) on the interface. It defaults to 16.

1.4.2 Configuring PPP Stac LZS Compression

Perform the following configuration in interface view.

The current system version supports the Stac compression described in RFC 1974.

Table 1-31 Configure PPP Stac LZS compression

Operation	Command
Enable Stac LZS compression on the interface.	**ppp compression stac-lzs**
Disable Stac LZS compression on the interface.	**undo ppp compression stac-lzs**

By default, compression is disabled.

1.4.3 Configuring VJ TCP Header Compression for PPP Packets

Perform the following configuration in interface view.

Table 1-32 Configure VJ TCP header compression

Operation	Command
Enable VJ TCP header compression on the PPP interface.	**ip tcp vjcompress**
Disable VJ TCP header compression on the PPP interface.	**undo ip tcp vjcompress**

By default, VJ TCP header compression is disabled on the PPP interface.

1.4.4 Configuring Link Fragmentation and Interleaving on PPP

The real-time interactive communication may be congested and delayed because of large packets on the low-speed serial link. For example, the voice packet arrives while the large packet is being dispatched and waiting for transmission, it can only be dispatched upon the completion of the large packet transmission; thus, delay occurs. For the real-time reference programs such as the interacting voice, congestion delay resulted from large packet is too long. Link Fragment and Interleave (LFI) divides the large data frame into small frames and then transmits them to the front of the transmission queue and inserts the small packets that are sensitive to delay between the fragments. In this way, the delay of small real-time packet is reduced and fragments can be reassembled at the destination.

The LFI configuration tasks are described in the following subsections:

- Enabling LFI
- Configuring maximum time delay of LFI fragments

I. Enabling LFI

Perform the following configurations in virtual template interface view or MP-group interface view.

Table 1-33 Enable LFI

Operation	Command
Enable LFI on Virtual Template interface	**ppp mp lfi**
Disable LFI on Virtual Template interface	**undo ppp mp lfi**

LFI is not enabled by default.

II. Configuring maximum time delay of LFI fragments

The following command sets the maximum time delay for transmitting an LFI fragment.

Perform the following configurations in virtual template interface view or mp-group interface view.

Table 1-34 Configure maximum time delay of LFI fragment

Operation	Command
Configure maximum time delay of LFI fragment	**ppp mp lfi delay-per-frag** *time*
Restore the default maximum time delay of LFI fragment	**undo ppp mp lfi delay-per-frag**

The default fragment delay is 10 milliseconds after LFI is enabled.

The fragment size is calculated considering the specified forwarding delay as follows:

Fragment size = Virtual bandwidth of virtual interface x LFI delay

The minimum fragment size you can configure on the router is 40 bytes. If a smaller fragment size is calculated for a packet, the router chops it into 40-byte fragments.

For assigning bandwidth to a virtual interface, refer to the **qos max-bandwidth** command.

1.5 Displaying and Debugging PPP/MP/PPP Link Efficiency Mechanisms

Execute the **display** command in any view and the **debugging** and **reset** commands in user view.

Table 1-35 Display and debug PPP and MP

Operation	Command
Display PPP configuration and running state of an interface	**display interface** *type number*
Display MP interface information	**display ppp mp** [**interface** *interface-type interface-num*]
Display information about one or all virtual template interfaces	**display virtual-access vt** [*vt-number*]
Display information about one or all virtual access interfaces	**display virtual-access** [*va-number*]

Table 1-36 Display and debug PPP link efficiency mechanisms

Operation	Command
Display statistics about TCP header compression	**display ppp compression iphc tcp** [*interface-type interface-number*]
Display statistics about RTP header compression	**display ppp compression iphc rtp** [*interface-type interface-number*]
Display statistics about Stac LZS header compression	**display ppp compression stac-lzs**
Enable TCP header compression debugging	**debugging ppp compression iphc tcp** { **all** | **context_state** | **error** | **full_header** | **general_info** }
Enable RTP header compression debugging	**debugging ppp compression iphc rtp** { **all** | **context_state** | **error** | **full_header** | **general_info** }
Clear all statistics about IP header compression	**reset ppp compression iphc** [*interface-type interface-number*]
Clear all statistics about Stac LZS header compression	**reset ppp compression stac-lzs**

1.6 PPP and MP Configuration Example

1.6.1 PAP Authentication

I. Network requirements

As shown in Figure 1-5, routers 3Com1 and 3Com2 are interconnected through the interface Serial3/0/0, and 3Com1 is required to authenticate 3Com2 in PAP mode.

II. Network diagram

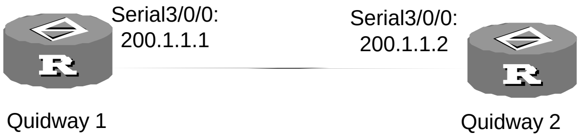


Figure 1-5 Network diagram for PAP authentication

III. Configuration procedure

1) Configure router 3Com1:

```
[3Com] local-user 3Com2
[3Com-luser-3Com2] service-type ppp
[3Com-luser-3Com2] password simple 3Com
[3Com] interface serial 3/0/0
[3Com-Serial3/0/0] link-protocol ppp
[3Com-Serial3/0/0] ppp authentication-mode pap domain system
[3Com-Serial3/0/0] ip address 200.1.1.1 16
[3Com] domain system
[3Com-isp-system] scheme local
```

2) Configure router 3Com2:

```
[3Com] interface serial 3/0/0
[3Com-Serial3/0/0] link-protocol ppp
[3Com-Serial3/0/0] ppp pap local-user 3Com2 password simple 3Com
[3Com-Serial3/0/0] ip address 200.1.1.2 16
```

1.6.2 Unidirectional CHAP Authentication

I. Network requirements

As shown in Figure 1-6, 3Com 1 is required to use CHAP to authenticate 3Com 2.

II. Network diagram

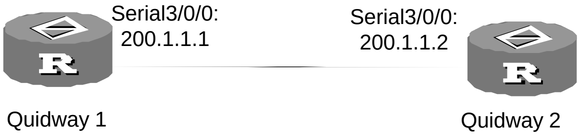


Figure 1-6 Network diagram for CHAP authentication

III. Configuration procedure

Approach I: 3Com 1 and 3Com 2 have users with the same password.

1) Configure 3Com 1

```
[3Com] local-user 3Com2
```

```
[3Com-luser-3Com2] password simple hello
[3Com-luser-3Com2] service-type ppp
[3Com-luser-3Com2] quit
[3Com] interface serial 3/0/0
[3Com-Serial3/0/0] link-protocol ppp
[3Com-Serial3/0/0] ppp chap user 3Com1
[3Com-Serial3/0/0] ppp authentication-mode chap domain system
[3Com-Serial3/0/0] ip address 200.1.1.1 16
[3Com-Serial3/0/0] quit
[3Com] domain system
[3Com-isp-system] scheme local
```

2) Configure 3Com 2

```
[3Com] local-user 3Com1
[3Com-luser-3Com1] service-type ppp
[3Com-luser-3Com1] password simple hello
[3Com-luser-3Com1] quit
[3Com] interface serial 3/0/0
[3Com-Serial3/0/0] link-protocol ppp
[3Com-Serial3/0/0] ppp chap user 3Com2
[3Com-Serial3/0/0] ip address 200.1.1.2 16
```

Approach II: 3Com 1and 3Com 2 have no users with the same password.

3) Configure 3Com 1

```
[3Com] local-user 3Com2
[3Com-luser-3Com2] password simple hello
[3Com-luser-3Com2] service-type ppp
[3Com-luser-3Com2] quit
[3Com] interface serial 3/0/0
[3Com-Serial3/0/0] ppp authentication-mode chap domain system
[3Com-Serial3/0/0] ip address 200.1.1.1
[3Com-Serial3/0/0] quit
[3Com] domain system
[3Com-isp-system] scheme local
```

4) Configure 3Com 2

```
[3Com] interface serial 3/0/0
[3Com-Serial3/0/0] ppp chap user 3Com2
[3Com-Serial3/0/0] ppp chap password simple hello
[3Com-Serial3/0/0] ip address 200.1.1.2
```

If you configure the **ppp authentication-mode chap** command without specifying a domain to system for example, the default domain named system is adopted at the time of authentication and local authentication applies by default.

1.6.3 Bidirectional CHAP Authentication

I. Network requirements

As shown in Figure 1-7, 3Com 1 and 3Com 2 are required to use CHAP to authenticate each other. The password for CHAP authentication is hello-1 on 3Com 1 and hello-2 on 3Com 2.

II. Network diagram

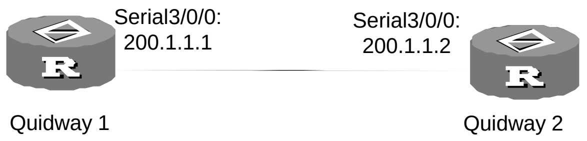


Figure 1-7 Network diagram for CHAP authentication

III. Configuration procedure

1) Configure 3Com 1

```
[3Com1] local-user 3Com2
[3Com1-luser-3Com2] password simple hello-2
[3Com1-luser-3Com2] service-type ppp
[3Com1-luser-3Com2] quit
[3Com1] interface serial 3/0/0
[3Com1-Serial3/0/0] ppp authentication-mode chap domain system
[3Com2-Serial3/0/0] ppp chap user 3Com1
[3Com1-Serial3/0/0] ppp chap password simple hello-1
[3Com1-Serial3/0/0] ip address 200.1.1.1
[3Com1-Serial3/0/0] quit
[3Com1] domain system
[3Com1-isp-system] scheme local
```

2) Configure 3Com 2

```
[3Com2] local-user 3Com1
[3Com2-luser-3Com2] password simple hello-1
[3Com2-luser-3Com2] service-type ppp
[3Com2-luser-3Com2] quit
[3Com2] interface serial 3/0/0
[3Com2-Serial3/0/0] ppp authentication-mode chap domain system
[3Com2-Serial3/0/0] ppp chap user 3Com2
[3Com2-Serial3/0/0] ppp chap password simple hello-2
[3Com2-Serial3/0/0] ip address 200.1.1.2
```

As the password configured with the **ppp chap password** command takes priority over the one configured in local user view at the authenticatee end, CHAP authentication can pass even when the two parties use different passwords.

1.6.4 MP Configuration

I. Network requirements

Figure 1-8 presents a scenario, where:

- On an E1 interface of Router A, four channels are created with interface names being Serial 2/0/0:1, Serial 2/0/0:2, Serial2/0/0:3, and Serial 2/0/0:4 respectively.
- On Router B, two channels are created with interface names being Serial 2/0/0:1 and Serial 2/0/0:2 respectively. The same is done on Router C.

Do the following:

- Bind two channels on Router A with the two channels on Router B and another two channels with the two channels on Router C.
- Adopt binding authentication.

II. Network diagram

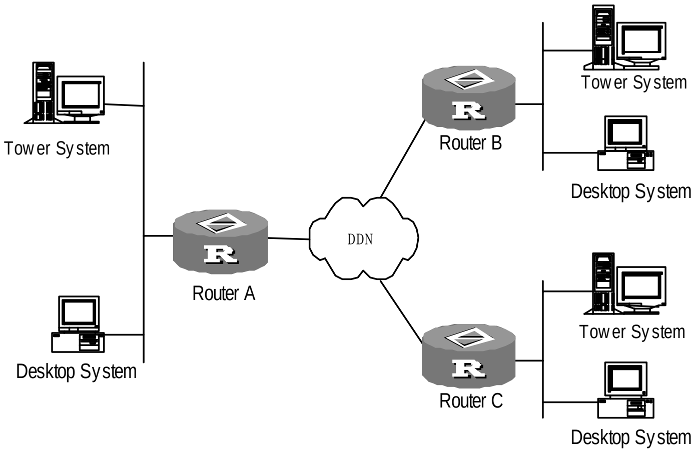


Figure 1-8 Network diagram of MP configuration example

III. Configuration procedure

1) Configure Router A:

# Add the users for Router B and Router C

```
[3Com] local-user router-b
[3Com-luser-router-b] password simple router-b
[3Com] local-user router-c
[3Com-luser-router-c] password simple router-c
```

# Specify the virtual-templates for the two users and begin PPP negotiation by using the NCP information of the virtual-templates.

```
[3Com] ppp mp user router-b bind virtual-template 1
[3Com] ppp mp user router-c bind virtual-template 2
```

# Configure the virtual-templates

```
[3Com] interface virtual-template 1
[3Com-virtual-template1] ip address 202.38.166.1 255.255.255.0
[3Com] interface virtual-template 2
[3Com-virtual-template2] ip address 202.38.168.1 255.255.255.0
```

# Assign interfaces Serial 2/0/0:1, Serial 2/0/0:2, Serial 2/0/0:3, and Serial 2/0/0:4 to MP channels, taking Serial2/0/0:1 for an example.

```
[3Com] interface serial 2/0/0:1
[3Com-Serial2/0/0:1] link-protocol ppp
[3Com-Serial2/0/0:1] ppp mp
[3Com-Serial2/0/0:1] ppp authentication-mode pap domain system
[3Com-Serial2/0/0:1] ppp pap local-user router-a password simple router-a
```

# Configure the users in the domain to use the local authentication scheme.

```
[3Com] domain system
[3Com-isp-domain] scheme local
```

2) Configure Router B:

# Add a user for Router A

```
[3Com] local-user router-a
[3Com-luser-router-a] password simple router-a
```

# Specify the virtual-template for this user and begin PPP negotiation by using the NCP information of this template

```
[3Com] ppp mp user router-a bind virtual-template 1
```

# Configure operating parameters of the virtual-template

```
[3Com] interface virtual-template 1
[3Com-Virtual-Template1] ip address 202.38.166.2 255.255.255.0
```

# Assign interfaces Serial 2/0/0:1 and Serial 2/0/0:2 to the MP channel, taking Serial 2/0/0:1 for an example.

```
[3Com] interface serial 2/0/0:1
[3Com-Serial2/0/0:1] ppp mp
[3Com-Serial2/0/0:1] ppp authentication-mode pap domain system
[3Com-Serial2/0/0:1] ppp pap local-user router-b password simple router-b
```

3) Configure Router C:

# Add a user for Router A

```
[3Com] local-user router-a
[3Com-luser-router-a] password simple router-a
```

# Specify a virtual-template for this user and the NCP information of the template will be used for PPP negotiation.

```
[3Com] ppp mp user router-a bind virtual-template 1
```

# Configure operating parameters of the virtual-template

```
[3Com] interface virtual-template 1
[3Com-Virtual-Template1] ip address 202.38.168.2 255.255.255.0
```

# Assign interfaces Serial 2/0/0:1 and Serial 2/0/0:2 to the MP channel, taking Serial 2/0/0:1 for an example.

```
[3Com] interface serial 2/0/0:1
[3Com-Serial2/0/0:1] ppp mp
[3Com-Serial2/0/0:1] ppp authentication-mode pap domain system
[3Com-Serial2/0/0:1] ppp pap local-user router-c password simple router-c
```

# Configure the users in the domain to use the local authentication scheme.

```
[3Com] domain system
[3Com-isp-domain] scheme local
```

1.6.5 Three Types of MP Binding Mode

I. Network requirements

As showed in the figure below, RouterA and RouterB are connected together through serial ports, serial1/0/0 to serial1/0/0 and serial2/0/0 to serial 2/0/0 respectively. Three binding modes that are demonstrated are directly Virtual-Template binding mode, authentication binding mode and MP-group interface binding mode.

II. Network diagram

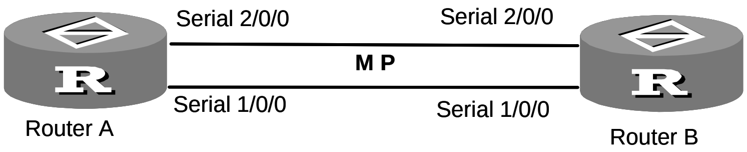


Figure 1-9 Network diagram of MP binding

III. Configuration procedure

1) Directly assign physical interfaces to a virtual template interface

Configure Router A:

# Configure the user name and password of Router B

```
<3Com> system-view
[3Com] local-user RTB
[3Com-luser-RTB] password simple RTB
[3Com-luser-RTB] service-type ppp
[3Com-luser-RTB] quit
```

# Create a virtual template interface and assign an IP address to it.

```
[3Com] interface Virtual-Template 1
[3Com-Virtual-Template1] ip address 8.1.1.1 24
```

# Configure Serial1/0/0.

```
[3Com-Virtual-Template1] interface Serial1/0/0
[3Com-Serial1/0/0] link-protocol ppp
[3Com-Serial1/0/0] ppp authentication-mode pap domain system
[3Com-Serial1/0/0] ppp pap local-user RTA password simple RTA
[3Com-Serial1/0/0] ppp mp virtual-template 1
[3Com-Serial1/0/0] shutdown
[3Com-Serial1/0/0] undo shutdown
```

# Configure Serial2/0/0.

```
[3Com-Serial1/0/0] interface Serial2/0/0
[3Com-Serial2/0/0] link-protocol ppp
[3Com-Serial2/0/0] ppp authentication-mode pap domain system
[3Com-Serial2/0/0] ppp pap local-user RTA password simple RTA
[3Com-Serial2/0/0] ppp mp virtual-template 1
[3Com-Serial2/0/0] shutdown
[3Com-Serial2/0/0] undo shutdown
[3Com-Serial2/0/0] quit
[3Com] domain system
[3Com-isp-domain] scheme local
```

Configure Router B:

# Configure the user name and password of Router A

```
<3Com> system-view
[3Com] local-user RTA
[3Com-luser-RTA] password simple RTA
[3Com-luser-RTA] service-type ppp
[3Com-luser-RTA] quit
```

# Create a virtual-template interface and assign an IP address to it.

```
[3Com] interface Virtual-Template 1
[3Com-Virtual-Template1] ip address 8.1.1.2 24
```

# Configure Serial1/0/0.

```
[3Com-Virtual-Template1] interface Serial1/0/0
[3Com-Serial1/0/0] link-protocol ppp
[3Com-Serial1/0/0] ppp authentication-mode pap domain system
[3Com-Serial1/0/0] ppp pap local-user RTB password simple RTB
[3Com-Serial1/0/0] ppp mp virtual-template 1
[3Com-Serial1/0/0] shutdown
[3Com-Serial1/0/0] undo shutdown
```

# Configure Serial2/0/0.

```
[3Com-Serial1/0/0] interface Serial2/0/0
```

```
[3Com-Serial2/0/0] link-protocol ppp
[3Com-Serial2/0/0] ppp authentication-mode pap domain system
[3Com-Serial2/0/0] ppp pap local-user RTB password simple RTB
[3Com-Serial2/0/0] ppp mp virtual-template 1
[3Com-Serial2/0/0] shutdown
[3Com-Serial2/0/0] undo shutdown
[3Com-Serial2/0/0] quit
```

# Configure the users in the domain to use the local authentication scheme.

```
[3Com] domain system
[3Com-isp-domain] scheme local
[3Com-isp-domain] quit
```

Verify the results on Router A:

```
[3Com] display ppp mp
Template is Virtual-Template1
max-bind: 16, min-fragment: 128
Bundle RTB, 2 members, slot 1, Master link is Virtual-Template1:0
Peer's endPoint descriptor: 72341c2a4093
 Bundle Up Time:        2005/04/07  16:02:32:30
0 lost fragments, 0 reordered, 0 unassigned, 0 interleaved,
sequence 0/0 rcvd/sent

The member channels bundled are:
      Serial1/0/0         Up-Time:2005/04/07  16:02:32:30
      Serial2/0/0         Up-Time:2005/04/07  16:07:38:30
```

Check information about virtual access interfaces:

```
[3Com] display virtual-access vt
----------------Slot 1----------------
Virtual-Template1:0 current state : UP
Line protocol current state : UP
Description : Virtual-Template1:0 Interface
The Maximum Transmit Unit is 1500
Link layer protocol is PPP
LCP opened, MP opened, IPCP opened, OSICP opened, MPLSCP opened
Physical is MP,baudrate: 128000
Output queue : (Urgent queue : Size/Length/Discards)  0/500/0
Output queue : (Protocol queue : Size/Length/Discards) 0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
Last 300 seconds input:  0 bytes/sec 0 packets/sec
Last 300 seconds output:  0 bytes/sec 0 packets/sec
    6 packets input, 66 bytes, 0 drops
    6 packets output, 66 bytes, 0 drops
```

The display about Router A is similar.

On Router B ping the IP address 8.1.1.1.

```
[3Com] ping 8.1.1.1
  PING 8.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 8.1.1.1: bytes=56 Sequence=1 ttl=255 time=29 ms
    Reply from 8.1.1.1: bytes=56 Sequence=2 ttl=255 time=31 ms
    Reply from 8.1.1.1: bytes=56 Sequence=3 ttl=255 time=29 ms
    Reply from 8.1.1.1: bytes=56 Sequence=4 ttl=255 time=31 ms
    Reply from 8.1.1.1: bytes=56 Sequence=5 ttl=255 time=30 ms

  --- 8.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 29/30/31 ms
```

Because PPP authentication is configured on the physical interface, the Bundle field in the output of the **display ppp mp** command is identified by remote user name. If authentication is disabled, the Bundle field should be identified by the remote endpoint descriptor.

In addition, you can view the state of MP virtual channels by viewing the state of virtual access interfaces with the **display virtual-access** command.

2) Associate remote user name with virtual template interface

Configure Router A:

# Configure the user name and password of Router B

```
<3Com> system-view
[3Com] local-user RTB
[3Com-luser-RTB] password simple RTB
[3Com-luser-RTB] service-type ppp
[3Com-luser-RTB] quit
```

# Assign a virtual-template to user RTB

```
[3Com] ppp mp user RTB bind virtual-template 1
```

# Create a virtual-template and configure the IP address

```
[3Com] interface Virtual-Template 1
[3Com-Virtual-Template1] ip address 8.1.1.1 24
```

# Configure Serial1/0/0.

```
[3Com-Virtual-Template1] interface Serial1/0/0
[3Com-Serial1/0/0] link-protocol ppp
[3Com-Serial1/0/0] ppp authentication-mode pap domain system
[3Com-Serial1/0/0] ppp pap local-user RTA password simple RTA
```

```
[3Com-Serial1/0/0] ppp mp
[3Com-Serial1/0/0] shutdown
[3Com-Serial1/0/0] undo shutdown
```

# Configure Serial2/0/0.

```
[3Com-Serial1/0/0] interface Serial2/0/0
[3Com-Serial2/0/0] link-protocol ppp
[3Com-Serial2/0/0] ppp authentication-mode pap domain system
[3Com-Serial2/0/0] ppp pap local-user RTA password simple RTA
[3Com-Serial2/0/0] ppp mp
[3Com-Serial2/0/0] shutdown
[3Com-Serial2/0/0] undo shutdown
[3Com-Serial2/0/0] quit
```

# Configure the user in the domain to use the local authentication scheme

```
[3Com] domain system
[3Com-isp-domain] scheme local
[3Com-isp-domain] quit
```

Configure Router B

# Configure the user name and password of Router A

```
<3Com> system-view
[3Com] local-user RTA
[3Com-luser-RTA] password simple RTA
[3Com-luser-RTA] service-type ppp
[3Com-luser-RTA] quit
```

# Assign a virtual-template to user RTA

```
[3Com] ppp mp user RTA bind virtual-template 1
```

# Create a virtual-template and configure the IP address

```
[3Com] interface Virtual-Template 1
[3Com-Virtual-Template1] ip address 8.1.1.2 24
```

# Configure Serial1/0/0.

```
[3Com-Virtual-Template1] interface Serial1/0/0
[3Com-Serial1/0/0] link-protocol ppp
[3Com-Serial1/0/0] ppp authentication-mode pap domain system
[3Com-Serial1/0/0] ppp pap local-user RTB password simple RTB
[3Com-Serial1/0/0] ppp mp
[3Com-Serial1/0/0] shutdown
[3Com-Serial1/0/0] undo shutdown
```

# Configure Serial2/0/0.

```
[3Com-Serial1/0/0] interface Serial2/0/0
[3Com-Serial2/0/0] link-protocol ppp
```

```
[3Com-Serial2/0/0] ppp authentication-mode pap domain system
[3Com-Serial2/0/0] ppp pap local-user RTB password simple RTB
[3Com-Serial2/0/0] ppp mp
[3Com-Serial2/0/0] shutdown
[3Com-Serial2/0/0] undo shutdown
[3Com-Serial2/0/0] quit
```

# Apply user authentication to domain users.

```
[3Com] domain system
[3Com-isp-domain] scheme local
[3Com-isp-domain] quit
```

Verify the results on RouterA:

```
<3Com> display ppp mp
Template is Virtual-Template1
max-bind: 16, min-fragment: 128
Bundle RTB, 2 member, slot 1, Master link is Virtual-Template1:0
Peer's endPoint descriptor: 73b03a692ec9
 Bundle Up Time:        2005/04/08  11:13:45:980
0 lost fragments, 0 reordered, 0 unassigned, 0 interleaved,
sequence 0/0 rcvd/sent
The bundled son channels are:
      Serial1/0/0       Up-Time:2005/04/08  11:13:45:980
      Serial2/0/0       Up-Time:2005/04/08  11:13:45:980
```

Verify the results on Router B:

```
[3Com] display ppp mp
Template is Virtual-Template1
max-bind: 16, min-fragment: 128
Bundle RTA, 2 member, slot 1, Master link is Virtual-Template1:0
Peer's endPoint descriptor: 73b03a692ec9
 Bundle Up Time:        2005/04/08  11:13:45:980
0 lost fragments, 0 reordered, 0 unassigned, 0 interleaved,
sequence 0/0 rcvd/sent
The bundled son channels are:
      Serial1/0/0           Up-Time:2005/04/08  11:13:45:980
      Serial2/0/0           Up-Time:2005/04/08  11:13:45:980
```

Check information about virtual access interfaces:

```
<3Com> display virtual-access vt
Virtual-Template1:0 current state : UP
Line protocol current state : UP
Description : Virtual-Template1:0 Interface
The Maximum Transmit Unit is 1500
```

```
Link layer protocol is PPP
LCP opened, MP opened, IPCP opened, OSICP opened, MPLSCP opened
Physical is MP, baudrate: 128000
Output queue : (Urgent queue : Size/Length/Discards)  0/500/0
Output queue : (Protocol queue : Size/Length/Discards) 0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
    Last 300 seconds input:  0 bytes/sec 0 packets/sec
    Last 300 seconds output:  0 bytes/sec 0 packets/sec
    21 packets input, 1386 bytes, 0 drops
    21 packets output, 1386 bytes, 0 drops
```

On Router B ping the remote IP address 8.1.1.1:

```
[3Com] ping 8.1.1.1
  PING 8.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 8.1.1.1: bytes=56 Sequence=1 ttl=255 time=29 ms
    Reply from 8.1.1.1: bytes=56 Sequence=2 ttl=255 time=31 ms
    Reply from 8.1.1.1: bytes=56 Sequence=3 ttl=255 time=30 ms
    Reply from 8.1.1.1: bytes=56 Sequence=4 ttl=255 time=31 ms
    Reply from 8.1.1.1: bytes=56 Sequence=5 ttl=255 time=30 ms

  --- 8.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 29/30/31 ms
```

Incorrect configuration:

The two interfaces (Serial1/0/0 and Serial2/0/0) will be bound to two different MP links if one of them is configured as **ppp mp** while the other is configured as **ppp mp virtual-template 1**. The system cannot run well as our expectation.

3) Configure MP bundling on an MP-group interface

In addition to virtual template interfaces, V 2.41 provides MP-group interfaces to implement MP bundling. This implementation is similar to directly assigning physical interfaces to a virtual template.

Configure Router A:

# Configure the user name and password of Router B

```
<3Com> system-view
[3Com] local-user RTB
[3Com-luser-RTB] password simple RTB
[3Com-luser-RTB] service-type ppp
[3Com-luser-RTB] quit
```

# Create MP-group interface, configure the ip address

```
[3Com] interface mp-group 1
[3Com-Mp-group1] ip address 111.1.1.1 24
```

# Configure Serial1/0/0.

```
[3Com-Mp-group1] interface Serial1/0/0
[3Com-Serial1/0/0] link-protocol ppp
[3Com-Serial1/0/0] ppp authentication-mode pap domain system
[3Com-Serial1/0/0] ppp pap local-user RTA password simple RTA
[3Com-Serial1/0/0] ppp mp mp-group 1
[3Com-Serial1/0/0] shutdown
[3Com-Serial1/0/0] undo shutdown
```

# Configure Serial2/0/0.

```
[3Com-Serial1/0/0] interface Serial2/0/0
[3Com-Serial2/0/0] link-protocol ppp
[3Com-Serial2/0/0] ppp authentication-mode pap domain system
[3Com-Serial2/0/0] ppp pap local-user RTA password simple RTA
[3Com-Serial2/0/0] ppp mp mp-group 1
[3Com-Serial2/0/0] shutdown
[3Com-Serial2/0/0] undo shutdown
[3Com-Serial2/0/0] quit
```

# Configure the users in the domain to use the local authentication scheme.

```
[3Com] domain system
[3Com-isp-domain] scheme local
[3Com-isp-domain] quit
```

Configure Router B

# Configure user name and password for Router A

```
<3Com> system-view
[3Com] local-user RTA
[3Com-luser-RTA] password simple RTA
[3Com-luser-RTA] service-type ppp
[3Com-luser-RTA] quit
```

# Create Mp-group interface and configure ip address

```
[3Com] interface mp-group 1
[3Com-Mp-group1] ip address 111.1.1.2 24
```

# Configure Serial1/0/0.

```
[3Com-Mp-group1] interface Serial1/0/0
[3Com-Serial1/0/0] link-protocol ppp
[3Com-Serial1/0/0] ppp authentication-mode pap domain system
[3Com-Serial1/0/0] ppp pap local-user RTB password simple RTB
[3Com-Serial1/0/0] ppp mp mp-group 1
```

```
[3Com-Serial1/0/0] shutdown
[3Com-Serial1/0/0] undo shutdown
```

# Configure Serial2/0/0.

```
[3Com-Serial1/0/0] interface Serial2/0/0
[3Com-Serial2/0/0] link-protocol ppp
[3Com-Serial2/0/0] ppp authentication-mode pap domain system
[3Com-Serial2/0/0] ppp pap local-user RTB password simple RTB
[3Com-Serial2/0/0] ppp mp mp-group 1
[3Com-Serial2/0/0] shutdown
[3Com-Serial2/0/0] undo shutdown
[3Com-Serial2/0/0] quit
```

# Configure the users in the domain to use the local authentication scheme.

```
[3Com] domain system
[3Com-isp-domain] scheme local
[3Com-isp-domain] quit
```

Verify the results on RouterA

```
[3Com] display ppp mp
Mp-group is Mp-group1
max-bind: 16, min-fragment: 128

Bundle Multilink, slot 1, Master link is Mp-group1
Peer's endPoint descriptor: 73b03a692ec9
 Bundle Up Time:        2005/04/08  11:20:40:970
0 lost fragments, 0 reordered, 0 unassigned, 0 interleaved,
sequence 0/0 rcvd/sent
Member channels: 2 active, 0 inactive
      Serial1/0/0        Up-Time:2005/04/08  11:20:40:970
      Serial2/0/0        Up-Time:2005/04/08  11:20:40:970
```

Check the state about Mp-group1

```
[3Com] display interface Mp-group 1
Mp-group1 current state : UP
Line protocol current state : UP
Description : Mp-group1 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 111.1.1.1/24
Link layer protocol is PPP
LCP opened, MP opened, IPCP opened, MPLSCP opened
Physical is MP, baudrate: 128000
Output queue : (Urgent queue : Size/Length/Discards)  0/500/0
Output queue : (Protocol queue : Size/Length/Discards) 0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
    Last 300 seconds input:  0 bytes/sec, 0 packets/sec
    Last 300 seconds output:  0 bytes/sec, 0 packets/sec
    5 packets input, 58 bytes, 0 drops
    5 packets output, 54 bytes, 0 drops
```

On RouterA ping the remote IP address:

```
[3Com] ping 111.1.1.2
  PING 111.1.1.2: 56  data bytes, press CTRL_C to break
    Reply from 111.1.1.2: bytes=56 Sequence=1 ttl=255 time=29 ms
    Reply from 111.1.1.2: bytes=56 Sequence=2 ttl=255 time=31 ms
    Reply from 111.1.1.2: bytes=56 Sequence=3 ttl=255 time=29 ms
    Reply from 111.1.1.2: bytes=56 Sequence=4 ttl=255 time=30 ms
    Reply from 111.1.1.2: bytes=56 Sequence=5 ttl=255 time=30 ms
  --- 111.1.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 29/29/31 ms
```

Note that in this approach to MP binding, all users are bound together and the concept of virtual access is not involved.

1.7 Troubleshooting

Fault 1: Link never turns into up state.

Problem solving: This problem may arise because of the PPP authentication failure due to the incorrect configuration of PPP authentication parameters.

Enable the debugging of PPP, and you will see the information describing that LCP went up upon a successful LCP negotiation but went down after the PAP or CHAP negotiation.

Fault 2: Physical link failed in going up.

Problem solving: Execute the **display interface serial** *type number* command to view the current interface statuses, including:

“serial number is administratively down, line protocol is down”, which indicates that the interface has been shut down by the administrator.

“serial number is down, line protocol is down”, which indicates that the interface is not active or the physical layer has not gone up yet.

“Virtual-template number is down, line protocol is spoofing up”, which indicates that this interface is a dialer interface and the call establishment attempt has failed.

”serial number is up, line protocol is up”, which indicates that the link negotiation, i.e., the LCP negotiation on this interface has succeeded.

”serial number is up, line protocol is down”, which indicates that this interface is active, but link negotiation has failed.

Chapter 2 PPPoE Configuration

2.1 Introduction to PPPoE

I. PPPoE

Point-to-point protocol over Ethernet (PPPoE) connects a network of hosts formed by Ethernet to a remote access device to gain access to the Internet. It allows you to perform access control and accounting on a per-host basis. Due to its attractive cost effectiveness, PPPoE is widely adopted, for example, in network constructions for residential areas.

PPPoE adopts the client/server model. It provides point-to-point connectivity over Ethernet by encapsulating PPP packets in Ethernet frames.

PPPoE is divided into two distinct phases: discovery and PPP session.

- Discovery phase

When a host wants to start a PPPoE process, it must first identify the MAC address of the Ethernet on the access end and create the SESSION ID of PPPoE. This is the very purpose of the discovery phase.

- PPP session phase

After entering the session phase of PPPoE, the system can encapsulate the PPP packet as the payload of PPPoE frame into an Ethernet frame and then send the Ethernet frame to the peer. In the frame, the SESSION ID must be the one determined at the discovery phase, MAC address must be the address of the peer, and the PPP packet section begins with the Protocol ID. In the Phase of Session, either the host or the server may send PPPoE Active Discovery Terminate (PADT) packets to notify the other to end this Session.

For more information about PPPoE, refer to RFC2516.

II. PPPoE server

The PPPoE server available on 3Com AR Series Routers delivers these features:

- Dynamic IP address allocation.
- Multiple authentication methods such as local authentication and RADIUS/TACACS+. Along with ASPF and packet filter, it provides strong defense for your network.

PPPoE server is applicable to campus networks where Ethernet is used for connecting to the Internet. This however, requires installation of PPPoE client dialup software on user PCs.

III. PPPoE client

PPPoE is widely used in ADSL broadband access applications. Generally, a host must be installed with PPPoE client dialing software in order to access the Internet via ADSL. On 3Com AR Series Routers, the PPPoE client, or PPPoE client dialup, is available to enable users to access the Internet without installing client dial-up software on their PCs. Moreover, all PCs on the same LAN can share the same ADSL account.

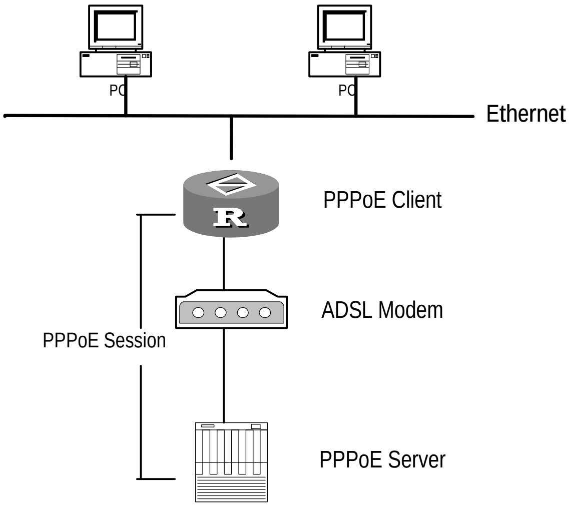


Figure 2-1 Network diagram for PPPoE client

As shown in the above figure, PCs on the Ethernet are connected to the 3Com router where PPPoE client runs. The data destined to the Internet first reaches the router and is encapsulated in PPPoE there. After leaving the router, it passes through the ADSL modem attached to the router and then the ADSL access server before reaching the Internet. This can be done without PPPoE client dial-up software.

2.2 PPPoE Server Configuration

PPPoE server configurations include:

Fundamental configuration task of PPPoE server includes:

Create a virtual template and configure the related parameters

- Enable/disable PPPoE server
- Configure PPPoE user authentication

Advanced configuration task of PPPoE includes:

- Configure other PPPoE server parameters

2.2.1 Creating a Virtual Template

I. Creating a virtual template

Perform the following configuration in system view.

Table 2-1 Create/delete a virtual template

Operation	Command
Create a virtual template and enter its view.	**interface virtual-template** *number*
Delete the specified virtual template.	**undo interface virtual-template** *number*

II. Setting the operating parameters of a virtual template

Compared with physical interfaces, the virtual template interface only supports PPP at the link layer and IP at the network layer. When configuring a virtual template, you need to perform the following tasks:

Set the operating parameters of PPP

Assign an IP address to the virtual template

Configure the IP address or address pool for address allocation

2.2.2 Enabling/Disabling PPPoE Server

Perform the following configuration in interface view.

The commands in the following table are restricted to Ethernet interfaces (including subinterfaces). More specifically, While PPPoE is enabled on an Ethernet interface, it is not accordingly enabled on other Ethernet interfaces. Likewise, when PPPoE is disabled on an Ethernet interface, it is not necessarily disabled on other Ethernet interfaces.

Note: Before beginning the configuration in Table 2-1, you have to finish the configuration of the virtual template interface. For detailed description of the virtual-template, please refer to the section of Virtual Interface Configuration.

Table 2-2 Enable/disable PPPoE

Operation	Command
Enable PPPoE on Ethernet interface	**pppoe-server bind virtual-template** *number*
Disable PPPoE on Ethernet interface	**undo pppoe-server bind**

Where, *number* is the number of virtual-template.

By default, PPPoE is disabled.

2.2.3 Configuring PPPoE Server Parameters

You may configure PPPoE server parameters as needed. Normally, you can use the default settings.

Perform the following configuration in system view.

Table 2-3 Configure PPPoE server parameters

Operation	Command
Configure the maximum number of PPPoE sessions allowed to be set up with a remote MAC address. This number is in the range of 1 to 4096.	**pppoe-server max-sessions remote-mac** *number*
Restore the default maximum number of PPPoE sessions (100) allowed to be set up with a remote MAC address.	**undo pppoe-server max-sessions remote-mac**
Configure the maximum number of PPPoE sessions that a local MAC address is allowed to set up. This number is in the range of 1 to 4096.	**pppoe-server max-sessions local-mac** *number*
Restore the default maximum number of PPPoE sessions (100) that a local MAC address is allowed to set up.	**undo pppoe-server max-sessions local-mac**
Configure the maximum number of PPPoE sessions that the current system is allowed to set up.	**pppoe-server max-sessions total** *number*
Restore the default maximum number of PPPoE sessions (4096) that the current system is allowed to set up.	**undo pppoe-server max-sessions total**

For the commands **pppoe-server max-sessions local-mac** and **pppoe-server max-sessions remote-mac**, the default value of *number* is 100; while for the command **pppoe-server max-sessions total**, the default value of *number* is 4096.

2.2.4 Configuring PPPoE User Authentication

Normally, PPPoE Server requires authentication and accounting on PPP users. For more information, refer to the “Security” part of this manual.

2.3 Configuring PPPoE Client

Fundamental PPPoE configuration tasks include:

- Configure a dialer interface
- Configure a PPPoE session

Advanced PPP configuration task includes:

- Terminate a PPPoE session

2.3.1 Configuring a Dialer Interface

Before configuring PPPoE session, you should first configure a dialer interface and configure a dialer bundle on the interface. Each PPPoE session uniquely corresponds to a dialer bundle and each dialer bundle uniquely corresponds to a dialer interface. Thus, a PPPoE session can be created via a dialer interface.

Execute the **dialer-rule** and **interface dialer** commands in system view, and execute other commands below in dialer interface view.

Table 2-4 Configure a dialer interface

Operation	Command
Configure a dialer rule	**dialer-rule** *dialer-group* { *protocol-name* { **permit | deny** } **| acl** *acl-number* }
Create a dialer interface	**interface dialer** *number*
Enable RS-DCC and set a remote user name	**dialer user** *username*
Configure IP address of the interface.	**ip address** { *address mask* | **ppp-negotiate** }
Configure the Dialer Bundle on an interface	**dialer bundle** *bundle-number*
Configure the Dialer Group on an interface	**dialer-group** *group-number*

PPPoE only supports RS-DCC. As needed, such parameters as PPP authentication may also be necessarily configured on a dialer interface. For more information on how to configure a dialer interface, refer to the chapter discussing DDD configurations in the “Dial-up” part of this manual.

2.3.2 Configuring a PPPoE Session

PPPoE session can be configured on a physical Ethernet interface (or Ethernet subinterface) or a virtual Ethernet (VE) interface created on an ADSL interface. When a router is to be linked to the Internet through an ADSL interface, it is necessary to configure PPPoE session on the virtual Ethernet interface; when a router is to be linked to an ADSL Modem and then the Internet via an Ethernet interface, it is necessary to configure the PPPoE session on the Ethernet interface.

Configure a virtual Ethernet interface in system view and PPPoEoA mapping in ADSL view.

Table 2-5 Configure a virtual Ethernet interface

Operation	Command
Create a virtual Ethernet interface	**interface virtual-ethernet** *number*
Delete the virtual Ethernet interface	**undo interface virtual-ethernet** *number*
Create a PPPoEoA map on a PVC	**map bridge virtual-ethernet** *interface-num*

Perform the following configuration in Ethernet interface (subinterface) view or virtual Ethernet interface view.

Table 2-6 Configure a PPPoE session

Operation	Command
Configure PPPoE session (permanently on-line mode)	**pppoe-client dial-bundle-number** *number* [**no-hostuniq**]
Configure PPPoE session (packet triggered)	**pppoe-client dial-bundle-number** *number* **idle-timeout** *seconds* [**queue-length** *packets*]
Delete PPPoE session	**undo pppoe-client dial-bundle-number** *number*

3Com Series Routers support two kinds of PPPoE connection mode: always-on mode and packet triggering mode.

- Always-on mode: When the physical line is UP, the router will quickly initiate PPPoE call to create a PPPoE session. The PPPoE session will always exist unless the user deletes it via the **undo pppoe-client** command.
- Packet triggering mode: When the physical line is UP, the router will not immediately initiate PPPoE call. Only when there is data transmission requirement will the router initiate PPPoE call to create a PPPoE session. If the free time of a PPPoE link exceeds the value set by user, the router will automatically terminate the PPPoE session.

2.3.3 Enabling/Disabling the PPPoE Server to Output PPP-Related Log

To avoid decreased device performance due to excessive log output, you can disable the PPPoE server to output log information.

Perform the following configuration in system view.

Table 2-7 Disable/enable the PPPoE server to output PPP-related log information

Operation	Command
Disable the PPPoE server to output PPP-related log information	**pppoe-server log-information off**

Operation	Command
Enable the PPPoE server to output PPP-related log information	**undo pppoe-server log-information off**

By default, the PPPoE server output the PPP-related information.

2.3.4 Resetting/Deleting a PPPoE Session

Execute the **reset pppoe-client** command and the **reset pppoe-server** command in user view and the **undo pppoe-client** command in Ethernet interface view or virtual Ethernet interface view.

Table 2-8 Reset/delete a PPPoE session

Operation	Command
Terminate a PPPoE session at the client end and recreate the session later	**reset pppoe-client** { **all** | **dial-bundle-number** *number* }
Terminate a session at the PPPoE server end	**reset pppoe-server** { **all** | **virtual-template** *number* **| interface** *interface-type interface-num* }
Terminate a PPPoE session at the client end and never recreate it again	**undo pppoe-client dial-bundle-number** *number*

The difference between the **reset pppoe-client** command and the **undo pppoe-client** command lies in: The former only temporarily terminates a PPPoE session, while the latter permanently deletes a PPPoE session.

When a PPPoE session works in permanent on-line mode, if it is terminated by the **reset pppoe-client** command, the router will automatically recreate a PPPoE session in 16 seconds. When a PPPoE session works in packet triggering mode, if it is terminated via the **reset pppoe-client** command, the router will recreate a PPPoE session only upon data transmission.

No matter a PPPoE session works in permanent on-line mode or in packet triggering mode, it will be deleted permanently by the **undo pppoe-client** command. If it is necessary to recreate a PPPoE session, the user must reconfigure it.

2.4 Displaying and Debugging PPPoE

After finishing the above configuration, execute the **display** commands in any view to view the running state of PPPoE for verifying the effect of the configuration.

Execute the **debugging** command in user view.

Table 2-9 Display and debug PPPoE

Operation	Command
Display statistics and state information about PPPoE server sessions.	**display pppoe-server session** { **all** | **packet** }
Display statistics and state information about PPPoE client sessions.	**display pppoe-client session** { **summary** | **packet** } [**dial-bundle-number** *number*]
Enable PPPoE client debugging.	**debugging pppoe-client** *option* [**interface** *type number*]

2.5 PPPoE Configuration Example

2.5.1 Configuring PPPoE Server

I. Network requirements

In Figure 2-2, the hosts access the Internet through the router 3Com by making use of PPPoE.

II. Network diagram

Router 3Com is connected to the Ethernet through the interface Ethernet 1/0/0 and the Internet through Serial3/0/0.

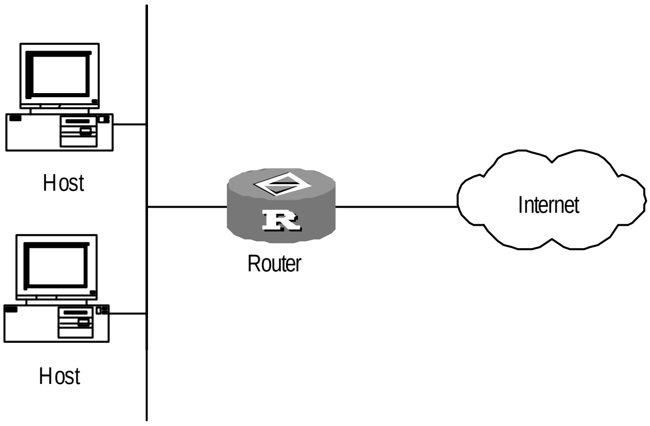


Figure 2-2 PPPoE network diagram

III. Configuration procedure

# Add a PPPoE user

```
[router] local-user NE
[router-luser-NE] password simple 3Com
[router-luser-NE] service-type ppp
[router-luser-NE] quit
```

# Configure PPPoE parameters on 3Com:

```
[router] interface ethernet 1/0/0
[router-Ethernet1/0/0] pppoe-server bind virtual-template 1
```

# Configure virtual-template parameters on 3Com:

```
[router-Ethernet1/0/0] interface virtual-template 1
[router-Virtual-Template1] ppp authentication-mode chap domain system
[router-Virtual-Template1] ppp chap user 3Com
[router-Virtual-Template1] remote address pool 1
[router-Virtual-Template1] ip address 1.1.1.1 255.0.0.0
[router-Virtual-Template1] quit
```

# Configure the users in the domain to use the local authentication scheme.

```
[3Com] domain system
[3Com-isp-domain] scheme local
```

# Add a local IP address pool containing nine IP addresses.

```
[router-isp-domain] ip pool 1 1.1.1.2 1.1.1.10
```

When installed with PPPoE client software and configured with user name and password (herein as NE and 3Com respectively), every host on the Ethernet can access the Internet through the router 3Com with PPPoE.

If **radius-scheme** or **hwtacacs-scheme** is configured for authentication, the 3Com router may also be configured with RADIUS/HWTACACS parameters, thus enabling the system to charge. For detailed configuration procedures, please refer to the Chapter "Security Configuration".

2.5.2 Configuring PPPoE Client

I. Network requirements

3Com 1 and 3Com 2 are connected using interface Ethernet 1/0/0. 3Com 1 authenticates 3Com 2 using PAP or CHAP.

II. Network diagram

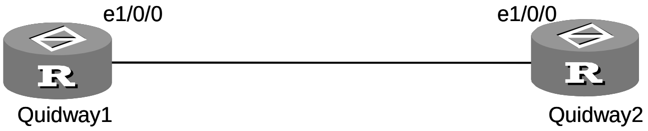


Figure 2-3 Network diagram for PPPoE client

III. Configuration procedure

When PAP authentication applies, configure the routers as follows:

1) Configure 3Com 1

# Add a PPPoE user.

```
[3Com] local-user 3Com2
[3Com-luser-3Com2] password simple 3Com
[3Com-luser-3Com2] service-type ppp
[3Com-luser-3Com2] quit
```

# Configure the parameters of the virtual template.

```
[3Com] interface virtual-template 1
[3Com-Virtual-Template1] ppp authentication-mode pap
[3Com-Virtual-Template1] ip address 1.1.1.1 255.0.0.0
[3Com-Virtual-Template1] remote address 1.1.1.2
[3Com-Virtual-Template1] quit
```

# Configure PPPoE Server.

```
[3Com] interface ethernet 1/0/0
[3Com-Ethernet1/0/0] pppoe-server bind virtual-template 1
```

2) Configure 3Com 2

```
[3Com] dialer-rule 1 ip permit
[3Com] interface dialer 1
[3Com-Dialer1] dialer user 3Com2
[3Com-Dialer1] dialer-group 1
[3Com-Dialer1] dialer bundle 1
[3Com-Dialer1] ip address ppp-negotiate
[3Com-Dialer1] ppp pap local-user 3Com2 password simple 3Com
[3Com-Dialer1] quit
```

# Configure a PPPoE session.

```
[3Com] interface ethernet 1/0/0
[3Com-Ethernet1/0/0] pppoe-client dial-bundle-number 1
```

When CHAP authentication applies, configure the routers as follows:

1) Configure 3Com 1

# Add a PPPoE user.

```
[3Com] local-user 3Com2
[3Com-luser-3Com2] password simple 3Com
[3Com-luser-3Com2] service-type ppp
[3Com-luser-3Com2] quit
```

# Configure the parameters of the virtual template.

```
[3Com] interface virtual-template 1
[3Com-Virtual-Template1] ppp authentication-mode chap
[3Com-Virtual-Template1] ppp chap user 3Com1
[3Com-Virtual-Template1] ip address 1.1.1.1 255.0.0.0
```

```
[3Com-Virtual-Template1] remote address 1.1.1.2
[3Com-Virtual-Template1] quit
```

# Configure PPPoE Server.

```
[3Com] interface ethernet 1/0/0
[3Com-Ethernet1/0/0] pppoe-server bind virtual-template 1
```

2) Configure 3Com 2

```
[3Com] dialer-rule 1 ip permit
[3Com] interface dialer 1
[3Com-Dialer1] dialer user 3Com2
[3Com-Dialer1] dialer-group 1
[3Com-Dialer1] dialer bundle 1
[3Com-Dialer1] ip address ppp-negotiate
[3Com-Dialer1] ppp chap user 3Com2
[3Com-Dialer1] ppp chap password simple 3Com
[3Com-Dialer1] quit
[3Com] local-user 3Com1
[3Com-luser-3Com1] password simple 3Com
[3Com-luser-3Com1] quit
```

# Configure a PPPoE session.

```
[3Com] interface ethernet 1/0/0
[3Com-Ethernet1/0/0] pppoe-client dial-bundle-number 1
```

2.5.3 Connecting a LAN to the Internet via ADSL Modem

I. Network requirements

PCs on a LAN access the Internet through Router A, which is connected in permanent on-line mode to the DSLAM through an ADSL modem. The username and password of the ADSL account are huawei and 123456 respectively. Enable the PPPoE client function on the router, allowing the hosts on the LAN to access the Internet without PPPoE client software.

Router B is operating as PPPoE Server. It is connected to the DSLAM through interface 25M atm2/0/0, providing RADIUS authentication and accounting.

II. Network diagram

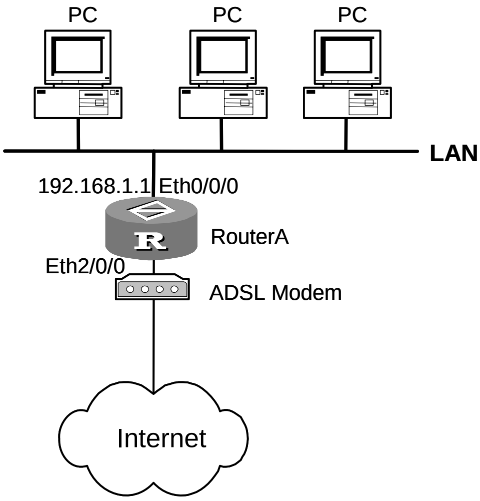


Figure 2-4 Connect a LAN to the Internet through ADSL

III. Configuration procedure

1) Configure Router A

# Configure the dialer interface.

```
[3Com] dialer-rule 1 ip permit
[3Com] interface dialer 1
[3Com-Dialer1] dialer user huawei
[3Com-Dialer1] dialer-group 1
[3Com-Dialer1] dialer bundle 1
[3Com-Dialer1] ip address ppp-negotiate
[3Com-Dialer1] ppp pap local-user huawei password cipher 123456
[3Com-Dialer1] quit
```

# Configure a PPPoE session.

```
[3Com] interface ethernet 2/0/0
[3Com-Ethernet2/0/0] pppoe-client dial-bundle-number 1
```

# Configure a LAN interface and the default route.

```
[3Com-Ethernet2/0/0] interface ethernet 0/0/0
[3Com-Ethernet0/0/0] ip address 192.168.1.1 255.255.255.0
[3Com-Ethernet0/0/0] quit
[3Com] ip route-static 0.0.0.0 0 dialer 1
```

If the IP addresses of the PCs in the LAN are private addresses, it is necessary to configure NAT (Network Address Translation) on the router. The NAT configuration will not be elaborated here. For details, refer to the chapter discussing NAT configuration in the “Network Protocol” part of *V 2.41 Operation Manual*.

2) Configure Router B

# Configure the ATM interface.

```
[RouterA] interface atm2/0/0
[RouterA-Atm1/0/0] pvc 0/32
[RouterA-atm-pvc-Atm1/0/0-0/32] map bridge virtual-ethernet 1
[RouterA-atm-pvc-Atm1/0/0-0/32] quit
```

# Enable PPPoE Server on the VE interface.

```
[RouterA-Atm1/0/0] interface virtual-ethernet 1
[RouterA-Virtual-Ethernet1] pppoe-server bind virtual-template 1
[RouterA-Virtual-Ethernet1] mac-address 0022-0022-00c1
```

# Configure the parameters of the virtual template.

```
[router-Virtual-Ethernet1/0/0] interface virtual-template 1
[router-Virtual-Template1] ppp authentication-mode pap domain system
[router-Virtual-Template1] remote address pool 1
[router-Virtual-Template1] ip address 1.1.1.1 255.0.0.0
[router-Virtual-Template1] quit
```

# Apply RADIUS authentication to the domain users.

```
[router] domain system
[router -isp-domain] scheme radius-scheme cams
```

# Add a local IP address pool that contains nine IP addresses.

```
[router -isp-domain]  ip pool 1 1.1.1.2 1.1.1.10
[router -isp-domain] quit
```

# Configure a RADIUS scheme.

```
[3Com] radius scheme cams
[3Com-radius-cams] primary authentication 10.110.91.146 1812
[3Com-radius-cams] primary accounting 10.110.91.146 1813
[3Com-radius-cams] key authentication expert
[3Com-radius-cams] key accounting expert
[3Com-radius-cams] server-type Huawei
[3Com-radius-cams] user-name-format with-domain
[3Com-radius-cams] quit
```

For more information on the configurations of RADIUS Server, refer to the documentation of the RADIUS Server software.

2.5.4 Using ADSL for Line Backup

I. Network requirements

RouterA is connected to the network center via a DDN dedicated line and an ADSL, among which the ADSL is the backup of the DDN dedicated line. When the DDN dedicated line is in failure, RouterA can still initiate a PPPoE call and access the network center via the ADSL. If there is no packet transmission on ADSL for 2 minutes, the PPPoE session will terminate automatically. Later on, if there are new packets that need forwarding, the PPPoE session will be recreated.

II. Network diagram

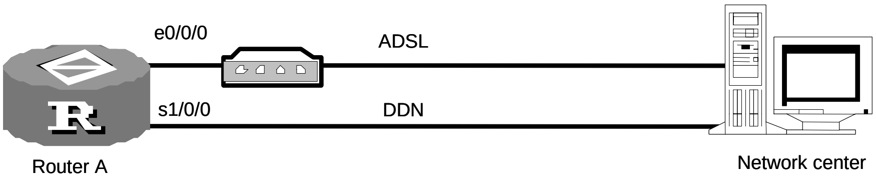


Figure 2-5 Network diagram for PPPoE

III. Configuration procedure

Configure Router A:

# Configure a dialer interface.

```
[3Com] dialer-rule 1 ip permit
[3Com] interface dialer 1
[3Com-Dialer1] dialer user 3Com
[3Com-Dialer1] dialer-group 1
[3Com-Dialer1] dialer bundle 1
[3Com-Dialer1] ip address ppp-negotiate
```

# Configure a PPPoE session.

```
[3Com-Dialer1] interface ethernet 0/0/0
[3Com-Ethernet0/0/0] pppoe-client dial-bundle-number 1 idle-timeout 120
```

# Configure the DDN interface Serial 1/0/0.

```
[3Com-Ethernet0/0/0] interface serial 0/0/0
[3Com-Serial1/0/0] ip address 10.1.1.1 255.255.255.0
[3Com-Serial1/0/0] standby interface dialer 1
[3Com-Serial1/0/0] quit
```

# Configure the static route to the peer.

```
[3Com] ip route 0.0.0.0 0 serial 0/0/0 preference 60
[3Com] ip route 0.0.0.0 0 dialer 1 preference 70
```

2.5.5 Accessing the Internet through an ADSL Interface

I. Network requirements

Router A has an ADSL interface, through which it can access the Internet directly rather than via an ADSL modem.

II. Network diagram

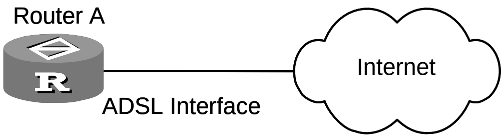


Figure 2-6 Accessing the Internet through an ADSL interface

III. Configuration procedure

# Configure a dialer interface

```
[3Com]dialer-rule 1 ip permit
[3Com]interface dialer 1
[3Com-Dialer1]dialer user mypppoe
[3Com-Dialer1]dialer-group 1
[3Com-Dialer1]dialer bundle 1
[3Com-Dialer1]ip address ppp-negotiate
```

# Configure a VE interface

```
[3Com]interface virtual-ethernet 1
[3Com-Virtual-Ethernet1] mac 0001-0002-0003
[3Com-Virtual-Ethernet1] quit
[3Com] interface atm 1/2/0.1
[3Com-atm1/2/0.1] pvc to_adsl_a 0/60
[3Com-atm-pvc-atm1/2/0.1-0/60-to_adsl_a] map bridge virtual-ethernet 1
```

# Configure a PPPoE session.

```
[3Com]interface virtual-ethernet 1
[3Com-Virtual-Ethernet1] pppoe-client dial-bundle-number 1 idle-timeout 120
```

# Configure a default route.

```
[3Com] ip route-static 0.0.0.0 0.0.0.0 dialer 1
```

Chapter 3 Bridge Configuration

3.1 Introduction to Bridge

Bridge is a type of network device on the data link layer, which interconnects Local Area Networks (LANs) and transfers data between them. In some small-sized networks, especially those widely dispersed networks, the employment of bridges can reduce the network maintenance cost, and the network terminal users do not need to make special settings for the devices, since the bridges interconnect networks just like hubs.

In practice, there are four types of bridging:

- Transparent Bridging: Such bridging is used to interconnect LANs of the same medium. It is mainly applied in the Ethernet environment. Usually, transparent bridging keeps a bridging table that records the correlation between destination MAC addresses and interfaces.
- Source-route Bridging: Such bridging forwards frames based on the routing indicators contained in the frames. The table of correlation between destination MAC addresses and routing indicators will be determined and maintained by the end stations (the starting and the ending point). This bridging is found primarily in the Token Ring environments.
- Translational Bridging: Such bridging is used to interconnect LANs of different physical media. It is typically applied to interconnect different types of networks, such as Ethernet, Fiber Distributed Data Interface (FDDI) and Token Ring.
- Source-route Translational Bridging: As the name implies, such bridging is the hybrid of “Source-route Bridging” and “Translational Bridging”. They allow of the communication between devices in mixed Toke Ring and Ethernet environments.

The router supports transparent bridging function, supporting:

- Bridging on PPP and HDLC links
- Bridging on X.25 links
- Bridging on ATM
- Bridging on VLAN sub-interfaces
- Bridging on dial interface
- Both routing and bridging
- Command configuration and management
- Logging, trapping and debugging

3.1.1 Main Functions of Bridging

The following covers the overall functions of bridging.

I. Obtaining address table

A bridge makes forwarding decision based on the bridging table, which consists of MAC addresses and interfaces. It should obtain the associations between MAC addresses and interfaces. When the bridge connects with a physical network segment, it will detect all the Ethernet frames on this segment. Once the Ethernet frame sent from a node on an interface is detected, the source MAC address of this frame will be picked up and the correlation between this MAC address and the interface receiving this frame will be added to the bridging address table.

As shown in the following figure, four workstations A, B, C and D are distributed in two LANs: Ethernet segment 1 connected with Bridge port 1 and Ethernet segment 2 connected with Bridge port 2. At a certain moment, when Workstation A transmits an Ethernet frame to Workstation B, both the bridge and Workstation B will receive this frame.

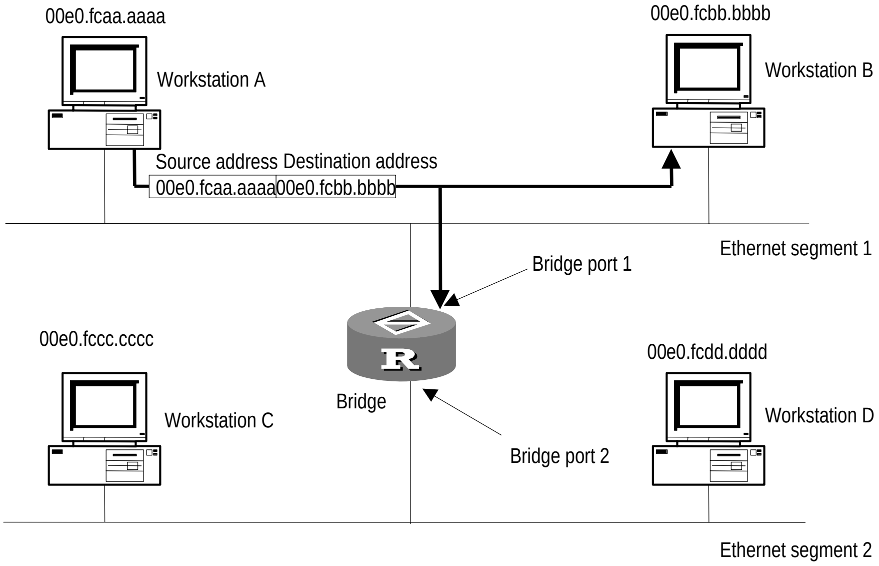
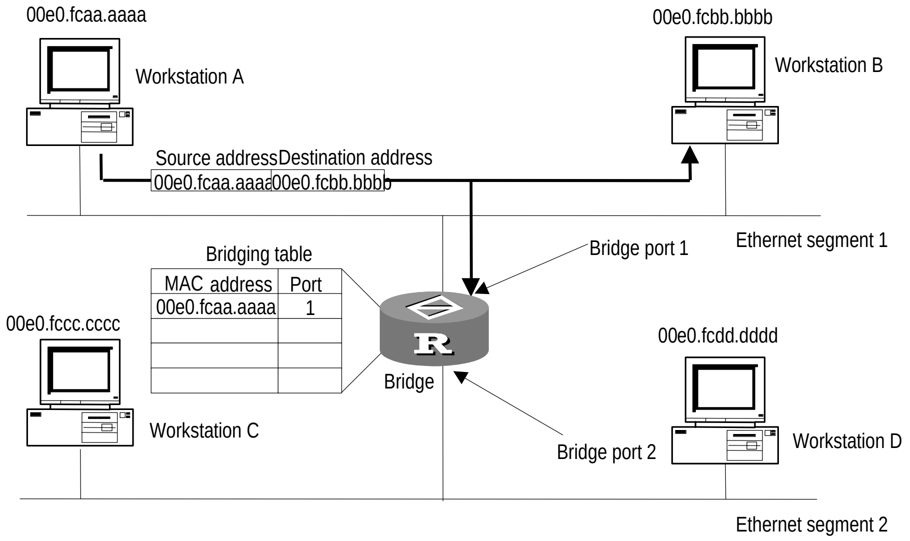


Figure 3-1 Workstation A transmits information to workstation B on the Ethernet segment 1

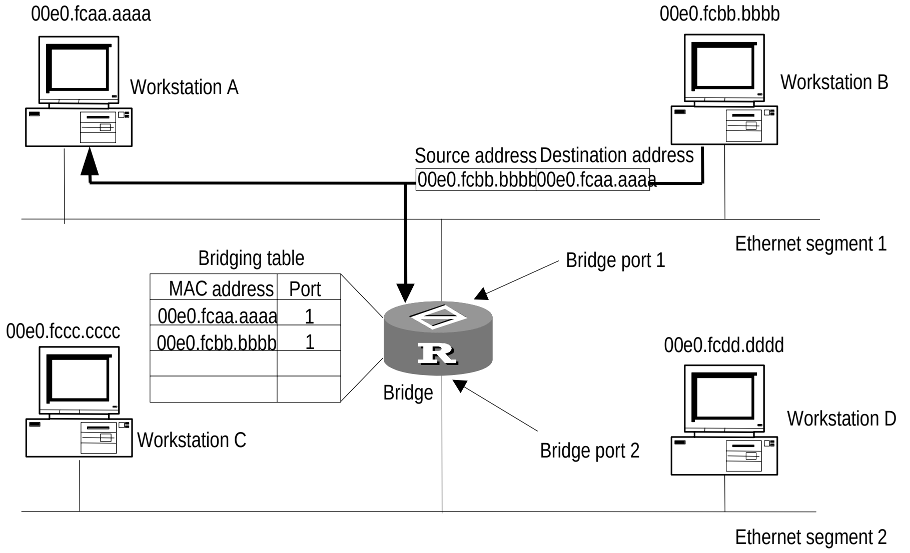
Upon receiving the Ethernet frame, the bridge learns that Workstation A is connected with Bridge port 1 since the frame is received from Port 1. As a result, the correlation between the MAC address of Workstation A and Bridge port 1 will be added to the bridging table, as shown in the following figure:



MAC address	Port
00e0.fcaa.aaaa	1

Figure 3-2 Bridge learns that Workstation A is connected with Port 1

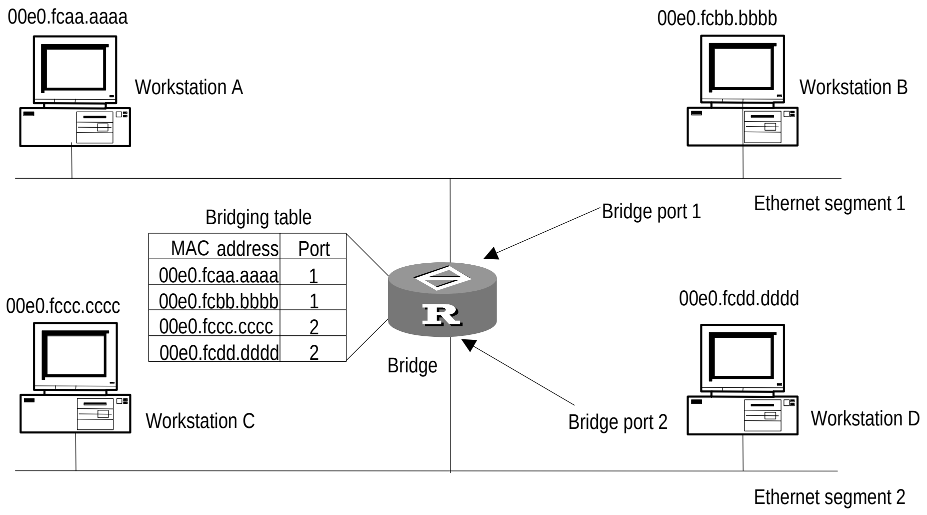
Once Workstation B responds to Workstation A, the bridge can detect the responding Ethernet frame from Workstation B and learn that Workstation B is also connected to Bridge port 1 because the frame is detected on port 1 too. As a result, the correlation between the MAC address of Workstation B and Bridge port 1 is added to the bridging table too, as shown in the following figure:



MAC address	Port
00e0.fcaa.aaaa	1
00e0.fcbb.bbbb	1

Figure 3-3 Bridge learns that Workstation B is connected with the port 1 too

At last, given that all the workstations are in use, the bridge will obtain all correlation between the MAC addresses and the bridge ports as shown in the following figure:



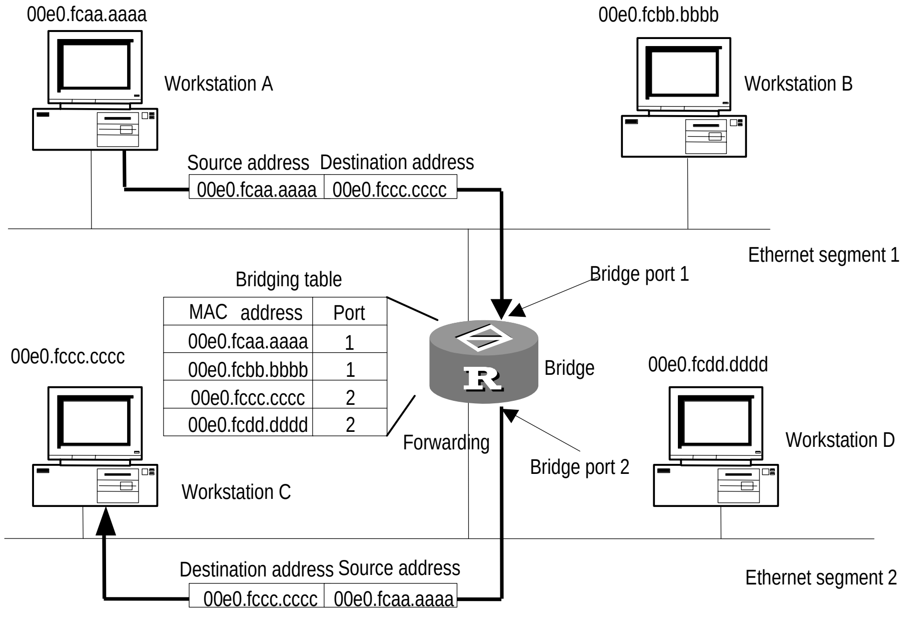
MAC address	Port
00e0.fcaa.aaaa	1
00e0.fcbb.bbbb	1
00e0.fccc.cccc	2
00e0.fcdd.dddd	2

Figure 3-4 Final bridging address table

II. Forward and Filter

The bridge will make the decision to forward frames or not (that is, to filter frames) depending on the following three conditions:

- If Workstation A sends an Ethernet frame whose destination is Workstation C, the bridge will detect this frame and learn that Workstation C corresponds to Bridge port 2 by looking up its bridging table. So, it will forward the frame to Bridge port 2, as shown in the following figure.

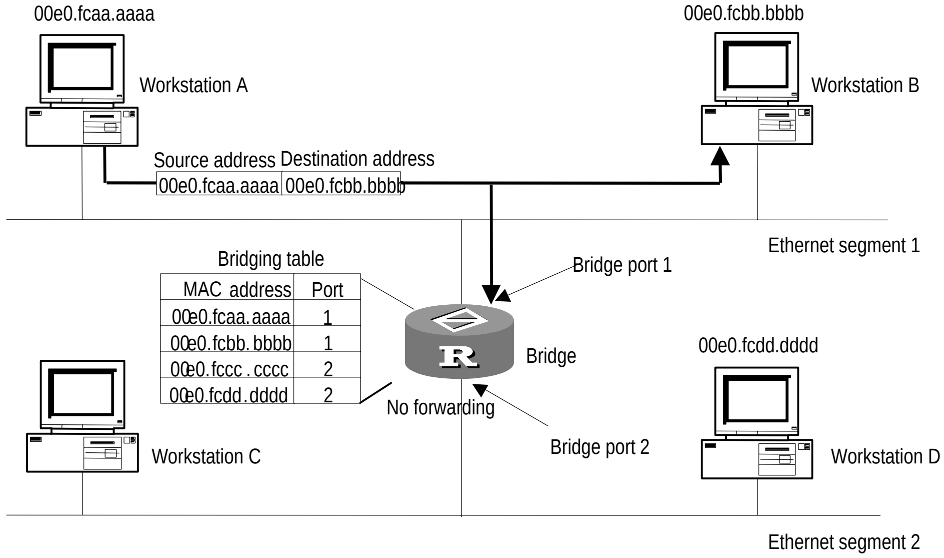


MAC address	Port
00e0.fcaa.aaaa	1
00e0.fcbb.bbbb	1
00e0.fccc.cccc	2
00e0.fcdd.dddd	2

Figure 3-5 Forward

Please be aware that the bridge will forward the broadcast or multicast frames received on one port to the other ports.

- Given that Workstation A sends an Ethernet frame to Workstation B, the bridge will filter this frame rather than forwarding it, for Workstation B and Workstation A are located on the same physical network segment.



Bridging table

MAC address	Port
00e0.fcaa.aaaa	1
00e0.fcbb.bbbb	1
00e0.fccc.cccc	2
00e0.fcdd.dddd	2

Figure 3-6 Filter(not forward)

- Suppose that Workstation A sends an Ethernet frame to Workstation C, and the bridge does not find the correlation between the MAC address of Workstation C and the port in the bridging address table, what will the bridge do? The bridge will forward this frame destined to an unknown MAC address to all ports except the one on which it is received. In this case, the bridge actually plays the role of a hub to make sure the continuous information transmission, as shown in the following figure:

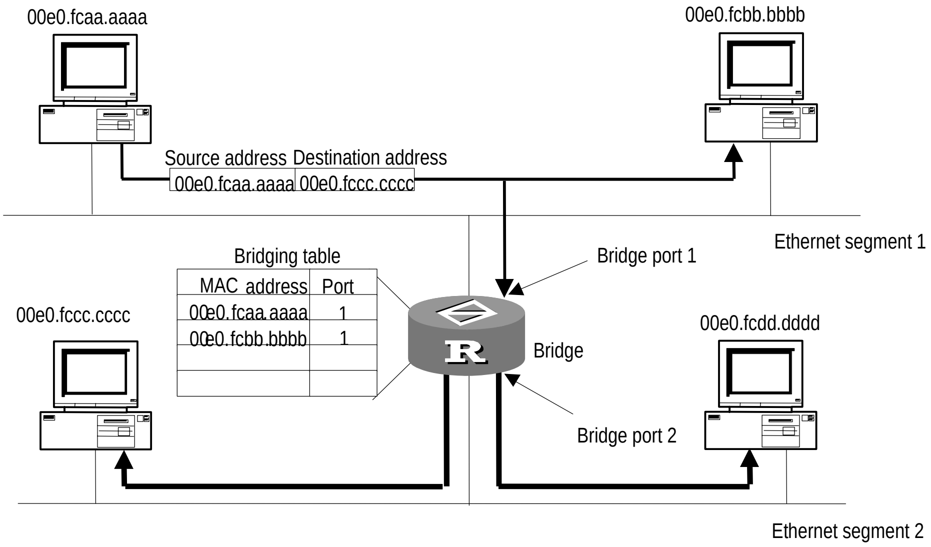


Figure 3-7 No matched MAC address is found in the bridging table

III. Eliminating loop

As shown in the following figure, both bridge X and bridge Y are connected with Ethernet segment 1. Once detecting a broadcasting frame, both bridges will send it to all ports except the source port on which the frame is detected. That is, both bridge X and bridge Y will forward this broadcast frame.

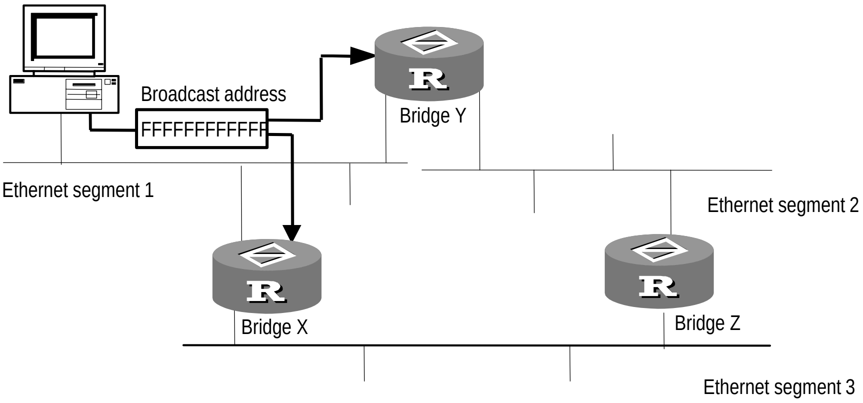


Figure 3-8 Preliminary examination state of bridging loops

As shown in the following figure, the broadcast frame is forwarded over Ethernet segment 2 and Ethernet segment 3 that are connected with Bridge Z. Upon detecting two copies of this frame on two different ports, Bridge Z forwards them to Ethernet segment 3 and Ethernet segment 2 again. Thus, Ethernet segment 2 and Ethernet segment 3 receive a copy of this frame for the second time. In this way, the frame is repeatedly forwarded over the network, which is called bridging loop. See the figure below.

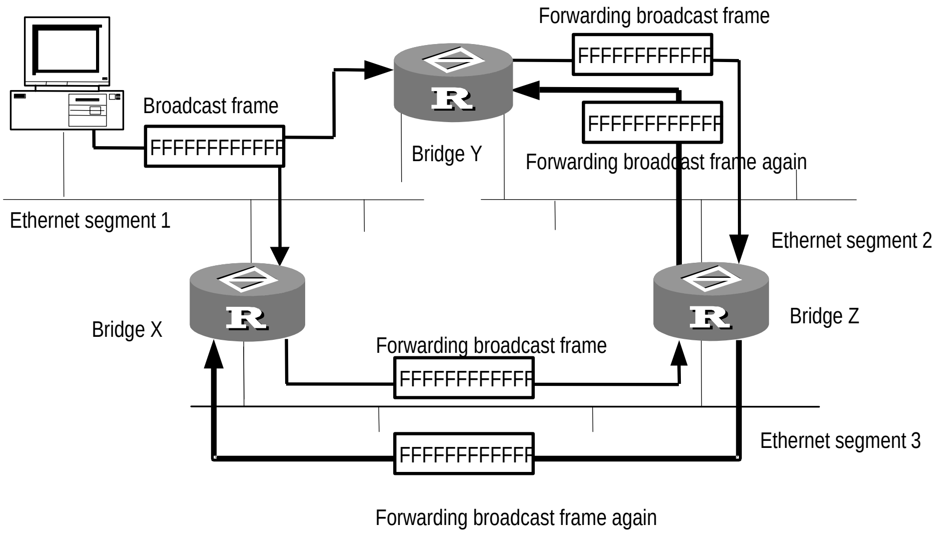


Figure 3-9 Bridging loop

In practice, if there are hundreds of physical segments, bridging loops will cause a sharp decline to the network performance. After the location where loops occur is detected, the only solution is to cut off all connections. It is obvious that eliminating loops is an essential requirement for ensuring the bridge working normally. Therefore, the third function of bridge is to locate loops and block redundant ports.

3.1.2 Spanning Tree Protocol

Spanning Tree Protocol (STP) is used to prevent redundant paths through certain algorithms. A loop network is thus pruned to be a loop-free tree network so as to avoid the infinite cycling of data frames in the loop network. Currently, the bridge module does not support STP, so the following text will only simply introduces some aspects about STP.

STP transmits a kind of special data frame called Bridge Protocol Data Unit (BPDU) between bridges. The overall network will compute a minimum spanning tree describing the distribution of bridges in the network. This minimum spanning tree will also specify which bridge to be the “root bridge” and which bridges to be the “leaf nodes”.

A BPDU contains the following information:

- Root Identifier: Consists of the Root Bridge Priority and the MAC address of the root bridge.
- Root Path Cost: Path cost from the individual leaf nodes to the root bridge.
- Bridge Identifier: Consists of the Bridge priority and the MAC address of the current bridge.
- Port Identifier: Consists of the Port Priority and the Port Number.
- Message Age of BPDU

- Max Age of BPDU
- Hello Time of BPDU
- Forward Delay of port state transition

I. Spanning tree protocol algorithm

The spanning tree protocol algorithm contains enough information for a bridge to perform the following tasks:

Specify the root bridge. The bridge with the smallest Bridge Identifier will be the root bridge of the local network.

Specify the designated bridge. Designated bridge is the one directly connected with the current (subordinate) bridge and responsible for forwarding data to the current (subordinate) bridge. The path cost via a designated bridge is the lowest between the leaf nodes and root bridge.

Specify the designated port. Designated ports are those on the designated bridge and responsible for forwarding data to the subordinate bridges. The path cost of BPDUs sent on a designated port will be the lowest.

Specify the root port. Root port refers to the one on the current bridge and responsible for receiving the data forwarded by the designated bridge.

Specify blocked ports. Except the designated ports and the root ports, all other ports will be blocked and are called blocked ports.

Upon the computation of the minimum spanning tree, the newly generated root port and designated ports begin to forward packets after a period of forward delay. After all the bridges on the network accomplish the spanning tree computation, the network topology will be stabilized and will remain the same until the network takes changes.

The following figure illustrates the topology of the minimum spanning tree on a network:

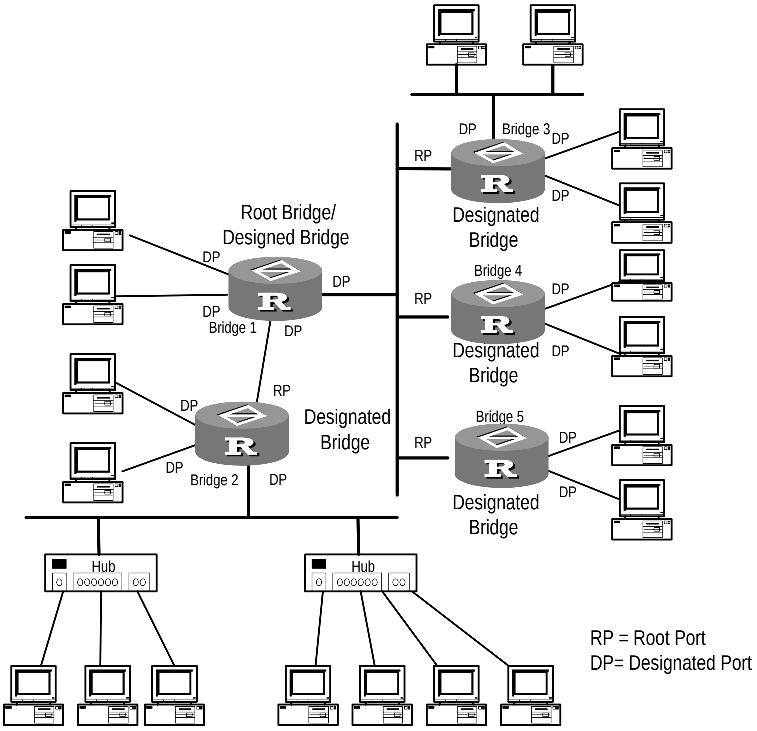


Figure 3-10 Spanning tree topology

II. BPDU forwarding mechanism

Upon the initiation of STP, all the bridges assume themselves as the root bridge. The designated interface of the bridge regularly sends its BPDU once each Hello Time. If it is the root port that receives the BPDU, it will increase the Message Age carried in the BPDU and enable the timer to time this BPDU. If a path fails, the root port on this path will not receive new BPDUs any more and old BPDUs will be discarded due to timeout, which will result in the spanning tree recompilation. A new path will thus be generated to replace the failed one.

However, the recomputed new BPDU will not be propagated throughout the network right away, so the old root port and designated ports that have not detected the topology changes will still forward the data through the old path. If the newly elected root port and designated ports begin to forward data immediately, a temporary loop may be introduced. In STP, a transitional state mechanism is thus adopted. Specifically, the root port and the designated ports will undergo a transitional state for an interval of forwarding delay to enter the forwarding state to resume the data forwarding. Such a delay ensures that the new BPDU has already been propagated throughout the network before the data frames are forwarded according to the latest topology.

3.1.3 Multi-Protocol Router

Generally, a router is called multi-protocol router when it can implement the routed protocols like IP and IPX, as well as the bridging protocol. For a multi-protocol router, the bridging protocol can be either enabled or disabled. However, if both the routing protocols such as IP and IPX at netwokr layer and the bridging protocols at MAC layer are enabled on a router, the router will be taken as a multi-protocol router. In this case, whether a packet should be routed through IP or IPX or forwarded via the bridge will depend on the protocol type of the packet. For example, bridging protocol and IP are concurrently enabled on a router. If the packet to be processed is an IP packet, it will be routed through IP. Certainly, if IP cannot find a route, it will discard the packet instead of forwarding it to the bridge for processing. If the packet uses a protocol other than IP (for example, if it is the packet from the network like AppleTalk or DecNet), it will be bridged.

3.2 Configuring the Bridging Functions

The bridge configuration tasks are described in the following sections:

1) Basic Bridge Configuration

- Enabling/disabling bridging
- Enabling/disabling a bridge-set
- Adding interfaces to a bridge-set

2) Configuring Bridging over Link Layer Protocols

- Configuring bridging on VLAN
- Configuring bridging on PPP
- Configuring bridging on MP
- Configuring bridging on HDLC
- Configuring bridging on X.25
- Configuring bridging on frame relay
- Configuring bridging on ATM

3) Configuring the Bridging Address Table

- Configuring static address entries
- Enabling/disabling forwarding by using dynamic address table
- Configuring the aging timer of the dynamic address table

4) Configuring the Bridge to Support STP

- Disabling/enabling STP on ports
- Specifying the STP version supported by a bridge-set
- Assigning a priority to the bridge (optional)
- Assigning a path cost to a bridge port (Optional)
- Assigning a priority to a bridge port (optional)
- Setting the Hello Time timer (optional)
- Setting the Forward Delay timer (optional)
- Setting the Max Age timer (optional)

5) Creating and Applying Bridging ACLs

- Create a bridging ACL
- Creating a bridging ACL
- Applying the ACL on an interface

6) Configuring the Routing Function of the Bridge

- Enabling the routing function of the bridge
- Configuring a bridge-template interface
- Configuring a bridge-set to route or bridge for the network layer protocol

3.2.1 Basic Bridge Configuration

I. Enabling/disabling bridging

Perform the following configuration in system view.

Table 3-1 Enable/disable bridging

Operation	Command
Enable bridging	**bridge enable**
Disable bridging	**undo bridge enable**

By default, bridging is disabled.

II. Enabling/disabling a bridge-set

As bridge-sets are independent, packets cannot be transmitted between ports that belong to different bridge-sets. A packet that is received on a bridging port can only be sent out another port in the same bridge-set. The interfaces on the router can join only one bridge-set.

Perform the following configuration in system view.

Table 3-2 Enable/disable a bridge-set

Operation	Command
Enable a specified bridge-set.	**bridge** *bridge-set* **enable**
Disable a specified bridge-set.	**undo bridge** *bridge-set* **enable**

III. Adding interfaces to a bridge-set

In addition to Ethernet interfaces (including subinterfaces), PPP/MP, HDLC, X.25, FR, ATM, and dial (such as dialer and ISDN BRI/PRI) interfaces can be assigned to bridge-sets. Refer to the following section for more information.

One interface on the router cannot be added to more than one bridge set.

Perform the following configuration in interface view.

Table 3-3 Add the port to a bridge-set

Operation	Command
Add the port to a bridge-set	**bridge-set** *bridge-set*
Remove the port from the bridge-set	**undo bridge-set** *bridge-set*

By default, the port is not added to any bridge-set.

3.2.2 Configuring Bridging over Link Layer Protocols

I. Configuring bridging on VLAN

When setting up a bridge, you only need to add the bridging function to the subinterfaces after you configure a VLAN.

Perform the following configuration in VLAN sub-interface view.

Table 3-4 Configure bridging on VLAN

Operation	Command
Apply a bridge-set on the VLAN subinterface.	**bridge-set** *bridge-set*

II. Configuring bridging on PPP

Perform the following configuration in interface view.

Table 3-5 Configure bridging on PPP

Operation	Command
Apply a bridge-set on the PPP interface.	**bridge-set** *bridge-set*

III. Configuring bridging on MP

Perform the following configuration in virtual template interface view or MP-group interface view.

Table 3-6 Configure bridging on MP

Operation	Command
Apply a bridge-set on MP	**bridge-set** *bridge-set*

IV. Configuring bridging on HDLC

Perform the following configuration in interface view.

Table 3-7 Configure bridging on HDLC

Operation	Command
Apply a bridge-set on the HDLC interface.	**bridge-set** *bridge-set*

V. Configuring bridging on X.25

In setting up a bridge, you need to map the bridge address to the X.121 address of X.25.

Perform the following configuration in X.25 interface view.

Table 3-8 Configure a bridge address to X.121 map entry

Operation	Command
Apply a bridge-set on the X.25 interface.	**bridge-set** *bridge-set*
Configure a bridge-set to X.25 map entry.	**x25 map bridge x121-address** *x.121-address* **broadcast**
Delete a map entry.	**undo x25 map bridge x121-address** *x.121-address*

VI. Configuring bridging on frame relay

In setting up a bridge, you need to map the bridge address to DLCI.

Perform the following configuration in frame relay interface view.

Table 3-9 Configure a bridge address to DLCI map entry

Operation	Command
Apply a bridge-set on the frame relay interface.	**bridge-set** *bridge-set*
Configure a bridge-set to frame relay map entry.	**fr map bridge** *dlci* **broadcast**
Delete a map entry.	**undo fr map bridge** *dlci*

VII. Configuring bridging on ATM

Bridging on VLAN uses the same spanning tree algorithm adopted by bridging on other protocols. When setting up a bridge, you only need to add the bridging function to the ATM interface after you configure a PVC.

Table 3-10 Configure bridging on ATM

Operation	Command
Assign a bridge-set to an ATM interface (in ATM interface view)	**bridge-set** *bridge-set*
Enable a PVC to transmit and receive BPDUs (in PVC view)	**map bridge-group broadcast**

VIII. Configuring bridging on dial interface

Bridging configuration on dial interface, such as dialer interface, ISDN BRI/PRI interface, is for connection with remote LAN through PSTN/ISDN line.

When configuring bridging on dial interface, note that:

- Configuring dial strings with the **dialer route** command is not allowed.
- STP is not supported.
- The **dialer number** command must be configured for incoming calls.
- The link layer protocol must be set to PPP. MP is not allowed.
- Any network parameter negotiation failure may result in dial link disconnection.

Perform the following configuration in dial interface view.

Table 3-11 Configure bridging on dial interface

Operation	Command
Assign a bridge-set to a dial interface	**bridge-set** *bridge-set*

When configuring bridging on dial interface, configure the **bridge-set** command on the top layer dial interface. For example, when using a dialer interface for dial purpose, the top-layer dial interface is the dialer interface rather than its physical interface. You should therefore configure the bridge-set command on the dialer interface.

3.2.3 Configuring the Bridging Address Table

The bridging address table records the association between destination MAC addresses and the ports for the bridge to make forwarding decision.

I. Configuring static address entries

Normally, a bridging table is dynamically generated according to the correlation between the MAC addresses and the ports obtained by the bridge. However, there are still some static entries in the bridging address table, which are manually configured and maintained by the administrators and will not age forever.

Perform the following configuration in system view.

Table 3-12 Configure a static address entry

Operation	Command
Configure a static address entry	**bridge** *bridge-set* **mac-address** *mac-address* { **permit** | **deny** } [**interface** *interface-type interface-number* | **dlsw**]
Delete a static address entry.	**undo bridge** *bridge-set* **mac-address** *mac-address* [**interface** *interface-type interface-number*]

By default, frames are forwarded according to the dynamic address table.

II. Enabling/disabling forwarding by using dynamic address table

Perform the following configuration in system view.

Table 3-13 Enable/disable forwarding by using dynamic address table

Operation	Command
Enable forwarding using the dynamic address table	**bridge** *bridge-set* **learning**
Disable forwarding using the dynamic address table	**undo bridge** *bridge-set* **learning**

By default, the dynamic address table is used to forward frames.

III. Configuring the aging timer of the dynamic address table

The aging timer of the dynamic address table controls the time to live (TTL) of an entry before it is deleted from the table. The entry is deleted when the timer times out.

Perform the following configuration in system view.

Table 3-14 Configure the aging timer of the dynamic address table

Operation	Command
Configure the aging timer of the dynamic address table.	**bridge aging-time** *seconds*
Restore the default aging timer value.	**undo bridge aging-time**

The aging timer of the dynamic address table is in the range 10 to 1000000 seconds and defaults to 300 seconds.

3.2.4 Configuring the Bridge to Support STP

I. Disabling/enabling STP on ports

To have STP parameters take effect on a bridge port, you must enable STP on it.

Perform the following configuration in interface view.

Table 3-15 Disable/enable STP on the port

Operation	Command
Disable STP on the port	**bridge-set** *bridge-set* **stp disable**
Enable STP on the port	**undo bridge-set** *bridge-set* **stp disable**

By default, STP is enabled on the port.

II. Specifying the STP version supported by a bridge-set

STP has multiple standards, which are not compatible. To prevent bridging loops, the communicating parties must use the same STP standard.

Currently, 3Com Routers only support IEEE STP.

Perform the following configuration in system view.

Table 3-16 Specify the STP version supported by a bridge-set

Operation	Command
Specify the STP version supported by a bridge-set	**bridge** *bridge-set* **stp ieee**
Disable a bridge-set to support STP	**undo bridge** *bridge-set* **stp ieee**

By default, bridge-sets support IEEE STP.

III. Assigning a priority to the bridge (optional)

The ID of a bridge consists of two parts: bridge priority and bridge MAC address. During a spanning tree calculation in a network, the bridge with the lowest ID is elected as the root. The process is as follows:

- Compare the priorities of the bridges in the network. The one with the lowest bridge priority is elected as the root.
- In case multiple bridges in the network have the same priority, compare their MAC addresses and elect the bridge with the lowest MAC address as the root.

When STP is enabled, changing the priority of a bridge may cause spanning tree recalculation.

Perform the following configuration in system view.

Table 3-17 Assign a priority to the bridge

Operation	Command
Assign a priority to the bridge	**bridge stp priority** *value*
Restore the default priority of the bridge	**undo bridge stp priority**

The default priority of the bridge is 32,768.

IV. Assigning a path cost to a bridge port (Optional)

Assign a path cost to a bridge port depending on its link speed. The higher the link speed is, the lower the path cost should be configured.

When a bridge port uses the default path cost, STP can automatically identify the type of the port and get the corresponding default path cost value.

Perform the following configuration in interface view.

Table 3-18 Assign a path cost to a bridge port

Operation	Command
Assign a path cost to a bridge port	**bridge-set** *bridge-set* **stp port pathcost** *cost*
Restore the default path cost of the bridge port	**undo bridge-set** *bridge-set* **stp port pathcost**

For an Ethernet port, the default path cost is 19; for a serial port, the default path cost is 1000.

V. Assigning a priority to a bridge port (optional)

The ID of a bridge port comprises port priority and port number.

When the path costs of all ports on a bridge are the same, the one with the lowest port ID is more likely to be elected as the designated port. The process is as follows:

- Compare the priorities of the ports on the bridge. The one with the lowest port priority is elected as the designated port.
- In case multiple ports on the bridge have the same priority, compare their port numbers and elect the port with the lowest number as the designated port.

Perform the following configuration in interface view.

Table 3-19 Assign a priority to the bridge port

Operation	Command
Assign a priority to the bridge port	**bridge-set** *bridge-set* **stp port priority** *value*

Operation	Command
Restore the default priority of the bridge port	**undo bridge-set** *bridge-set* **stp port priority**

The default priority of the bridge port is 128.

VI. Setting the Hello Time timer (optional)

A Hello Time timer is used to control the interval for sending BPDUs. Enabling STP on a port starts a Hello Time timer. An appropriately set Hello Time timer allows the bridge to discover link faults on the network without occupying many resources.

Perform the following configuration in system view.

Table 3-20 Set the Hello Time timer

Operation	Command
Set the Hello Time timer	**bridge stp timer hello** *seconds*
Restore default setting of the Hello Time timer	**undo bridge stp timer hello**

By default, the time value for a Hello Time timer is 2 seconds.

When configuring a Hello Time timer, consider the following:

- On a spanning tree, all bridges must use the Hello Time timer of the root bridge instead of their own.
- Set the Hello Time timer appropriately. A small Hello time timer may increase the frequency of BPDU sending, increasing undesired CPU load. A large Hello Time timer, on the contrary, may cause the bridge to take a frame loss for a link failure, and then to recalculate the spanning tree. You are recommended to use the default timer setting if possible.

VII. Setting the Forward Delay timer (optional)

A link fault on the network may cause a spanning-tree recalculation immediately; however, it takes time for the new BPDU to propagate throughout the entire network. If new root ports and designated ports start forwarding frames immediately after they are elected, a temporary loop may occur.

To resolve the problem, STP adopts a state transition mechanism, where a root or designated port must undergo a transitional state before it enters the forwarding state to forward frames. The duration of this transitional state depends on the setting of a timer called Forward Delay timer. It ensures that the new BPDU has been propagated throughout the network before frames are forwarded according to the latest topology.

Perform the following configuration in system view.

Table 3-21 Set the Forward Delay timer

Operation	Command
Set the Forward Delay timer	**bridge stp timer forward-delay** *seconds*
Restore the default setting of the Forward Delay timer	**undo bridge stp timer forward-delay**

The default setting of the Forward Delay timer is 15 seconds.

When configuring a Forward Delay timer, consider the following:

- On a spanning tree, all bridges must use the Forward Delay timer of the root bridge instead of their own.
- Use the default Forward Delay timer setting if possible. A small forward delay may create temporary path redundancy; while a large forward delay may increase the time required for the topology of the spanning tree to converge. In the latter case, network connectivity recovery may take a long time.

VIII. Setting the Max Age timer (optional)

A Max Age timer is used to limit the lifetime of BPDUs. Enabling STP on a port starts a Max Age timer. If the interface receives no BPDU before the timer expires, its link is considered faulty and STP starts to recalculate its topology.

Perform the following configuration in system view.

Table 3-22 Set the Max Age timer

Operation	Command
Set the Max Age timer	**bridge stp max-age** *seconds*
Restore default setting of the Max Age timer	**undo bridge stp max-age**

The default setting of the Max Age timer is 20 seconds.

When configuring a Max Age timer, consider the following:

- On a spanning tree, all bridges use the Max Age timer of the root instead of their own.
- Set the timer appropriately. A small timer may result in undesired spanning tree calculation frequency and have the bridge mistake congestions for link failures. A large timer, on the contrary, may decrease the self-tuning capability of the network preventing the bridge from discovering link failures quickly.

You are recommended to use the default Max Age timer setting in normal cases.

3.2.5 Creating and Applying Bridging ACLs

I. Creating a bridging ACL

You can create MAC-based ACLs.

Perform the following configuration in system view (for the command **acl**) and ACL view (for the command **rule**).

Table 3-23 Create a MAC-based ACL

Operation	Command
Create an ACL and enter the ACL view.	**acl number** *acl-number*
Delete one or all ACLs.	**undo acl** { *acl-number* **|** **all** }
Create a MAC-based access control rule.	**rule** [*rule-id*] { **deny** | **permit** } [**type** *type-code type-mask* **|** **lsap** *lsap-code lsap-mask*]] [**source-mac** *sour-addr source-mask*] [**dest-mac** *dest-addr dest-mask*]
Delete a MAC-based access control rule.	**undo rule** *rule-id*

By default, no MAC-based ACL is created.

In creating a MAC-based ACL, *acl-number* takes a value in the range 4000 to 4999. *rule-id* represents a rule number.

type-code is a hexadecimal number in the format of xxxx, used for matching the protocol type of the transmitted packets.

type-mask represents the mask of the protocol type. For type-code values recommended by RFC1700, see Table 3-30 Ethernet type-code values.

lsap-code is a hexadecimal number in the format of xxxx, used for matching the encapsulation format of bridged packet on an interface.

lsap-mask represents the protocol type mask.

sour-addr represents the source MAC address of a data frame in the format of xxxx-xxxx-xxxx. It is used to match the source address of a data frame.

source-mask represents the source MAC address mask.

dest-addr represents the destination MAC address of a packet in the format of xxxx-xxxx-xxxx. It is used to match the destination address of a data frame.

dest-mask represents the destination MAC address mask.

For ACL commands, refer to *V 2.41 Command Manual — Security*.

II. Applying the ACL on an interface

You can apply a MAC-based ACL onto any interface supporting bridging.

Perform the following configuration in interface view.

1) Applying a MAC-based ACL in the inbound/outbound direction of the interface

Perform the following configuration in interface view.

Table 3-24 Apply a MAC-based ACL on an interface

Operation	Command
Apply a MAC-based ACL on the inbound direction of the interface.	**firewall ethernet-frame-filter** *acl-number* **inbound**
Remove the MAC-based ACL applied in the inbound direction of the interface.	**undo firewall ethernet-frame-filter inbound**
Apply a MAC-based ACL on the outbound direction of the interface.	**firewall ethernet-frame-filter** *acl-number* **outbound**
Remove the MAC-based ACL applied in the outbound direction of the interface.	**undo firewall ethernet-frame-filter outbound**

2) Applying a MAC-based ACL to the interface of the DLSw module in the inbound/outbound direction

Perform the following configuration in interface view.

Table 3-25 Apply a MAC-based ACL on an interface

Operation	Command
Apply a MAC-based ACL on the inbound direction of the interface.	**dlsw ethernet-frame-filter** *acl-number* **inbound**
Remove the MAC-based ACL applied in the inbound direction of the interface.	**undo dlsw ethernet-frame-filter inbound**
Apply a MAC-based ACL on the outbound direction of the interface.	**dlsw ethernet-frame-filter** *acl-number* **outbound**
Remove the MAC-based ACL applied in the outbound direction of the interface.	**undo dlsw ethernet-frame-filter outbound**

By default, no ACL is applied on the interface.

When applying an ACL on an interface, consider the following:

- Add the interface into a bridge-set before applying the ACL on the interface.
- When you apply the same type of ACLs on the interface, the last one will overwrite the previous one.

3.2.6 Configuring the Routing Function of the Bridge

I. Enabling the routing function of the bridge

Bridge routing provides forwarding that integrates routing and bridging. For some particular protocol data units (PDUs), if the communication is conducted between bridging ports, they are bridged; if the communication is conducted with a network outside the bridge-set, they are routed. When the integrated bridging and routing function is disabled, all PDUs are bridged. With the function enabled, you can specify to forward the PDUs of a particular protocol by means of bridging or routing and toggle between them through commands.

Perform the following configuration in system view.

Table 3-26 Enable/disable the routing function of the bridge

Operation	Command
Enable the routing function of the bridge	**bridge routing-enable**
Disable the routing function of the bridge	**undo bridge routing-enable**

By default, the routing function of the bridge is disabled.

II. Configuring a bridge-template interface

A bridge-template interface exists on the router. It does not support bridging; but on the router it represents the bridge-set associated to a routing interface and carries the number of the bridge-set. Bridge-template interfaces are virtual routing interfaces on which you can configure network layer attributes. For each bridge-set, you can assign only one bridge-template interface.

Perform the following configuration in system view.

Table 3-27 Configure a bridge-template interface

Operation	Command
Create a bridge-template interface to connect the specified bridge-set to the network of the route	**interface bridge-template** *bridge-set*
Delete a bridge-template interface	**undo interface bridge-template** *bridge-set*

III. Configuring a bridge-set to route or bridge for the network layer protocol

Perform the following configuration in system view.

Table 3-28 Configure a bridge-set to route or bridge for the network layer protocol

Operation	Command
Enable the routing function of a bridge-set for the network layer protocol.	**bridge** *bridge-set* **routing** { **ip | ipx** }
Disable the routing function of a bridge-set for the network layer protocol.	**undo bridge** *bridge-set* **routing** { **ip | ipx** }
Enable the bridging function of a bridge-set for the network layer protocol.	**bridge** *bridge-set* **bridging** { **ip | ipx** }
Disable the bridging function of a bridge-set for the network layer protocol.	**undo bridge** *bridge-set* **bridging** { **ip | ipx** }

By default, bridging is enabled and routing is disabled.

You can view the routing and bridging configurations on each interface with the **display bridge information bridge-template** *bridge-set* command.

3.3 Displaying and Debugging Bridging Information

After you complete the aforesaid configurations, execute **display** command in any view to view the operating state of the bridge and verify effect of the configurations.

Execute the **debugging** command in user view for the debugging of bridge and the **reset** command in user view to clear the related information.

Table 3-29 Display and debug bridges

Operation	Command
Enable bridge-set debugging	**debugging bridge eth-forwarding** [**dlsw** | **interface** *interface-type interface-number*]
Disable bridge-set debugging	**undo debugging bridge eth-forwarding** [**dlsw** | **interface** *interface-type interface-number*]
Display information on one or all the enabled bridge-sets in the bridge module.	**display bridge information** [**bridge-set** *bridge-set*]
Display information on the bridging address table.	**display bridge address-table** [**bridge-set** *bridge-set* | **interface** *interface-type interface-number* | **mac** *mac-address* | **dlsw**] [**static** | **dynamic**]
Display traffic statistics on one or all interfaces in a bridge-set.	**display bridge traffic** [**bridge-set** *bridge-set* | **interface** *interface-type interface-number* | **dlsw**]

Operation	Command
Clear the MAC address forwarding table.	**reset bridge address-table** [**bridge-set** *bridge-set* | **interface** *interface-type interface-number* | **dlsw**]
Reset traffic statistics on one or all interfaces in a bridge-set.	**reset bridge traffic** [**bridge-set** *bridge-set* | **interface** *interface-type interface-number* | **dlsw**]
Clear statistics about ACL-based filtering.	**reset firewall ethernet-frame-filter** { **all** | **dlsw** | **interface** *interface-type interface-number* }

3.4 Transparent Bridging Configuration Examples

3.4.1 Transparent Bridging on PPP

I. Network requirements

There are several PCs located on the Ethernet segment LAN1 of a building's floor and several PCs and servers on the Ethernet segment LAN2 of another floor of the building. Set up transparent bridging between these two LANs.

II. Network diagram

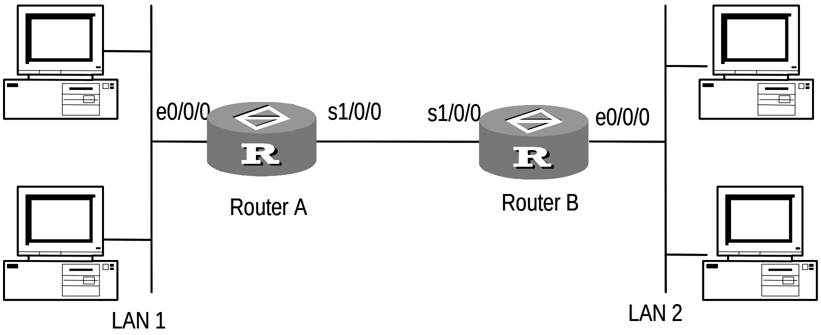


Figure 3-11 Network diagram for setting up transparent bridging between multiple Ethernet segments

III. Configuration procedure

Configure Router A

```
[RouterA] bridge enable
[RouterA] bridge 1 enable
[RouterA] interface ethernet 0/0/0
[RouterA-Ethernet0/0/0] bridge-set 1
[RouterA-Ethernet0/0/0] interface serial 1/0/0
[RouterA-Serial1/0/0] link-protocol ppp
```

```
[RouterA-Serial1/0/0] bridge-set 1
```

Configure Router B:

```
[RouterB] bridge enable
[RouterB] bridge 1 enable
[RouterB] interface ethernet 0/0/0
[RouterB-Ethernet0/0/0] bridge-set 1
[RouterB-Ethernet0/0/0] interface Serial 1/0/0
[RouterB-Serial1/0/0] link-protocol ppp
[RouterB-Serial1/0/0] bridge-set 1
```

3.4.2 Transparent Bridging on MP

I. Network requirements

Router A and Router B are connected using MP. For the Ethernet segments of LAN 1 and LAN 2 to communicate, configure transparent bridging on the routers.

II. Network diagram

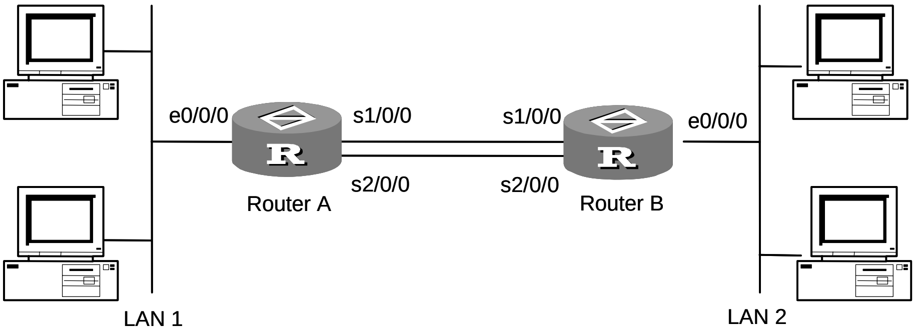


Figure 3-12 Network diagram for transparent bridging

III. Configuration procedure

1) Configure Router A

```
[RouterA] bridge enable
[RouterA] bridge 1 enable
[RouterA] interface virtual-template 1
[RouterA-virtual-template1] bridge-set 1
[RouterA virtual-template1] interface ethernet 0/0/0
[RouterA-Ethernet0/0/0] bridge-set 1
[RouterA-Ethernet0/0/0] interface serial 1/0/0
[RouterA-Serial1/0/0] link-protocol ppp
[RouterA-Serial1/0/0] ppp mp virtual-template 1
[RouterA-Serial1/0/0] interface serial 2/0/0
[RouterA-Serial2/0/0] ppp mp virtual-template 1
```

2) Configure Router B:

```
[RouterB] bridge enable
[RouterB] bridge 1 enable
[RouterB] interface virtual-template 1
[RouterB-virtual-template1] bridge-set 1
[RouterB virtual-template1] interface ethernet 0/0/0
[RouterB-Ethernet0/0/0] bridge-set 1
[RouterB-Ethernet0/0/0] interface serial 1/0/0
[RouterB-Serial1/0/0] link-protocol ppp
[RouterB-Serial1/0/0] ppp mp virtual-template 1
[RouterB-Serial1/0/0] interface serial 2/0/0
[RouterB-Serial2/0/0] ppp mp virtual-template 1
```

3.4.3 Transparent Bridging on Frame Relay

I. Networkding requirements

Two routers are directly connected using their serial interfaces to implement transparent bridging on frame relay.

II. Network diagram

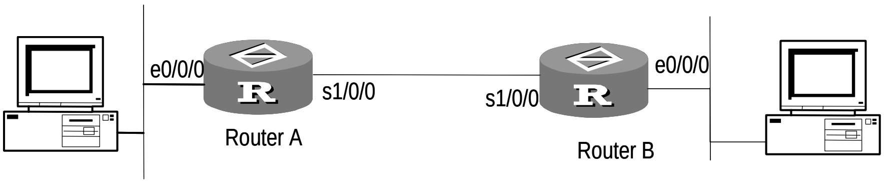


Figure 3-13 Network diagram for transparent bridging on frame relay

III. Configuration procedure

Configure Router A:

```
[RouterA] bridge enable
[RouterA] bridge 1 enable
[RouterA] interface ethernet 0/0/0
[RouterA-Ethernet0/0/0] bridge-set 1
[RouterA-Ethernet0/0/0] interface serial 1/0/0
[RouterA-Serial1/0/0] link-protocol fr
[RouterA-Serial1/0/0] fr interface-type dce
[RouterA-Serial1/0/0] fr dlci 50
[RouterA-Serial1/0/0] bridge-set 1
[RouterA-Serial1/0/0] fr map bridge 50 broadcast
```

Configure Router B:

```
[RouterB] bridge enable
```

```
[RouterB] bridge 1 enable
[RouterB] interface ethernet 0/0/0
[RouterB-Ethernet0/0/0] bridge-set 1
[RouterB-Ethernet0/0/0] interface serial 1/0/0
[RouterB-Serial1/O/0] link-protocol fr
[RouterB-Serial1/O/0] fr interface-type dte
[RouterB-Serial1/O/0] bridge-set 1
[RouterB-Serial1/O/0] fr map bridge 50 broadcast
```

3.4.4 Transparent Bridging on X.25

I. Network requirements

Two routers are directly connected using their serial interfaces to implement transparent bridging on X.25.

II. Network diagram

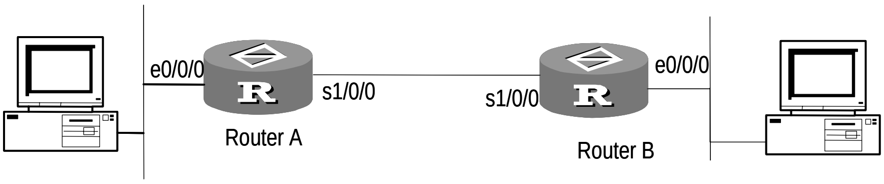


Figure 3-14 Network diagram for transparent bridging on X.25

III. Configuration procedure

Configure Router A:

```
[RouterA] bridge enable
[RouterA] bridge 1 enable
[RouterA] interface ethernet 0/0/0
[RouterA-Ethernet0/0/0] bridge-set 1
[RouterA-Ethernet0/0/0] interface serial 1/0/0
[RouterA-Serial1/0/0] link-protocol x25 dce
[RouterA-Serial1/0/0] x25 x121-address 100
[RouterA-Serial1/0/0] x25 map bridge x121-address 200 broadcast
[RouterA-Serial1/0/0] bridge-set 1
```

Configure Router B

```
[RouterB] bridge enable
[RouterB] bridge 1 enable
[RouterB] interface ethernet 0/0/0
[RouterB-Ethernet0/0/0] bridge-set 1
[RouterB-Ethernet0/0/0] interface serial 1/0/0
[RouterB-Serial1/0/0] link-protocol x25
```

```
[RouterB-Serial1/0/0] x25 x121-address 200
[RouterB-Serial1/0/0] x25 map bridge x121-address 100 broadcast
[RouterB-Serial1/0/0] bridge-set 1
```

3.4.5 Transparent Bridging on ATM

I. Network requirements

Two routers are directly connected using ATM interfaces to implement transparent bridging on ATM.

II. Network diagram

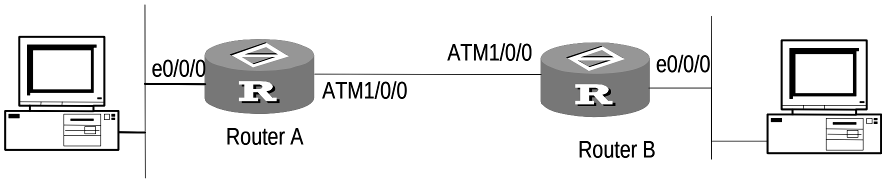


Figure 3-15 Network diagram for transparent bridging on ATM

III. Configuration procedure

Configure Router A:

```
[RouterA] bridge enable
[RouterA] bridge 1 enable
[RouterA] interface ethernet 0/0/0
[RouterA-Ethernet0/0/0] bridge-set 1
[RouterA-Ethernet0/0/0] interface atm 1/0/0
[RouterA-Atm1/0/0] pvc 10/50
[RouterA-atm-pvc-Atm1/0/0-10/50] map bridge-group broadcast
[RouterA-atm-pvc-Atm1/0/0-10/50] quit
[RouterA-Atm1/0/0] bridge-set 1
```

Configure Router B:

```
[RouterB] bridge enable
[RouterB] bridge 1 enable
[RouterB] interface ethernet 0/0/0
[RouterB-Ethernet0/0/0] bridge-set 1
[RouterB-Ethernet0/0/0] interface atm 1/0/0
[RouterB-Atm1/0/0] pvc 10/50
[RouterB-atm-pvc-Atm1/0/0-10/50] quit
[RouterB-Atm1/0/0] bridge-set 1
```

3.4.6 Implementing Integrated Routing and Bridging

I. Network requirements

Use a router, allowing routing through any interfaces in a bridge-set.

II. Network diagram

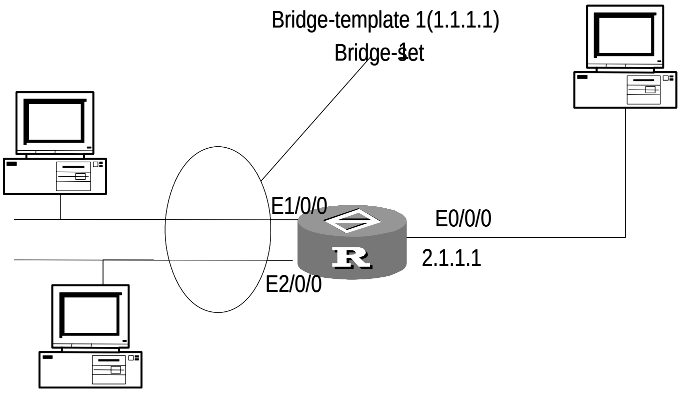


Figure 3-16 Network diagram for implementing integrated routing and bridging

III. Configuration procedure

```
[Router] bridge enable
[Router] bridge routing-enable
[Router] bridge 1 enable
[Router] bridge 1 routing ip
[Router] interface ethernet1/0/0
[Router-Ethernet1/0/0] bridge-set 1
[Router-Ethernet1/0/0] interface ethernet2/0/0
[Router-Ethernet2/0/0] bridge-set 1
[Router-Ethernet2/0/0] interface bridge-template 1
[Router-Bridge-Template1] ip address 1.1.1.1 255.255.0.0
[Router-Bridge-Template1] interface ethernet0/0
[Router-Ethernet0/0/0] ip address 2.1.1.1 255.255.0.0
```

3.4.7 Bridging on Ethernet Subinterfaces

I. Network requirements

Two routers are connected. Enabling bridging on the sub-interfaces so that the two bridges established on the routers can be interconnected.

II. Network diagram

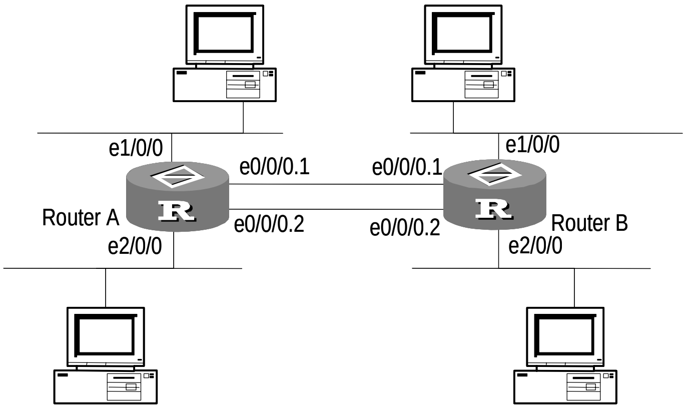


Figure 3-17 Network diagram for bridging on subinterfaces

III. Configuration procedure

# Configure Router A.

```
[RouterA] bridge enable
[RouterA] bridge 1 enable
[RouterA] bridge 2 enable
[RouterA] interface ethernet 1/0/0
[RouterA-Ethernet1/0/0] bridge-set 1
[RouterA-Ethernet1/0/0] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] bridge-set 2
[RouterA-Ethernet2/0/0] interface ethernet 0/0/0.1
[RouterA-Ethernet0/0/0.1] vlan-type dot1q vid 1
[RouterA-Ethernet0/0/0.1] bridge-set 1
[RouterA-Ethernet0/0/0.1] interface ethernet 0/0.2
[RouterA-Ethernet0/0/0.2] vlan-type dot1q vid 2
[RouterA-Ethernet0/0/0.2] bridge-set 2
```

# Configure Router B.

```
[RouterB] bridge enable
[RouterB] bridge 1 enable
[RouterB] bridge 2 enable
[RouterB] interface ethernet 1/0/0
[RouterB-Ethernet1/0/0] bridge-set 1
[RouterB-Ethernet1/0/0] interface ethernet 2/0/0
[RouterB-Ethernet2/0/0] bridge-set 2
[RouterB-Ethernet2/0/0] interface ethernet 0/0/0.1
[RouterB-Ethernet0/0/0.1] vlan-type dot1q vid 1
[RouterB-Ethernet0/0/0.1] bridge-set 1
[RouterB-Ethernet0/0/0.1] interface ethernet 0/0.2
[RouterB-Ethernet0/0/0.2] vlan-type dot1q vid 2
```

```
[RouterB-Ethernet0/0/0.2] bridge-set 2
```

3.4.8 Bridging on FR Subinterfaces

I. Network requirements

Router A and Router B are connected using an FR link. Enable bridging on FR subinterfaces S0/0/0.1 and S0/0/0.2, allowing PC 1 and PC 2 to communicate through bridge-set 1 and PC 3 and PC 4 to communicate through bridge-set 2.

In this example, Router B is at DCE side.

II. Network diagram

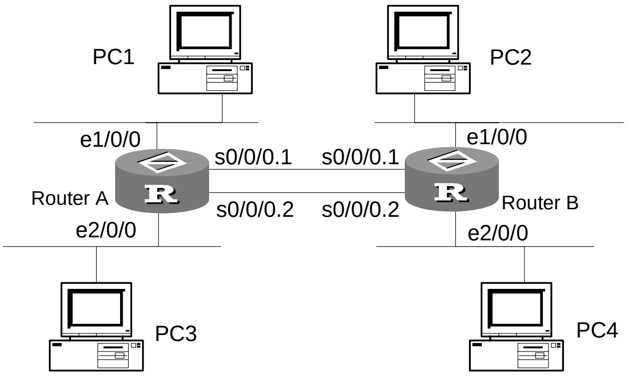


Figure 3-18 Network diagram for bridging on FR subinterfaces

III. Configuration procedure

1) Configure Router A

```
[RouterA] bridge enable
[RouterA] bridge 1 enable
[RouterA] bridge 2 enable
[RouterA] interface ethernet 1/0/0
[RouterA-Ethernet1/0/0] bridge-set 1
[RouterA-Ethernet1/0/0] interface ethernet 2/0/0
[RouterA-Ethernet2/0/0] bridge-set 2
[RouterA-Ethernet2/0/0] interface serial 0/0/0
[RouterA-Serial0/0/0] link-protocol fr
[RouterA-Serial0/0/0] interface serial 0/0/0.1
[RouterA-Serial0/0/0.1] fr map bridge 50 broadcast
[RouterA-Serial0/0/0.1] bridge-set 1
[RouterA-Serial0/0/0.1] interface serial 0/0/0.2
[RouterA-Serial0/0/0.2] fr map bridge 60 broadcast
[RouterA-Serial0/0/0.2] bridge-set 2
```

2) Configure Router B

```
[RouterB] bridge enable
[RouterB] bridge enable
[RouterB] bridge 1 enable
[RouterB] bridge 2 enable
[RouterB] interface ethernet 1/0/0
[RouterB-Ethernet1/0/0] bridge-set 1
[RouterB-Ethernet1/0/0] interface ethernet 2/0/0
[RouterB-Ethernet2/0/0] bridge-set 2
[RouterB-Ethernet2/0/0] interface serial 0/0/0
[RouterB-Serial0/0/0] link-protocol fr
[RouterB-Serial0/0/0] fr interface-type dce
[RouterB-Serial0/0/0] interface serial 0/0/0.1
[RouterB-Serial0/0/0.1] fr map bridge 50 broadcast
[RouterB-Serial0/0/0.1] fr dlci 50
[RouterB-Serial0/0/0.1] bridge-set 1
[RouterB-Serial0/0/0.1] interface serial 0/0/0.2
[RouterB-Serial0/0/0.2] fr map bridge 60 broadcast
[RouterB-Serial0/0/0.1] fr dlci 60
[RouterB-Serial0/0/0.2] bridge-set 2
```

Note that when implementing bridging on P2P FR subinterfaces, you need not to configure the **fr map** command, but must configure the same **fr dlci** at DCE and DTE sides.

3.4.9 Bridging on Dial Interface and Filtering MAC Address

I. Network requirements

IP addresses of two LANs connected by Router 1 and Router 2 belong to the same network segment.

Configure the bridge interfaces on the two routers, allowing only the packets with the source or destination MAC of 1111-2222-0000 (ffff-ffff-0000 in hexadecimal format) to pass.

II. Network diagram

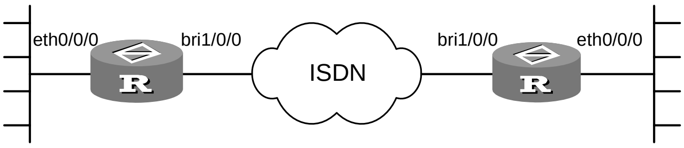


Figure 3-19 Network diagram for bridging and MAC-based filtering on dial interface

III. Configuration procedure

1) Configure Router 1

# Enable the firewall.

```
[Router1] firewall enable
```

# Enable bridging globally.

```
[Router1] bridge enable
[Router1] bridge 1 enable
```

# Configure a dialer ACL.

```
[Router1] dialer-rule 1 bridge permit
```

# Configure an ACL for MAC-based filtering.

```
[Router1] acl number 4000
[Router1-acl-ethernetframe-4000] rule 0 permit source-mac 1111-2222-0000
ffff-ffff-0000
[Router1-acl-ethernetframe-4000] rule 1 permit dest-mac 1111-2222-0000
ffff-ffff-0000
[Router1-acl-ethernetframe-4000] rule 2 deny
[Router1-acl-ethernetframe-4000] quit
```

# Configure dial-up on the ISDN BRI interface.

```
[Router1] interface Bri1/0/0
[Router1-Bri1/0/0] link-protocol ppp
[Router1-Bri1/0/0] dialer enable-circular
[Router1-Bri1/0/0] dialer-group 1
[Router1-Bri1/0/0] dialer circular-group 2
[Router1-Bri1/0/0] quit
```

# Assign the dialer interface to a bridge-set and configure MAC-based filtering on the interface.

```
[Router1] interface Dialer2
[Router1-Dialer2] link-protocol ppp
[Router1-Dialer2] firewall ethernet-frame-filter 4000 inbound
[Router1-Dialer2] firewall ethernet-frame-filter 4000 outbound
[Router1-Dialer2] bridge-set 1
[Router1-Dialer2] dialer enable-circular
[Router1-Dialer2] dialer-group 1
[Router1-Dialer2] dialer number 660208
[Router1-Dialer2] quit
```

# Assign the Ethernet interface to the bridge-set and configure MAC-based filtering on the interface.

```
[Router1] interface Ethernet0/0/0
```

```
[Router1-Ethernet0/0/0] promiscuous
[Router1-Ethernet0/0/0] firewall ethernet-frame-filter 4000 inbound
[Router1-Ethernet0/0/0] firewall ethernet-frame-filter 4000 outbound
[Router1-Ethernet0/0/0] bridge-set 1
```

2) Configure Router 2

# Enable the firewall.

```
[Router2] firewall enable
```

# Enable bridging globally.

```
[Router2] bridge enable
[Router2] bridge 1 enable
```

# Configure a dialer ACL.

```
[Router2] dialer-rule 1 bridge permit
```

# Configure an ACL for MAC-based filtering.

```
[Router2] acl number 4000
[Router2-acl-ethernetframe-4000] rule 0 permit source-mac 1111-2222-0000
ffff-ffff-0000
[Router2-acl-ethernetframe-4000] rule 1 permit dest-mac 1111-2222-0000
ffff-ffff-0000
[Router2-acl-ethernetframe-4000] rule 2 deny
[Router2-acl-ethernetframe-4000] quit
```

# Configure dial-up on the ISDN BRI interface.

```
[Router2] interface Bri1/0/0
[Router2-Bri1/0/0] link-protocol ppp
[Router2-Bri1/0/0] dialer enable-circular
[Router2-Bri1/0/0] dialer-group 1
[Router2-Bri1/0/0] dialer circular-group 2
[Router2-Bri1/0/0] quit
```

# Assign the dialer interface to a bridge-set and configure MAC-based filtering on the interface.

```
[Router2] interface Dialer2
[Router2-Dialer2] link-protocol ppp
[Router2-Dialer2] firewall ethernet-frame-filter 4000 inbound
[Router2-Dialer2] firewall ethernet-frame-filter 4000 outbound
[Router2-Dialer2] bridge-set 1
[Router2-Dialer2] dialer enable-circular
[Router2-Dialer2] dialer-group 1
[Router2-Dialer2] dialer number 660206
[Router2-Dialer2] quit
```

Assign the Ethernet interface to the bridge-set and configure MAC-based filtering on the interface.

```
[Router2] interface Ethernet0/0/0
[Router2-Ethernet0/0/0] promiscuous
[Router2-Ethernet0/0/0] firewall ethernet-frame-filter 4000 inbound
[Router2-Ethernet0/0/0] firewall ethernet-frame-filter 4000 outbound
[Router2-Ethernet0/0/0] bridge-set 1
```

3.5 Ethernet Type-Code Values

The following table lists the Ethernet type-code values recommended in RFC 1700 and their meanings.

Table 3-30 Ethernet type-code values

Ethernet type-code value (in hexadecimal)	Represents
0000-05DC	IEEE802.3 Length Field
0101-01FF	Experimental
200	XEROX PUP (see 0A00)
201	PUP Addr Trans (see 0A01)
400	Nixdorf
600	XEROX NS IDP
660	DLOG
661	DLOG
800	Internet IP (IPv4)
801	X.75 Internet
802	NBS Internet
803	ECMA Internet
804	Chaosnet
805	X.25 Level 3
806	ARP
807	XNS Compatibility
081C	Symbolics Private
0888-088A	Xyplex
900	Ungermann-Bass net debugr
0A00	Xerox IEEE802.3 PUP
0A01	PUP Addr Trans

Ethernet type-code value (in hexadecimal)	Represents
0BAD	Banyan Systems
1000	Berkeley Trailer nego
1001 – 100F	Berkeley Trailer encap/IP
1600	Valid Systems
4242	PCS Basic Block Protocol
5208	BBN Simnet
6000	DEC Unassigned (Exp.)
6001	DEC MOP Dump/Load
6002	DEC MOP Remote Console
6003	DEC DECNET Phase IV Route
6004	DEC LAT
6005	DEC Diagnostic Protocol
6006	DEC Customer Protocol
6007	DEC LAVC, SCA
6008 – 6009	DEC Unassigned
6010 – 6014	3Com Corporation
7000	Ungermann-Bass download
7002	Ungermann-Bass dia/loop
7020-7029	LRT
7030	Proteon
7034	Cabletron
8003	Cronus VLN
8004	Cronus Direct
8005	HP Probe
8006	Nestar
8008	AT&T
8010	Excelan
8013	SGI diagnostics
8014	SGI network games
8015	SGI reserved
8016	SGI bounce server

Ethernet type-code value (in hexadecimal)	Represents
8019	Apollo Computers
802E	Tymshare
802F	Tigan, Inc.
8035	Reverse ARP
8036	Aeonic Systems
8038	DEC LANBridge
8039 – 803C	DEC Unassigned
803D	DEC Ethernet Encryption
803E	DEC Unassigned
803F	DEC LAN Traffic Monitor
8040 – 8042	DEC Unassigned
8044	Planning Research Corp.
8046	AT&T
8047	AT&T
8049	ExperData
805B	Stanford V Kernel exp.
805C	Stanford V Kernel prod.
805D	Evans & Sutherland
8060	Little Machines
8062	Counterpoint Computers
8065	Univ. of Mass. @ Amherst
8066	Univ. of Mass. @ Amherst
8067	Veeco Integrated Auto.
8068	General Dynamics
8069	AT&T
806A	Autophon
806C	ComDesign
806D	Computgraphic Corp.
806E – 8077	Landmark Graphics Corp.
807A	Matra
807B	Dansk Data Elektronik

Ethernet type-code value (in hexadecimal)	Represents
807C	Merit Internodal
807D-807F	Vitalink Communications
8080	Vitalink TransLAN III
8081-8083	Counterpoint Computers
809B	Appletalk
809C – 809E	Datability
809F	Spider Systems Ltd.
80A3	Nixdorf Computers
80A4 – 80B3	Siemens Gammasonics Inc.
80C0 – 80C3	DCA Data Exchange Cluster
80C4	Banyan Systems
80C5	Banyan Systems
80C6	Pacer Software
80C7	Applitek Corporation
80C8 – 80CC	Intergraph Corporation
80CD – 80CE	Harris Corporation
80CF – 80D2	Taylor Instrument
80D3 – 80D4	Rosemount Corporation
80D5	IBM SNA Service on Ether
80DD	Varian Associates
80DE – 80DF	Integrated Solutions TRFS
80E0 – 80E3	Allen-Bradley
80E4 – 80F0	Datability
80F2	Retix
80F3	AppleTalk AARP (Kinetics)
80F4 – 80F5	Kinetics
80F7	Apollo Computer
80FF – 8103	Wellfleet Communications
8107 – 8109	Symbolics Private
8130	Hayes Microcomputers
8131	VG Laboratory Systems

Ethernet type-code value (in hexadecimal)	Represents
8132 – 8136	Bridge Communications
8137 – 8138	Novell, Inc.
8139 – 813D	KTI
8148	Logicraft
8149	Network Computing Devices
814A	Alpha Micro
814C	SNMP
814D	BIIN
814E	BIIN
814F	Technically Elite Concept
8150	Rational Corp
8151 – 8153	Qualcomm
815C – 815E	Computer Protocol Pty Ltd
8164 – 8166	Charles River Data System
817D – 818C	Protocol Engines
818D	Motorola Computer
819A – 81A3	Qualcomm
81A4	ARAI Bunkichi
81A5 – 81AE	RAD Network Devices
81B7 – 81B9	Xyplex
81CC – 81D5	Apricot Computers
81D6 – 81DD	Artisoft
81E6 – 81EF	Polygon
81F0 – 81F2	Comsat Labs
81F3 – 81F5	SAIC
81F6 – 81F8	VG Analytical
8203 – 8205	Quantum Software
8221 – 8222	Ascom Banking Systems
823E – 8240	Advanced Encryption Syste
827F – 8282	Athena Programming
8263 – 826A	Charles River Data System

Ethernet type-code value (in hexadecimal)	Represents
829A – 829B	Inst Ind Info Tech
829C – 82AB	Taurus Controls
82AC – 8693	Walker Richer & Quinn
8694 – 869D	Idea Courier
869E – 86A1	Computer Network Tech
86A3 – 86AC	Gateway Communications
86DB	SECTRA
86DE	Delta Controls
86DF	ATOMIC
86E0 – 86EF	Landis & Gyr Powers
8700 – 8710	Motorola
8A96 – 8A97	Invisible Software
9000	Loopback
9001	3Com(Bridge) XNS Sys Mgmt
9002	3Com(Bridge) TCP-IP Sys
9003	3Com(Bridge) loop detect
FF00	BBN VITAL-LanBridge cache
FF00-FF0F	ISC Bunker Ramo

Network Protocol

Table of Contents

Chapter 1 IP Address Configuration

1.1 IP Address Overview

IP addresses are unique 32-bit addresses assigned to hosts connected to Internet. An IP address is composed of two parts: network ID and host ID. Its structure enables convenient addressing on Internet. IP addresses are assigned by Network Information Center (NIC) of American National Defense Data Network.

IP address consists of the following fields:

- Network ID field (net-id), among which the former bits are called the category field (or category bits) used to distinguish the types of IP addresses.
- Host ID field (host-id). Since host number with all 1s or 0s has special usage, it is specified that the host number should not be all 1s or 0s.

For easy IP address management and convenient networking, IP address of Internet is divided into five classes. As shown in the following diagram:

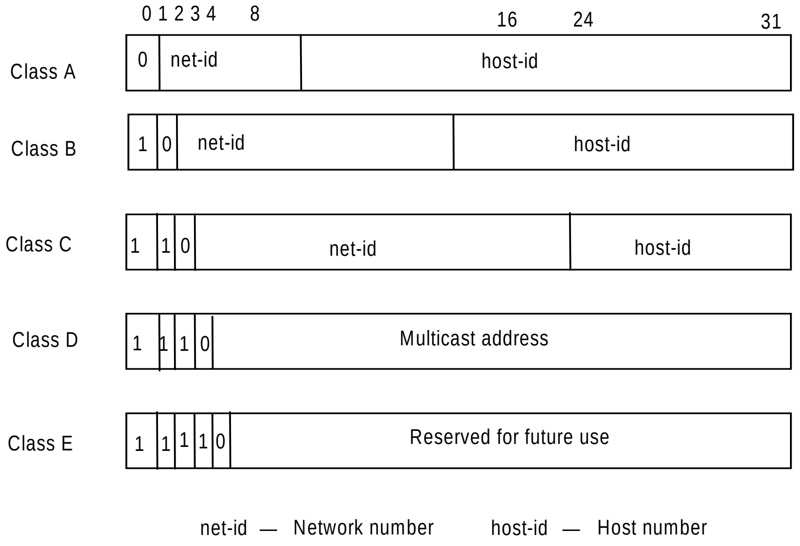


Figure 1-1 Classification of IP address

Address of class D is a multicast address, mainly used by IAB (Internet Architecture Board). Address of class E is reserved for future use. At present, Most IP addresses are class A, class B and class C.

When using IP addresses, it should also be noted that some of them are reserved for special uses, and are seldom used. The IP addresses you can use are listed in the following table.

Table 1-1 IP address classes and ranges

Network class	Address range	Description
A	0.0.0.0 to 127.255.255.255	Network ID with the format of 127.X.Y.Z is reserved for self-loop test and the packets sent to this address will not be output to the line. The packets are processed internally and regarded as input packets.
B	128.0.0.0 to 191.255.255.255	—
C	192.0.0.0 to 223.255.255.255	—
D	224.0.0.0 to 239.255.255.255	Addresses of class D are multicast addresses.
E	240.0.0.0 to 255.255.255.255	255.255.255.255 is a broadcast address, and the others are reserved for future use.

Important features of IP address:

- IP addresses are not in a hierarchical structure, which is different from the structure of telephone number. In other words, IP addresses cannot reflect any geographical information about the host position.
- When a host is connected to two networks at the same time (such as the host used as a router), it must have two IP addresses with different net-ids corresponding to two different networks. Such host is called multi-homed host.
- According to Internet concept, several LANs connected via transceiver or bridge are still in the same network, so these LANs have the same net-id.
- With respect to IP address, all networks with a net-ids are equal (no matter it is a small LAN or a huge WAN).

Since 1985, only the net-id of IP address is assigned by NIC, while the host-id is controlled by the enterprise. The IP address assigned to an enterprise is only a network ID: net-id. The specific host Ids, the host-ids for respective hosts, shall be assigned by the enterprise independently, so long as there is no repetition of host IDs within its network.

If there are many enterprise hosts widely scattered, the host IDs may be further divided into internal sub-nets to facilitate management. Note that the division of sub-nets is completely internal to the enterprise itself, and seen from the outside, the enterprise only has one net-id. When an external packet enters this enterprise network, the internal router can route according to the sub-net number, and finally reach the destination host.

The following figure shows the sub-net classification of a Class B IP address, in which a sub-net mask consists of a string of continuous "1" s and a string of continuous "0" s.

The 1s corresponds to the network ID field and the sub-net number field, while the 0s correspond to the host ID field.

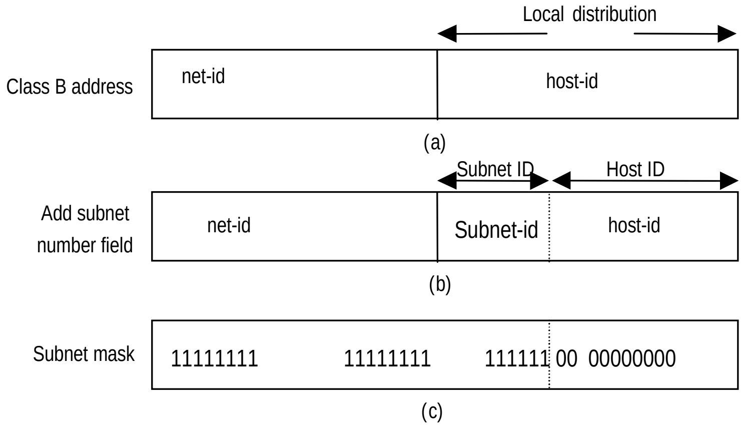


Figure 1-2 Sub-net classification of IP address

Classification of one more sub-net number field is at a price. For example, an IP address of class B originally consists of 65534 (2^{16}-2) host IDs. However, after a 6-bit-long sub-net field is classified, there may be at most 64 sub-nets. Each sub-net has 10-bit host ID, i.e., each sub-net has 1022 host IDs at most. There are 64 x 1022=65408 host IDs in total, 126 less than the sum before sub-net classification.

If there is no sub-net division in an enterprise, then its sub-net mask is the default value and the length of "1" indicates the net-id length. Therefore, for IP addresses of classes A, B and C, the default values of corresponding sub-net mask are 255.0.0.0, 255.255.0.0 and 255.255.255.0 respectively.

A router used to connect multiple sub-nets together will have multiple sub-net IP addresses.

The IP addresses mentioned above cannot be directly used in communication, because:

- An IP address is only an address of a host in the network layer. To send the data packets transmitted through the network layer to the destination host, physical address of the host is required. So the IP address must be first resolved into a physical address.
- IP address is hard to remember, but a host domain name will be much easier to remember and is also more popular. So the host domain name must also be resolved into an IP address.

The following figure illustrates relations among host name, IP address and physical address.

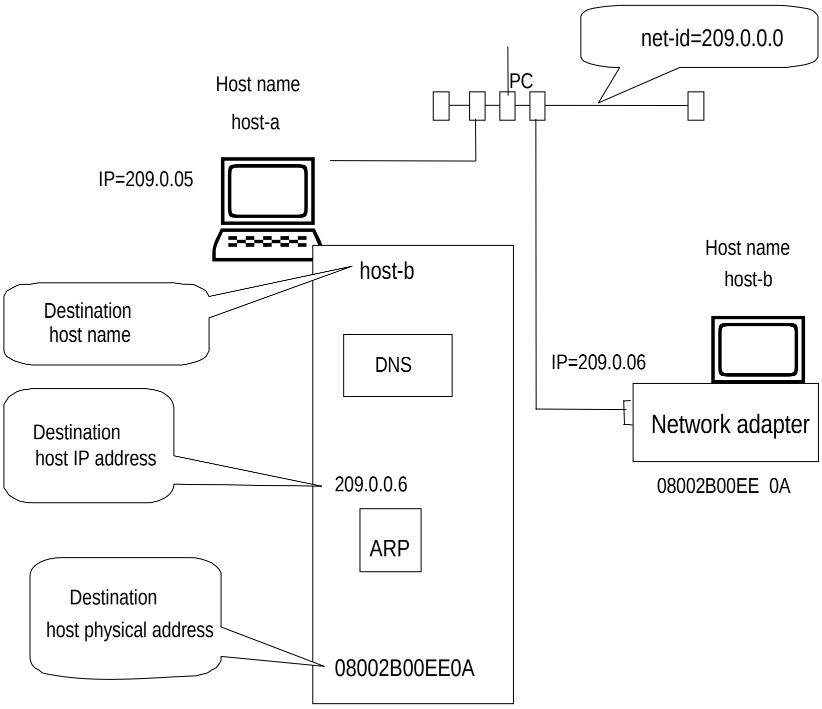


Figure 1-3 Relation between host name, IP address, and physical address

1.2 IP Address Configuration

IP address configuration includes:

- Assigning IP Addresses to an Interface
- Configuring IP Address Unnumbered for an Interface

1.2.1 Assigning IP Addresses to an Interface

Each interface of a router can have multiple IP addresses, among which one is the main IP address and the others are subordinate IP addresses (also called secondary IP addresses).

When assigning IP addresses to an interface, consider the following:

- A father interface and its subinterfaces must not reside on the same network segment.
- Peer interfaces must not reside on the same network segment.
- A main interface and a subordinate IP address can be in the same network segment.

I. Assigning a main IP address to an interface

Each interface can be assigned only one main IP address.

Perform the following configuration in interface view.

Table 1-2 Configure main IP address of an interface

Operation	Command
Configure main IP address of an interface	**ip address** *ip-address net-mask*

A mask identifies the netid boundary of an IP address. Suppose an Ethernet interface is assigned the IP address 129.9.30.42 with the mask of 255.255.0.0. Logic AND the IP address with the mask; then you can know that the Ethernet interface is assigned to the network segment 129.9.0.0.

Your main IP address configuration can overwrite the existing one, if there is any.

By default, no main IP address is assigned to any interface.

II. Configuring subordinate IP address of an interface

Besides the main IP address, several subordinate IP addresses can be configured on an interface. The purpose of assigning subordinate IP addresses is to have the same interface located in different sub-nets, to create network routes with the same interface as the output port, and set up connection via the same interface to multiple sub-nets.

Perform the following configuration in interface view.

Table 1-3 Configure a subaddress on an interface

Operation	Command
Configure a subaddress on an interface.	**ip address** *ip-address net-mask* **sub**

By default, no subaddress is configured.

You can configure up to 32 addresses on an interface, including the main IP address and subaddresses.

⚠ **Caution:**

For an interface that is configured to allocate IP addresses through BOOTP, DHCP, or PPP negotiation, you cannot define subaddresses.

III. Deleting IP addresses on an interface

Perform the following configuration in interface view.

Table 1-4 Delete IP addresses on the interface

Operation	Command
Delete IP addresses on the interface.	**undo ip address** [*ip-address net-mask* [**sub**]]

To delete all IP addresses on the interface, execute this command without specifying any argument.

To delete the main IP address, use the **undo ip address** *ip-address net-mask* command.

To delete subordinate addresses, use the **undo ip address** *ip-address net-mask* **sub** command.

Before you can delete the main IP address, you must delete all subordinate addresses.

IV. Setting negotiable attribute of an IP address for an interface

If a PPP-encapsulated interface is not assigned an IP address while its peer has been assigned one, you may configure PPP address negotiation to have it accept the address assigned by the peer. For example, when accessing the Internet through an ISP, you may use the **ip address ppp-negotiate** command to accept the addresses assigned by the ISP.

Perform the following configuration in interface view.

Table 1-5 Set negotiable attribute of IP address for an interface

Operation	Command
Set negotiable attribute of IP address for an interface	**ip address ppp-negotiate**
Cancel negotiable attribute of IP address for an interface	**undo ip address ppp-negotiate**

By default, the system does not allow to negotiate the interface IP address. For detailed configuration information about PPP interface address negotiation, refer to the section related to PPP protocol in the “Link Layer Protocol” part of this manual.

⚠ **Caution:**

- Because PPP supports IP address negotiation, IP address negotiation of an interface can be set only when the interface is encapsulated with PPP. When the PPP link is down, the IP address originated from negotiation will be deleted.
- If the interface has original address, then after setting IP address of the interface to negotiable, the original IP address will be deleted.
- After setting IP address of an interface to negotiable, it is unnecessary to configure IP address for the interface, as negotiation will automatically originate an IP address.
- After setting IP address of an interface to negotiable, if the interface is set to negotiable again, then the IP address originated from the original negotiation will be deleted, and the interface obtains IP address through the re-negotiation.
- The interface will have no address after the negotiation address is deleted.

1.2.2 Configuring IP Address Unnumbered for an Interface

I. Introduction to IP Address Unnumbered

The main purpose of borrowing IP address is to save IP address resource.

If an interface has no IP address, it can neither generate any route nor forward any packet. "IP Address Unnumbered" is used when you want to use an interface with no IP address. In such case, an IP address will be borrowed from another interface. If the lending interface has multiple IP addresses, then only the main one can be borrowed. However, if the lending interface has no IP address, then the IP address of the borrowing interface is 0.0.0.0. This function is implemented through the command **ip address unnumbered**.

The following should be noted:

- The borrower cannot be an Ethernet interface.
- The address of the lending interface cannot be an unnumbered address.
- The lending interface can lend its address tomultiple interfaces.
- The address of Loopback interface can be borrowed by other interfaces, but it cannot borrow the addresses of other interfaces.

Because the borrowing interface has no IP address of its own, and cannot route, two static routes need to be configured manually to connect routers together. Refer to the configuration examples for the specific configuration procedure.

II. IP Address Unnumbered configuration task list

The configuration of IP Address Unnumbered can be performed in the interface view. Serial interfaces encapsulated with PPP, HDLC, Frame Relay and Tunnel can borrow the IP addresses of the Ethernet interface and other kinds of interfaces.

IP Address Unnumbered configuration includes:

- Activating/deactivating IP address unnumbered

III. Activating/deactivating IP address unnumbered

Perform the following task in the interface view to activate/deactivate IP address unnumbered.

Table 1-6 Configure IP address unnumbered

Operation	Command
Activate IP address unnumbered	**ip address unnumbered interface** *interface-type interface-number*
Deactivate IP address unnumbered	**undo ip address unnumbered**

By default, IP address unnumbered is disabled.

1.2.3 Displaying and Debugging IP Address

After the above configuration, execute display command in all views to display the running of the IP Address, and to verify the effect of the configuration.

Table 1-7 Display and debug IP address

Operation	Command
Display IP-related information about the specified or all interfaces	**display ip interface** [*interface-type interface-number*]
Display IP-related summary about the specified or all interfaces	**display ip interface brief** [*interface-type interface-number*]

1.2.4 Displaying and Debugging IP Address Unnumbered

After the above configuration, execute display command in all views to display the running of the IP Address Unnumbered, and to verify the effect of the configuration.

Table 1-8 Display and debug IP Address Unnumbered

Operation	Command
Display information of IP Address Unnumbered	**display interface** [*interface-type* [*interface-number*]]

Operation	Command
Display the information of configuration that in now running	**display current-configuration**

1.2.5 IP Address Configuration Example

I. Network requirements

To configure IP addresses for a router's serial interface, it is required that the main IP address is 129.2.2.1, and the subordinate IP address is 129.1.3.1.

II. Network diagram

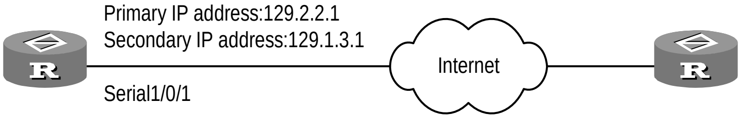


Figure 1-4 Configure the main and subordinate IP address for a router's interface

III. Configuration procedure

# Configure the main and subordinate IP address for router's interface serial1/0/1.

```
[3Com] interface serial 1/0/1
[3Com-Serial1/0/1] ip address 129.2.2.1 255.255.255.0
[3Com-Serial1/0/1] ip address 129.1.3.1 255.255.255.0 sub
```

1.2.6 IP Address Unnumbered Configuration Example

I. Network requirements

Suppose the headquarters of a company is in Beijing, with one subsidiary in Shenzhen and Shanghai respectively and one office in Wuhan. Its networking diagram is shown in the following figure. R is the headquarters router, which connects the subsidiaries and office routers R1, R2 and R3 through PSTN. The four routers R, R1, R2 and R3 each have a serial port for dialing and one Ethernet interface to connect with local network.

II. Network diagram

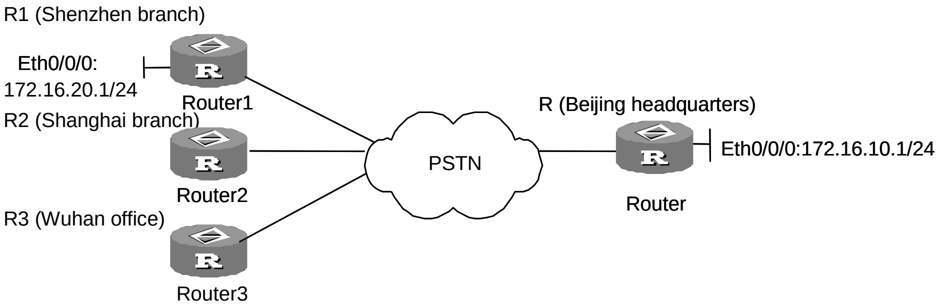


Figure 1-5 Network diagram for IP address unnumbered configuration

III. Configuration procedure

1) Configure headquarters router R

```
[3Com-Ethernet1/0/0] ip address 172.16.10.1 255.255.255.0
```

# Borrow IP address of Ethernet.

```
[3Com-Serial2/0/0] ip address unnumbered interface ethernet 1/0/0
[3Com-Serial2/0/0] link-protocol ppp
```

# Configure routing to Ethernet segment of Shenzhen router R1.

```
[3Com] ip route-static 172.16.20.0 255.255.255.0 172.16.20.1
```

# Configure the interface routing to Shenzhen router R1 serial interface.

```
[3Com] ip route-static 172.16.20.0 255.255.255.0 serial2/0/0
```

2) Configure router R1 at Shenzhen branch

```
[3Com-Ethernet1/0/0] ip address 172.16.20.1 255.255.255.0
```

# Borrow IP address of Ethernet.

```
[3Com-Serial2/0/0] ip address unnumbered interface ethernet 1/0/0
[3Com-Serial2/0/0] link-protocol ppp
```

# Configure routing to Ethernet segment on Beijing headquarters router R, this routing is default routing.

```
[3Com] ip route-static 0.0.0.0 0.0.0.0 172.16.10.1
```

# Configure interface routing to serial interface of Beijing router R.

```
[3Com] ip route-static 172.16.10.1 255.255.255.255 serial2/0/0
```

1.2.7 Troubleshooting IP Address Configuration

A router is a network interconnection device. So when IP address for an interface is configured, networking requirements and sub-net classification should be known. Normally, the following rules should be observed:

- The main IP address of a router Ethernet interface must be in the same network segment with the LAN to which this Ethernet interface is connected.
- Serial interface IP addresses of the routers at both ends of WAN must be in the same network segment.

Fault 1: the router cannot **ping** through a certain host in LAN

Troubleshooting:

- First check if the IP address configuration of the router's Ethernet interface and the host in LAN are in the same network segment
- If the configuration is correct, enable ARP debugging on the router, and check if the router can correctly send and receive ARP packets. If it can only send but cannot receive ARP packets, then possibly errors occur on the Ethernet physical layer.

Chapter 2 ARP Configuration

2.1 Dynamic/Static ARP Configuration

2.1.1 Introduction to Dynamic ARP

ARP (Address Resolution Protocol) is mainly used for resolution from IP address to Ethernet MAC address. Normally, dynamical ARP is used to resolve the mapping relation from the IP address to the Ethernet MAC address. The resolution is completed automatically without interference of the administrator.

In the implementation of V 2.41, the system creates or updates ARP entries when receiving an ARP message compliant with one of the following conditions:

- The source IP address is a non-broadcast address located in the same segment attached to the receiving interface, the destination IP address is the same as the IP address of the interface.
- The source IP address is a non-broadcast address located in the same segment attached to the receiving interface, the destination IP address is the VRRP virtual IP address on the interface.
- The destination IP address is included in the NAT address pool on the receiving interface.

In addition, if one ARP entry has existed for the source IP address, the system updates the entry.

2.1.2 Brief Introduction to Static ARP

Static ARP applies to:

- Bind packets destined to an address beyond this segment to a network adapter, so that they can be forwarded through this gateway.
- Filter out invalid IP addresses by binding them to a MAC address that does not exist.

2.1.3 Static ARP Configuration

The static ARP configuration includes:

- Manually add/delete static ARP mapping table item.

Perform the following task in the system view.

Table 2-1 Manually add/delete static ARP mapping table item

Operation	Command
Manually add static ARP mapping table item	**arp static** *ip-address ethernet-address* [*vpn-instance-name*]
Manually delete static ARP mapping table item	**undo arp** *ip-address* [*vpn-instance-name*]

While the lifetime of dynamic ARP mappings is only 20 minutes, static ARP mappings never age out.

The ARP table on the router can accommodate up to 2048 static entries.

By default, address mappings are obtained through dynamic ARP.

2.1.4 Dynamic ARP Configuration

I. Enabling/disabling ARP entry check (optional)

You can enable or disable the device to learn the ARP entries with broadcast MAC addresses.

Perform the following configuration in system view.

Table 2-2 Enable/disable ARP entry check

Operation	Command
Enable ARP entry check to have the device not learn the ARP entries with broadcast MAC addresses.	**arp check enable**
Disable ARP entry check to have the system learn the ARP entries with broadcast MAC addresses.	**undo arp check enable**

By default, ARP entry check is enabled. The device does not learn the ARP entries with broadcast MAC addresses.

II. Enabling/disabling ARP request in the scope of natural network segments (optional)

ARP request is usually restricted only in subnets, but you are allowed to enable ARP request in the scope of natural segments.

Perform the following configuration in system view.

Table 2-3 Enable/disable ARP request in the scope of natural network segments

Operation	Command
Enable ARP request in the scope of natural segments.	**naturemask-arp enable**
Disable ARP request in the scope of natural segments.	**undo naturemask-arp enable**

By default, ARP request in the scope of natural network segments is not supported.

III. Setting the aging timer for dynamic ARP entries

Perform the following configuration in system view.

Table 2-4 Set the aging timer for dynamic ARP entries

Operation	Command
Set the aging timer for dynamic ARP entries	**arp timer aging** *minutes*
Restore the default setting of the aging timer for dynamic ARP entries	**undo arp timer aging**

By default, the aging timer for dynamic ARP entries is set to 20 minutes.

2.1.5 Displaying and Debugging ARP

After the above configuration, execute the **display** command in all views to display the running of the ARP configuration, and to verify the effect of the configuration.

Execute the **reset** command in user views to clear the running.

Execute the **debugging** command in user view for the debugging of ARP configuration.

Table 2-5 Display and debug ARP

Operation	Command
Show ARP mapping table	**display arp** [**static** | **dynamic** | **all**]
Display the aging timer for dynamic ARP entries (only for the AR46 Series)	**display arp timer aging**
Clear the ARP entries in the ARP mapping table	**reset arp** [**all** | **dynamic** | **static** | **interface** *interface-type interface-number*]
Enable ARP information debugging	**debugging arp packet**
Disable ARP information debugging	**undo debugging arp packet**

2.2 Proxy ARP Configuration

2.2.1 Introduction

You can assign physically distributed computers and routers to the same network segment by assigning them IP addresses in the same network segment. Proxy ARP allows them to communicate with each other as they would in the same physical network.

The late 1980s witnessed an explosive growth of LANs along with the development of network applications. A good example is that even the Ethernet of a university could be connected to as many as hundreds of hosts. This increased the likelihood of collisions on the Ethernet. In addition, to implement new applications, a LAN must be expanded, for example, by using repeaters to connect new computers. This however, might cause overload and decrease network performance because of presence of heavy collisions. To solve the problem, proxy ARP was thus introduced.

2.2.2 Application Environments for Proxy ARP

Proxy ARP functions to connect two networks that are physically separated but on the same IP network segment at the same.

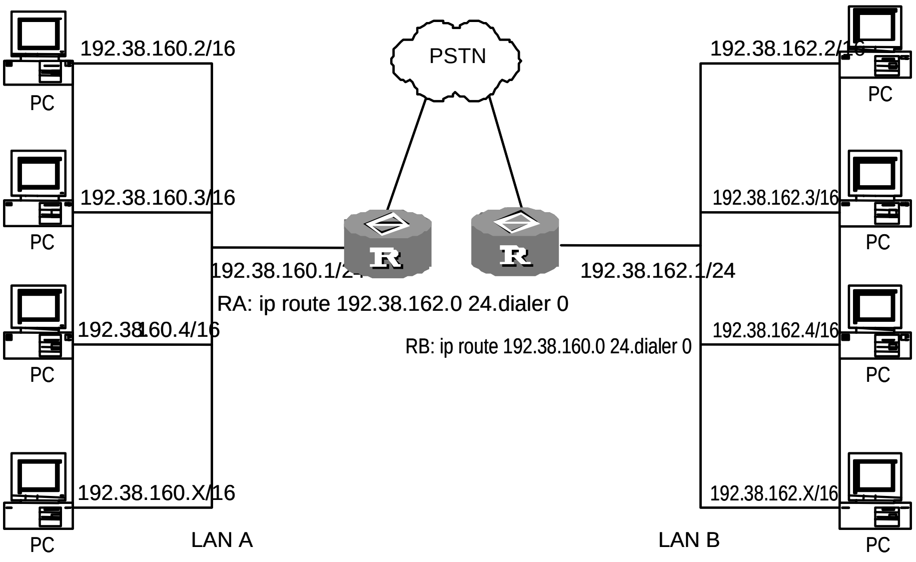


Figure 2-1 Application environment for proxy ARP

The scenario in the above figure illustrates that:

- LAN A and LAN B are connected each to an Ethernet interface on a router.
- All hosts on the LANs belong to network segment 192.38.0.0, with LAN using 192.38.160.0 and LAN B using 192.38.162.0.
- For both LANs, the host mask is 16 bits. As the result, all hosts on the LANs consider that they are located on the network segment 192.38.0.0.

- On the two routers, the involved interfaces are assigned to the 192.38.0.0 segment and enabled with proxy ARP.
- The two routers are connected through PSTN and each configured with a static route to the network segment of the opposite end.

Assume that the IP address of Host A on LAN A is 192.38.160.2, and the IP address of Host B on LAN B is 192.38.162.2. The following is how ARP works when Host A accesses Host B:

- Host A sends an ARP request for reaching Host B.
- Router A receives the request and looks up its routing table. If finding a routing entry, 192.38.162.0 for example, for reaching Host B, the router sends back an ARP response with its own MAC address included.
- After receiving the ARP response, Host A sends IP packets to Router A.
- After receiving the IP packets, Router A forwards them to Router B.
- Router B forwards the received IP packets to Host B.

To send responses to Host A, Host B undergoes the same procedure.

Thus, these two physically separated hosts can access each other as they would on the same physical network.

2.2.3 Configuring Proxy ARP

Perform the following configuration in Ethernet interface view.

Table 2-6 Enable/disable proxy ARP

Operation	Command
Enable proxy ARP function	**arp-proxy enable**
Disable proxy ARP function	**undo arp-proxy enable**

By default, proxy ARP is disabled.

2.3 Gratuitous ARP Configuration

2.3.1 Introduction to Gratuitous ARP

A network device can check for IP address conflicts with other devices by sending gratuitous ARP messages.

When the network device broadcasts a gratuitous ARP message, it sets both the source and destination IP addresses to local addresses, and sets the source MAC address to a local MAC address. Every receiving device checks the IP addresses in the received gratuitous ARP message and sends back an ARP response if detecting an address conflict.

In addition, by sending gratuitous ARP messages, a network device can update its current hardware address to the caches on other devices if a hardware address change has occurred for example, after the device reconnected to the network with a new interface card. As ARP requests are broadcast, this update involves all devices on the network.

The following are characteristics of gratuitous ARP packets:

- Both source and destination IP addresses are local addresses, and their source MAC addresses are local MAC addresses.
- If a device finds that the IP addresses carried in a received gratuitous packet are in conflict with the address of its own, it returns an ARP response to the sending device.

2.3.2 Enabling the Address Learning Function of Gratuitous ARP

Perform the following configuration in system view.

Table 2-7 Enable the address learning function of gratuitous ARP

Operation	Command
Enable the address learning function of gratuitous ARP	**gratuitous-arp-learning enable**
Disable the learning function of gratuitous ARP	**undo gratuitous-arp-learning enable**

By default, the address learning function of gratuitous ARP is disabled.

2.3.3 Responding to the Gratuitous ARP Requests from Other Network Segments

Perform the following configuration in system view.

Table 2-8 Respond to the gratuitous ARP requests from other network segments

Operation	Command
Enable the system to respond to the gratuitous ARP requests from other network segments	**gratuitous-arp-sending enable**
Disable the system to respond to the gratuitous ARP requests from other network segments	**undo gratuitous-arp-sending enable**

By default, the router does not respond to the gratuitous ARP requests received from other network segments.

2.4 Map between WAN Interface IP Address and Link Layer Protocol Address

In a router, you shall maintain both the mapping from an Ethernet interface IP address to an MAC address, and that from a WAN interface IP address to a link layer protocol address. Namely there are the following types:

- On an interface encapsulated with X.25, the mapping between an IP address and X.121 address is maintained by the command **x25 map ip**.
- On an interface encapsulated with Frame Relay, mapping between an IP address and a virtual circuit number (DLCI) is maintained by the command **fr map ip**.

The above mapping tables are also called second routing, which is essential to the normal working of the router. For details, refer to related chapters in "Link Layer Protocol" of this manual.

2.5 Authorized ARP Configuration

2.5.1 Introduction to Authorized ARP

Authorized address resolution protocol (authorized ARP) enables the DHCP server or other modules to automatically add authorized ARP entries to the ARP table based on certain conventions. Allowing only static entries and entries with IP addresses from the DHCP server to be added to the ARP table, authorized ARP can stop a DHCP server learning dynamically from illegal ARP responses, making illegal clients unable to access the Internet. Authorized ARP also provides a probing mechanism called ARP ping. It can identify a log-off DHCP client and notify the DHCP Server of that. By deploying authorized ARP, you can achieve both enhanced network security and quick detection of a client going down.

Note:

- Currently, authorized ARP can only be implemented on a router with the DHCP server function enabled.
- Currently, authorized ARP supports only the scenario that the DHCP server and DHCP clients are on the same segment.

2.5.2 Basic Concepts

- ARP cache

Each host has an ARP cache, in which the recently learned mappings between the IP addresses and hardware addresses are kept. By default, the lifetime of each entry in the cache is 20 minutes.

During ARP translation, the ARP cache is searched at first. If no match is found, the ARP table is searched.

- ARP table

An ARP table keeps the mappings between IP addresses and physical addresses. A mapping can be generated dynamically, statically, or by any other way. Each device maintains an ARP table.

The fields of the ARP table are IF index, physical address, IP address, and type.

- ARP ping

The aging of authorized ARP is implemented by a mechanism called ARP ping. By periodically sending an ARP request to the IP address of a client recorded in an authorized ARP entry, ARP ping can detect whether the client is down. Whenever receiving an ARP response, whether the response is triggered by ARP ping or not, authorized ARP refreshes the aging time of the entry. ARP ping provides the DHCP server an initiative client status inquiry mechanism, enabling the DHCP server to detect offline clients in a shorter period of time and release the resources assigned to them.

- Authorized ARP entry

Authorized ARP entry is a kind of special entry. An authorized ARP entry is also added into the ARP table of the device, and has the features of the static ARP entry and the dynamic ARP entry. An authorized ARP entry has a higher priority than a dynamic ARP entry for the same mapping; a new authorized ARP entry overrides a dynamic ARP entry, while a new dynamic ARP entry cannot override an authorized ARP entry. At the same time, an authorized ARP entry has a lower priority than a static ARP entry for the same mapping; a new authorized ARP entry cannot override a static ARP entry, while a new static ARP entry overrides an authorized ARP entry.

The aging mechanism of authorized ARP is similar to that of dynamic ARP; they determine whether an entry needs to be aged by recording and refreshing the aging time of the entry. The aging of an authorized ARP entry is implemented by ARP ping, which is independent of the aging of a dynamic ARP entry.

The default aging time of an authorized ARP entry is the time that three ARP ping operations takes when no responses are received. Since the ARP ping interval is 30 seconds, the default aging time of an authorized ARP entry is 90 seconds. If no response is received for an authorized ARP entry or if the DHCP server fails to update the entry by re-adding the entry for example, after 90 seconds elapse, the entry ages out. The DHCP server is then notified of this.

An authorized ARP entry can be removed manually or automatically by the DHCP server.

- ARP security

For the sake of security, authorized ARP provides the ARP security function to disable dynamic ARP learning. When you enable this function, only static ARP entries and authorized ARP entries are allowed to be populated into the ARP table, while dynamic ARP learning is prohibited.

ARP security is independent of authorized ARP, and can be employed independently.

2.5.3 Structure of the ARP Packet

ARP packets fall into two categories: ARP request and ARP response. The following table illustrates the structure of the ARP request and response. For an ARP request, the field of hardware address of the receiver (that is, the address the sender wants to obtain) is null, and all other fields are employed. An ARP response employs all the fields.

<table>
<tr><td colspan="2">Hardware type (16 bits)</td></tr>
<tr><td colspan="2">Protocol type (16 bits)</td></tr>
<tr><td>Length of the hardware address</td><td>Length of protocol address</td></tr>
<tr><td colspan="2">Operator (16 bits)</td></tr>
<tr><td colspan="2">Hardware address of the sender</td></tr>
<tr><td colspan="2">IP address of the sender</td></tr>
<tr><td colspan="2">Hardware address of the receiver</td></tr>
<tr><td colspan="2">IP address of the receiver</td></tr>
</table>

Figure 2-2 Structure of the ARP request and ARP response

- Hardware type: Identifies the type of the hardware interface. The following table lists the valid values.

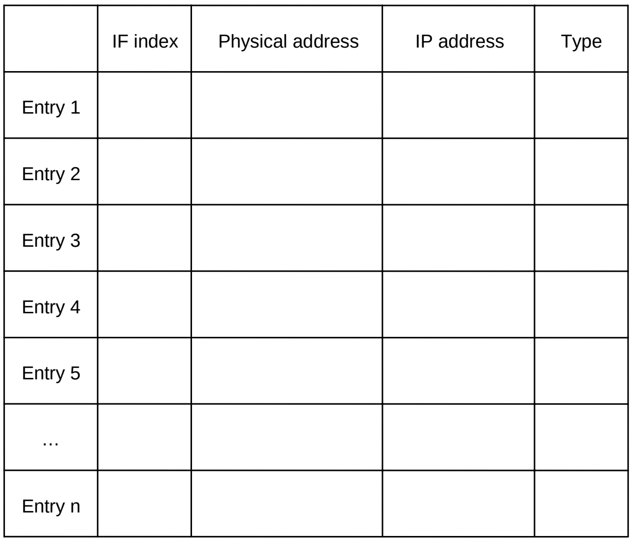
Table 2-9 Valid hardware interface types

Type	Description
1	Ethernet
2	Experimental Ethernet
3	X.25
4	Proteon ProNET
5	Chaos
6	IEEE802.X
7	ARC network

- Protocol type: Identifies the type of the protocol used by the sending device. In TCP/IP, it is usually EtherType.
- Length of the hardware address: Number of bytes in the hardware address.
- Length of protocol address: Number of bytes in the protocol address.

- Operator: Indicates whether the ARP packet is an ARP request or an ARP response. It can be 1 (for ARP request), 2 (for ARP response), 3 (for RARP request), or 4 (for RARP response).
- Hardware address of the sender: Hardware address of the sending device.
- IP address of the sender: IP address of the sending device.
- Hardware address of the receiver: Hardware address of the receiving device. In an ARP request, this field is null. In an ARP response, this field carries the hardware address of the receiver.
- IP address of the receiver: IP address of the receiving device.

2.5.4 ARP Table



	IF index	Physical address	IP address	Type
Entry 1				
Entry 2				
Entry 3				
Entry 4				
Entry 5				
…				
Entry n				

Figure 2-3 ARP table

- IF index: Physical interface or port on the device owning the physical address and IP address.
- Physical address: Physical address of the device, that is, the MAC address.
- IP address: IP address of the device.
- Type: Type of the entry, which can be 2 for an invalid entry, 3 for a dynamically learned entry, 4 for a statically configured entry, or 1 for an entry falling out of the previous three cases.

2.5.5 Fundamentals of Authorized ARP

The authorized ARP mechanism is a combination of the ARP mechanism and the DHCP mechanism. Currently, authorized ARP does not support DHCP relay. The following explains the operation of authorized ARP in a scenario with the DHCP clients and DHCP servers on the same segment:

1) A DHCP client broadcasts a DHCP_DISCOVER packet. When a DHCP server receives the broadcast packet, it responds with a DHCP_OFFER packet, in which the DHCP server fills the configuration parameters for the DHCP client.
2) If more than one DHCP server is present on the network and responds to the client, the client accepts the configuration parameters in the first received DHCP_OFFER packet and broadcasts a DHCP_REQUEST packet on the network. The DHCP_REQUEST packet contains the MAC address of the client and the IP address the client is ready to use.
3) After a DHCP server receives the DHCP_REQUEST packet of a client, it responds to the client with a DHCP_ACK packet. At the same time, the DHCP server adds an authorized ARP entry into the local ARP table, which contains the MAC address and IP address of the client, and the interface owning the addresses.
4) Once an authorized ARP entry is added into the ARP table of the DHCP server, the ARP ping mechanism is initiated to implement the aging of the authorized ARP entry. That is, ARP ping periodically sends an ARP request to the IP address of the client recorded in the authorized ARP entry to determine whether the client is down. If ARP ping sends three ARP requests but receives no response, it considers that the client is down, and then removes the authorized ARP entry from the ARP table.
5) For the sake of security, authorized ARP provides the ARP security function. When you enable this function, only static ARP entries and authorized ARP entries are allowed to be populated into the ARP table, while dynamically learned ARP entries are prohibited. Therefore, if the DHCP server acts as the gateway for accessing the Internet, illegal hosts with fixed addresses will not be able to access the Internet.

2.5.6 Configuring Authorized ARP

I. Configuration Prerequisites

Before configuring authorized ARP, complete the following configurations:

- Enable the DHCP server function on the router acting as the DHCP server, and configure the DHCP server parameters such as address pool.
- Configure the clients to obtain IP addresses through DHCP.

II. Configuring Authorized ARP

The following tables describe the authorized ARP configuration tasks, which must be performed on the DHCP server.

1) Enable authorized ARP in system view

Table 2-10 Enable authorized ARP for DHCP interface address pools

Operation	Command	Remarks
Enter system view	**system-view**	—
Configure interfaces to operate in DHCP server mode and specify to allocate addresses from interface address pools	**dhcp select interface** { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	Required
Enable authorized ARP for DHCP interface address pools	**dhcp server synchronize arp** { **interface** *interface-type interface-number* [**to** *interface-type interface-number* | **all** }	Required. By default, authorized ARP is not enabled.
Enter interface view	**interface** *interface-type interface-number*	Before creating an interface address pool, you must configure the IP addresses of the interfaces involved in the previous commands.
Configure the IP address of the interface	**ip address** *ip-address net-mask*	
Enable ARP security	**arp security**	Optional. By default, ARP security is disabled.
Configure the aging time of the authorized ARP entries	**arp security time-out** *seconds*	Optional. By default, the aging time of an authorized ARP entry is 90 seconds.

🕮 **Note:**

- This mode applies to scenarios where addresses from the interface address pools are assigned to clients.
- In this configuration mode, you can configure an interface range. Therefore, you can configure DHCP to support authorized ARP on multiple interfaces at the same time.

2) Enable authorized ARP in interface view

Table 2-11 Enable authorized ARP for DHCP interface address pools

Operation	Command	Remarks
Enter system view	**system-view**	—

Operation	Command	Remarks
Enter interface view	**interface** *interface-type interface-number*	—
Configure the IP address of the interface	**ip address** *ip-address net-mask*	—
Configure the interface to operate in DHCP server mode and specify to allocate addresses from interface address pools	**dhcp select interface**	Required
Enable authorized ARP for DHCP interface address pools	**dhcp server synchronize arp**	Required. By default, authorized ARP is not enabled.
Enable ARP security	**arp security**	Optional. By default, ARP security is disabled.
Configure the aging time of the authorized ARP entries	**arp security time-out** *seconds*	Optional. By default, the aging time of an authorized ARP entry is 90 seconds.

Note:

- This mode applies to scenarios where addresses from the interface address pools are assigned to clients.
- In this configuration mode, you may configure DHCP to support authorized ARP in interface view. Therefore, this mode is suitable when you want to configure a single interface to support authorized ARP.

3) Enable authorized ARP in DHCP global address pool view

Table 2-12 Enable authorized ARP for DHCP global address pools

Operation	Command	Remarks
Enter system view	**system-view**	—
Configure the interface to operate in DHCP server mode and specify to allocate addresses from global address pools	**dhcp select global** [**subaddress**] | **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	Required
Enter DHCP address pool view	**dhcp server ip-pool** *pool-name*	Required

Operation	Command	Remarks
Enable authorized ARP for global DHCP address pools	**synchronize arp**	Required. By default, authorized ARP is not enabled.
Exit to system view	**quit**	—
Enter interface view	**interface** *interface-type interface-number*	—
Enable ARP security	**arp security**	Optional. By default, ARP security is disabled.
Configure the aging time of the authorized ARP entries	**arp security time-out** *seconds*	Optional. By default, the aging time of an authorized ARP entry is 90 seconds.

📖 **Note:**

This mode applies to scenarios where addresses from the global address pools are assigned to clients.

⚠ **Caution:**

- Only when you configure the ARP security function, can ARP ping start to work. If ARP ping is not working, an authorized ARP entry will never be removed, even if it has timed out.
- If an authorized ARP entry is in the ARP table already when you configure the **arp security** command, the aging time of the entry will be refreshed.
- If you configure the **arp security time-out** command directly without configuring the **arp security** command, the aging time configuration is accepted but takes no effect.

2.5.7 Authorized ARP Configuration Example

I. Network requirements

- DHCP clients obtain IP addresses through a DHCP server.
- The router with the DHCP server function enabled supports authorized ARP, and the aging time of the authorized ARP entries is 120 seconds.
- Ethernet interface Ethernet1/0/0 on the DHCP server, that is, the interface connected to the clients, has an IP address of 10.1.1.1/24. Ethernet interface

Ethernet1/0/1, that is, the interface for accessing the Internet has an IP address of 10.1.2.1/24. The DHCP server is configured with global address pool 10.1.1.0/24.

- The DHCP server acts as the proxy gateway server for clients to access the Internet at the same time.

II. Network diagram

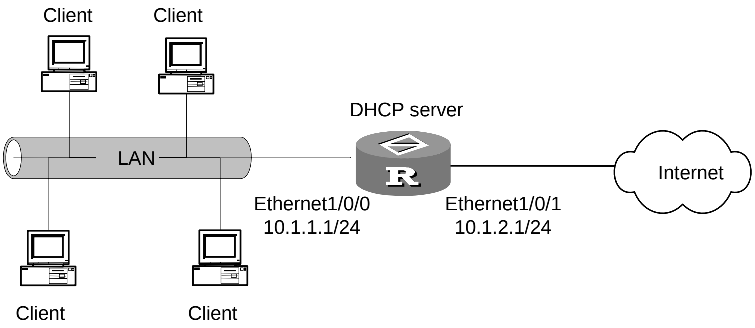


Figure 2-4 Network diagram for authorized ARP

III. Configuration procedure

# Enable DHCP.

```
[3Com] dhcp enable
```

# Configure interfaces to operate in DHCP server mode, and assign IP addreses from a global address pool.

```
[3Com] dhcp select global interface ethernet 1/0/0 to ethernet 1/0/1
```

# Configure the network parameters and address pool on the DHCP server.

```
<3Com> system-view
[3Com]interface Ethernet 1/0/0
[3Com-Ethernet1/0/0] ip address 10.1.1.1 255.255.255.0
[3Com-Ethernet1/0/0] quit
[3Com] interface Ethernet 1/0/1
[3Com-Ethernet1/0/1] ip address 10.1.2.1 255.255.255.0
[3Com-Ethernet1/0/1] quit
[3Com] dhcp server ip-pool 0
[3Com-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
```

# Enable authorized ARP for the DHCP global address pool.

```
[3Com-dhcp-pool-0] synchronize arp
[3Com-dhcp-pool-0] quit
```

# Enable ARP security, and configure an aging time of 120 seconds for authorized ARP entries.

```
[3Com-Ethernet1/0/0] arp security
[3Com-Ethernet1/0/0] arp security time-out 120
```

```
[3Com-Ethernet1/0/0] quit
```

Chapter 3 DNS Configuration

3.1 DNS Overview

TCP/IP not only provides IP address to specify devices, but also specially designs a kind of host naming mechanism called DNS (Domain Name System) in the form of character string. Adopting a hierarchical naming system, the DNS designates a meaningful name for the device in the Internet and associate the domain name with IP address with the help of the domain name resolution server. In this way, the user can use domain names that are easy to memorize and meaningful, and never needs to keep obscure IP addresses in mind.

There are two kinds of domain name resolutions, namely static domain name resolution and dynamic domain name resolution, which supplement each other in real application. On resolving a domain name, use the static resolution first. If it fails, use the dynamic resolution method. Some common domain names can be put into the static domain name resolution table to raise the domain name resolution efficiency greatly.

- Static resolution: To create the corresponding relationship between domain name and the IP address manually. When the client needs the IP address related to the domain name, it will search the specific domain name in the static domain name resolution table to obtain the corresponding IP address.
- Dynamic resolution: To receive the domain name resolution request lodged by the client with special domain name resolution server. The server first performs resolution within the local database. If it judges that the domain name does not belong to the local domain, it will forward the request to the upper level domain name resolution server until the resolution is finished. The resolution results, being either IP address or non-existed domain name, will be returned to the client.

3.2 Static Domain Name Resolution Configuration

3.2.1 Configuring Static Domain Name Resolution

The router performs static DNS by consulting a static DNS table containing domain name to IP address associations in common use. This table is similar to the hosts file on a Windows 9X OS. It allows users to use user-friendly hostnames rather than IP addresses to reach hosts.

Perform the following configuration in system view.

Table 3-1 Add or delete mapping entry in static domain name resolution table

Operation	Command
Add the mapping between domain name and IP address	**ip host** *hostname ip-address*
Delete the mapping between domain name and IP address	**undo ip host** *hostname* [*ip-address*]

Hostname to IP address associations are one-to-one associations. The IP address assigned to a hostname will overwrite the previous one, if there is any.

3.2.2 Displaying and debugging domain name resolution table

After the above configuration, execute the **display** command in all views to display the running of domain name resolution table, and to verify the effect of the configuration.

Table 3-2 Display and debug domain name resolution table

Operation	Command
Display static domain name resolution table	**display ip host**

3.3 DNS Client Configuration

3.3.1 Introduction to the Architecture of DNS

IP addresses, 202.112.131.109 for example, are 32 bits long and as such are difficult for human beings to memorize. To make it easier to memorize addresses, most organizations replace IP addresses with domain names, that is, abbreviations or meaningful names, www.sina.com.cn for example. To map a domain name to an IP address, you need a resolver and a domain name system (DNS) server.

DNS is a distributed database that applies to TCP/IP application programs. It functions to resolve between hostnames and IP addresses and provide email routing information. In applications, access to the DNS server is provided by an address resolver. The DNS client can accomplish the function of a resolver by translating between IP addresses and domain names of hosts.

This is how DNS operates:

1) First, a user program sends a request to the DNS client.
2) Upon receipt of this request, the DNS client looks up the local database; if no match is found, it sends a query to the name server.
3) After receiving the response sent back by the name server, the DNS client resolves the response packet and based on the packet contents decides its operation.

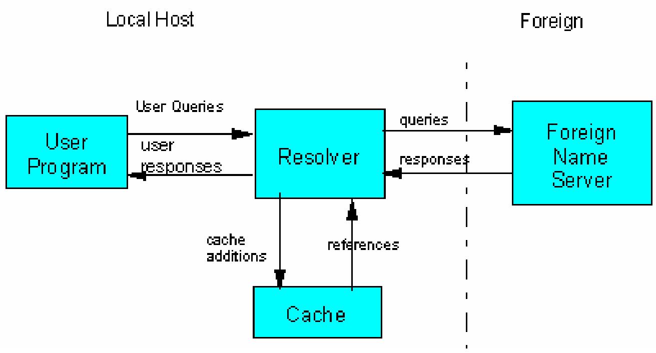


Figure 3-1 DNS system components

Figure 3-1 illustrates the process of DNS resolving:

1) The user program queries the resolver for a domain name or IP address.
2) Upon receipt of the query, the resolver first looks up the local cache. If the requested map entry is found, it directly replies. If not, it assembles a query packet appropriate to the query type, that is, whether IP address or domain name is needed. This packet can take TCP or UDP format, but in this program UDP is adopted.
3) Then, based on its DNS configuration, the resolver sends the query packet to port 53 on the default DNS server (the foreign name server in this scenario).
4) After receiving the response, the resolver resolves the response packet and replies to the user.

In this scenario, resolver and its cache are called DNS client and as a whole function to accept and respond to the DNS queries of user programs. Normally, the user program and resolver are on the same host whereas the foreign name server can be located on that same host or more likely on a different one.

3.3.2 Configuring the DNS Client

Following are the DNS client configuration tasks:

- Enable DNS resolving
- Configure IP address of the DNS server
- Configure the DNS domain name searching list

Where, you must enable DNS resolving and provide IP address of the DNS server. You need only to enable DNS resolving, however, if the interfaces on the device use IP addresses assigned by a DHCP client and the address of the DNS server and the domain name are included in the information that the DHCP server issues to the device.

I. Enabling DNS Resolving

To use the DNS client function, enable DNS resolving on the device first.

Perform the following configuration in system view.

Table 3-3 Enable/disable DNS resolving

Operation	Command
Enable DNS resolving.	**dns resolve**
Disable DNS resolving.	**undo dns resolve**

By default, DNS resolving is disabled.

II. Configuring IP Address of the DNS Server

To resolve domain names, the DNS client must know the domain server address where it can send queries.

Perform the following configuration in system view.

Table 3-4 Configure IP address of the DNS server

Operation	Command
Configure IP address of the DNS server.	**dns server** *ip-address*
Delete IP address of the DNS server.	**undo dns server** [*ip-address*]

III. Configuring the DNS Domain Name Searching List

Some of the websites that you access may have the same domain name, such as sina.com.cn, huawei.com.cn, and sohu.com.cn.

To facilitate website searching of users, you can set a domain name to com.cn for example. Thus, to search for the IP address mapped with "sina.com.cn", a user only needs to enter the command **ping sina**. If no response is received, the DNS client sends a request to query the IP address mapped with “sina”.

You can configure a DNS domain name searching list by using the following command repeatedly.

Perform the following configuration in system view.

Table 3-5 Configure a DNS domain name

Operation	Command
Configure a DNS domain name.	**dns domain** *domain-name*
Delete one or all DNS domain names.	**undo dns domain** [*domain-name*]

📖 **Note:**

RFC1034, however, uses a different searching approach: when you input the **ping sina** command, the DNS client first queries the IP address mapped to “sina”. And if no response is received, it then queries the IP address mapped to “sina.com.cn”.

3.3.3 Displaying and Debugging DNS Client Information

I. Displaying the DNS client information

Perform the following operation in any view.

Table 3-6 Display the DNS client information

Operation	Command
View whether DNS resolving is enabled	**display current-configuration**
Display the configurations of the DNS server	**display dns server** [**dynamic**]
Display the configurations of the DNS domain name searching list	**display dns domain** [**dynamic**]
Display contents of the dynamic domain name buffer	**display dns dynamic-host**
Display the domain name or IP address resolved from the specified IP address or domain name	**nslookup type** { **ptr** *ip-address* | **a** *domain-name* }

📖 **Note:**

Execute the **display dns server dynamic** command to view DNS server addresses that are dynamically obtained through DHCP or by other means.

II. Clearing the domain name cache

The DNS client retains the result of each successful domain name resolution in its cache. If it receives the same resolving request later, it first looks up the cache for a match. And if no match is found, it sends a domain name resolving request to the DNS server.

You can clear the current cache using the following command.

Perform the following operation in user view.

Table 3-7 Clear the dynamic domain name cache

Operation	Command
Clear the dynamic domain name cache.	**reset dns dynamic-host**

III. Debugging the DNS client

Perform the following operation in user view.

Table 3-8 Debug the DNS client

Operation	Command
Enable DNS client debugging.	**debugging dns**
Disable DNS client debugging.	**undo debugging dns**

By default, DNS client debugging is disabled.

3.3.4 Typical DNS Configuration Example

I. Networking rquirements

Enable DNS resolving on the router with the IP address 10.110.10.1. IP address of the DNS server is 10.110.66.66.

II. Network diagram

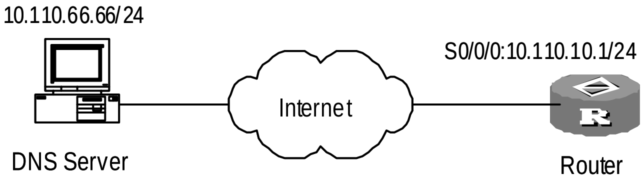


Figure 3-2 Network diagram

III. Configuration procedure

1) Configure the router

# Enable DNS resolving.

```
[Router] dns resolve
```

# Configure IP address of the DNS server.

```
[Router] dns server 10.110.66.66
```

# Configure IP address of the interface S0/0/0.

```
[Router] interface s 0/0/0
[Router-s0/0/0] ip address 10.110.10.1 255.255.255.0
```

Configure a static route to the DNS server.

```
[Router] ip route-static 10.110.66.66 s0
```

3.3.5 Troubleshooting

Symptom: Domain name resolving failed.

Solution:

1) Check the software, making sure that:

- IP address of the domain name server is correctly configured.
- The device and the domain name server have routes between them.
- DNS resolving is enabled.

2) Check the hardware, making sure the network connection cable is in good condition and securely connected.

3.4 DNS Proxy Configuration

3.4.1 Introduction to DNS Proxy

DNS proxy is enabled on the router functioning as the gateway proxy for a LAN. It allows clients on the LAN to contact an external DNS server for service when accessing the Internet in case no internal DNS server is present.

3.4.2 Operational Mechanism of DNS Proxy

The following describes how DNS proxy operates:

1) The DNS client sends a DNS request to the DNS proxy, using the IP address of the DNS proxy as the destination address.
2) When the DNS proxy receives the request, it replaces the destination address with the IP address of a DNS server, and then forwards the request to the DNS server. When multiple DNS server addresses are available, the DNS proxy sends the request to the one configured first. If no response is received, the DNS client resends the request and the DNS proxy forwards this resent request to the second DNS server. This process continues until a response is received from a DNS server.
3) The DNS server sends a response back to the DNS proxy.
4) The DNS proxy replaces the source IP address in the received response with the its own IP address and forwards the response to the DNS client.

Now, the DNS client can use the IP address carried in the received response to access the Internet.

3.4.3 Configuring DNS Proxy

I. Configuration prerequisites

Before configuring DNS proxy, make sure that

- IP addresses of DNS servers are available on the DNS proxy.
- The gateway enabled with DNS proxy is specified as the DNS server on the DNS client.
- The DNS client and the DNS server are reachable to the DNS proxy.

II. Configuring DNS proxy

Configure DNS proxy on the router functioning as the gateway.

Table 3-9 Configure DNS proxy

Operation	Command	Remarks
Enter system view	**system-view**	—
Enable DNS proxy	**dns-proxy enable**	Required

3.4.4 DNS Proxy Configuration Example

I. Network requirements

PCs on network segment 10.1.1.0/24 where no DNS server is present may obtain DNS service from an external DNS server, for example, the one with IP address 10.72.66.36/24. To this end, the gateway router must support DNS proxy.

II. Network diagram

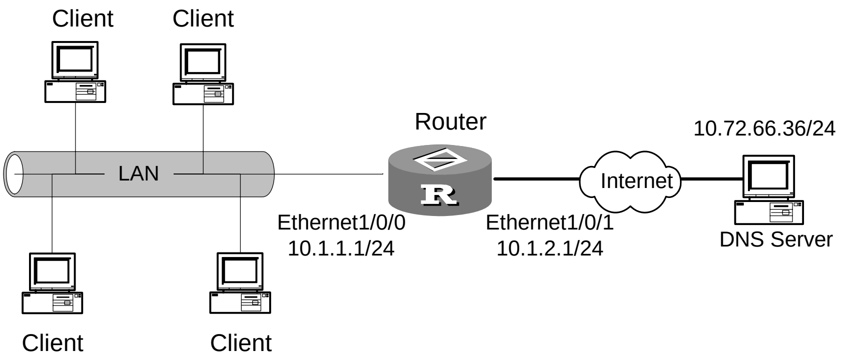


Figure 3-3 Network diagram for DNX proxy configuration

III. Configuration example

1) Configure the router

# Assign an IP address to interface Ethernet 1/0/0.

```
[3Com] interface Ethernet 1/0/0
[3Com-Ethernet 1/0/0] ip address 10.1.1.1 255.255.255.0
```

# Configure NAT, allowing the client to access the Internet by using DNS proxy.

```
[3Com] acl number 2000
[3Com-acl-basic-2000] rule 0 permit source 10.1.1.0 0.0.0.255
[3Com-acl-basic-2000] quit
[3Com] interface Ethernet 1/0/1
[3Com-Ethernet1/0/0] ip address 10.1.2.1 255.255.255.0
[3Com-Ethernet1/0/0] nat outbound 2000
[3Com-Ethernet1/0/0] quit
```

# Enable DNS proxy.

```
[3Com] dns-proxy enable
```

# Configure the IP address of the DNS server.

```
[3Com] dns server 10.72.66.36
```

# Configure routing, ensuring that the DNS client and the router are reachable to each other.

```
Omitted
```

2) Configure the PC

Set gateway and DNS server addresses to 10.1.1.1.

Chapter 4 DDNS Configuration

4.1 Introduction to DDNS

Dynamic domain name service (DDNS) is to set up bindings between static domain names and dynamic IP addresses of the hosts using the domain names.

As shown in Figure 4-1, Server A is an HTTP or FTP server connected to Router A to gain access to the Internet. When Server A obtains IP address through DHCP or connects to the Internet through PPPoE, PPTP or L2TP, its IP address is dynamic, meaning its IP address may change each time the connection is initialized.

The DNS server providing service to Server A maintains a static domain name-to-IP address binding for Server A. As this binding does not alter as the IP address changes, Internet users cannot reach Server A by using its domain name once the server’s IP address changes.

To help the DNS server maintain a binding between static domain name and dynamic IP address for Server A, you may use DDNS. This allows Internet users to reach Server A by its domain name despite the change of its IP address.

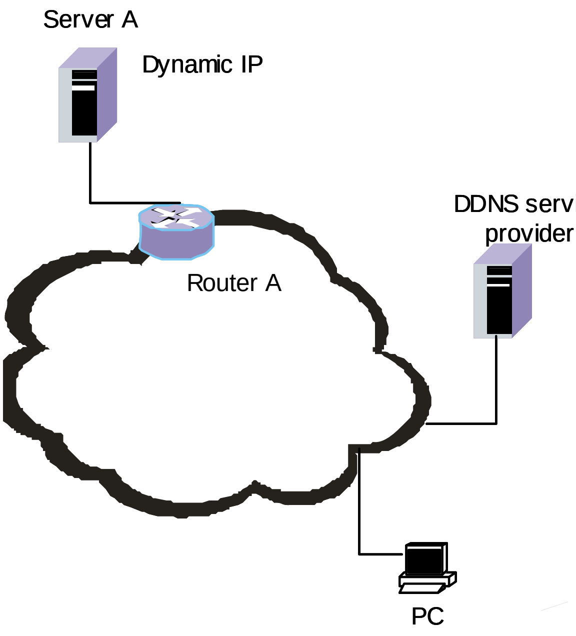


Figure 4-1 Network diagram for DDNS application

DDNS is divided into user side and service provider side.

- User side of DDNS

Usually, the user side of DDNS is a server providing HTTP, FTP, or other services. After the IP address of the server changes, the server needs to request the DDNS service provider to notify the DNS server of this. This is usually done by using a special client program provided by the DDNS service provider or through a specified HTTP page.

The domain name-to-IP address mapping update process does not follow a particular protocol; it varies by DDNS service provider.

- Service provider side of DDNS

After receiving an IP address update request from the user side, the DDNS service provider notifies the DNS server to update the involved domain name-to-IP address mapping.

At present, www.3322.org is the only DDNS service provider supported by 3Com Series Routers.

3Com Series Routers implement the user side of DDNS. When DDNS users' IP addresses change, 3Com Routers can request www.3322.org to notify DNS servers to update domain name-to-IP address mappings.

4.2 Configuring DDNS

4.2.1 Configuration Prerequisites

Before configuring DDNS on your router, make sure that:

- The router can obtain DNS service.
- On the DNS server, a domain name-to-IP address mapping entry has created for the domain name of the DDNS service provider, which can be www.3322.org only at present.

This is to ensure that your router can access the DDNS service provider.

4.2.2 Configuring DDNS

Table 4-1 Configure DDNS

Operation	Command	Remarks
Enter system view	**system-view**	--
Set 3322.org as the DDNS service provider and enter its view	**ddns-server 3322.org**	--
Set parameters for accessing the DDNS service provider	Refer to section 4.2.3 "Configuring Parameters for Accessing the DDNS Service Provider"	Required

Operation	Command	Remarks
Configure a domain name whose domain name-to-IP address mapping on DNS needs update by using the service of the DDNS service provider	**ddns domainname** *name*	Required
Request the DDNS service provider to notify the DNS server that the bound IP address of the domain name specified by the **ddns domainname** command has changed	**ddns refresh**	Required

4.2.3 Configuring Parameters for Accessing the DDNS Service Provider

Table 4-2 Configure parameters for accessing the DDNS service provider

Operation	Command	Remarks
Enter system view	**system-view**	--
Set 3322.org as the DDNS service provider and enter its view	**ddns-server 3322.org**	--
Set the user name used for accessing the DDNS service provider	**ddns username** *name*	Required
Set the password used for accessing the DDNS service provider	**ddns password** *password*	Required
Set the interface used for accessing the DDNS service provider	**ddns source-interface** *interface-type interface-number*	Required

4.2.4 DDNS Configuration Example

I. Network requirements

As shown in the following figure, Server A obtains IP address dynamically through DHCP service of Router A. It provides the WWW service at www.abc123.com to Internet users.

II. Network diagram

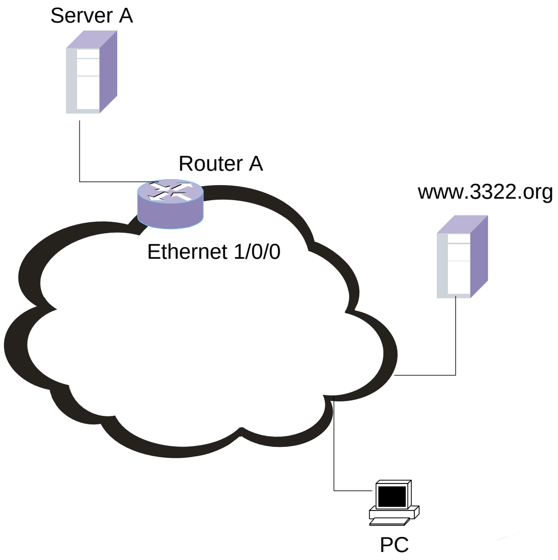


Figure 4-2 Network diagram for DDNS application

III. Configuration procedure

# Enter system view.

```
<3Com> system-view
```

# Set 3322.org as the DDNS service provider and enter its view.

```
[3Com] ddns-server 3322.org
```

# Set the user name used for accessing the DDNS service provider to user.

```
[3Com-ddns-3322.org] ddns username user
```

# Set the password used for accessing the DDNS service provider to pass.

```
[3Com-ddns-3322.org] ddns password pass
```

# Set the interface used for visiting the DDNS service provider to Ethernet 1/0/0.

```
[3Com-ddns-3322.org] ddns source-interface ethernet 1/0/0
```

# Configure domain name www.abc123.com, allowing its domain name-to-IP address mapping on DNS to be updated by using the service of the DDNS service provider.

```
[3Com-ddns-3322.org] ddns domainname www.abc123.com
```

# Request the DDNS service provider to notify the DNS server that the bound IP address of domain name www.abc123.com has changed.

```
[3Com-ddns-3322.org] ddns refresh
```

Chapter 5 URPF Configuration

5.1 URPF Overview

Unicast Reverse Path Forwarding (URPF) serves as a safeguard against source address based network attacks.

In source address spoofing attacks, attackers create a series of packets with forged source addresses. For applications using IP address based authentication method, this type of attack allows unauthorized users to access the system in the name of other users, or even access as root. Even the response packets cannot reach the attackers; it is disruptive to the attacked target.

There are generally two types of URPF check: strict check and loose check. It also supports ACL and default route check.

The procedures of the URPF check are as follows:

1) When the packet's source address is in the router's FIB table:

- **Strict** check: Searches reversely for outgoing interfaces for the packet. At least one outgoing address must match the packet's incoming interface; otherwise URPF rejects the packet.
- **Loose** check: The only requirement is that the packet's source address is in the router's FIB table.

2) If the packet's source address is not in the router's FIB table, then it checks the default route and the **allow-default** parameter.

Note:

The default route refers to the one configured on the router visited by the packet.

- In cases when only the default route is configured (the **allow-default** parameter is not configured), a packet is discarded if its source address is not in the router's FIB table in both the strict check and the loose check.
- In cases when both the default route and the **allow-default** parameter are configured: in strict URPF check, the packet is forwarded if its incoming interface matches the outgoing interface of the default route; otherwise, the packet is rejected. In loose URPF check, URPF pass and forward all the packets.

Finally, only when the packet is rejected by URPF will it match the ACL list. If ACL passes the packet, then the packet is forwarded; if ACL rejects the packet, then the packet is discarded.

Note:

URPF does not support fast forwarding. If a fast forwarding table exists, the result of a URPF check does not take effect. Thus, even a packet fails to pass URPF check, it is forwarded all the like.

5.2 URPF Configuration

Perform the following configuration in interface view.

Table 5-1 Enable/disable URPF check

Operation	Command
Enable URPF check	**ip urpf** { **strict** | **loose** } [**allow-default**] [**acl** *acl-number*]
Disable URPF check	**undo ip urpf**

By default, URPF check is disabled.

5.3 PRPF Display and Debugging

Perform the following configuration in user view.

Table 5-2 Display URPF discarded packets

Operation	Command
Display URPF discarded packets	**debugging ip urpf discards** [**interface** *interface-type interface-number*]
Cancel the display of URPF discarded packets	**undo debugging ip urpf discards** [**interface** *interface-type interface-number*]

Chapter 6 IP Accounting Configuration

6.1 Introduction to IP Accounting

IP Accounting counts inbound and outbound IP packets on the router. These IP packets include those sent and forwarded normally as well as those denied by the firewall.

The statistics of the IP Accounting provide information about source and destination IP addresses, protocol number, packet sum, and byte sum. The statistics are sorted into different tables for display depending on whether IP packets pass the firewall and whether they match IP accounting rules.

Each IP accounting rule consists of an IP address and its mask. The rule list records network segment addresses, which are the results of ANDing IP addresses with their masks. An IP packet is sorted as follows:

- If the source or destination IP address of the IP packet matches a network segment address in the rule list, the packet is recorded in an interior hash table as a valid packet (a packet not filtered out by the firewall) matching the rule. Otherwise, the packet is recorded in an exterior hash table as a valid packet not matching the rule.
- If the packet is filtered out by the firewall configured on the interface when it reaches a router, it is recorded in the firewall-denied hash table as an invalid packet.

6.2 IP Accounting Configuration

To configure IP accounting, first enable it, and then specify one or more types of packets to be counted on an interface. After that, the router can start counting IP packets.

6.2.1 Preparations for IP Accounting Configurations

You have assigned an IP address and mask to the interface, on which packets are to be counted. In addition, a firewall is configured on the interface.

6.2.2 IP Accounting Configuration Tasks

The following sections describe IP accounting configuration tasks:

Table 6-1 IP accounting configuration tasks

Operation	Command	Remarks
Enter system view	**system-view**	—

Operation	Command	Remarks
Enable IP accounting	**ip count enable**	Required
Set an aging time	**ip count timeout** *minutes*	Optional (720 minutes by default)
Set the maximum length of the interior hash table	**ip count interior-threshold** *number*	Optional (512 by default)
Set the maximum length of the exterior hash table	**ip count exterior-threshold** *number*	Optional (0 by default)
Add IP accounting rules	**ip count rule** *ip-address net-mask*	Required. If no rule is set, no packet matches rules.
Enter interface view	**interface** *interface-type interface-number*	Required
Specify the type of packets to be counted on the interface	**ip count** [**firewall-denied**] { **inbound-packets** | **outbound-packets** }	Required.
Display the IP accounting rule list	**display ip count rule**	You may execute the **display** command in any view.
Display IP accounting information	**display ip count** { **inbound-packets** | **outbound-packets** } { **interior** | **exterior** | **firewall-denied** }	Execute the **display** command in any view.

⚠ **Caution:**

- If the IP accounting function is configured on interfaces but no IP accounting rule exists, you must set the length of the exterior hash table to be greater than zero by using the **ip count exterior-threshold** *number* command. If the *number* argument is set to 50, the IP Accounting may count up to 50 IP packets with different combinations of source and destination.
- The IP packets with the same source and destination are counted in the same entry. For legitimate IP packets, they are further classified and then saved by protocol number. For illegitimate packets, no further classification is performed; their protocol information is omitted, and only packet sum and byte sum are recorded.
- You may configure up to 32 IP accounting rules.

6.2.3 IP Accounting Configuration Example

I. Network requirements

As shown in Figure 6-1, the router is connected to two hosts through Ethernet ports. Count the IP packets from PC1 to PC2, with the aging time for table entries as 24 hours.

II. Network diagram

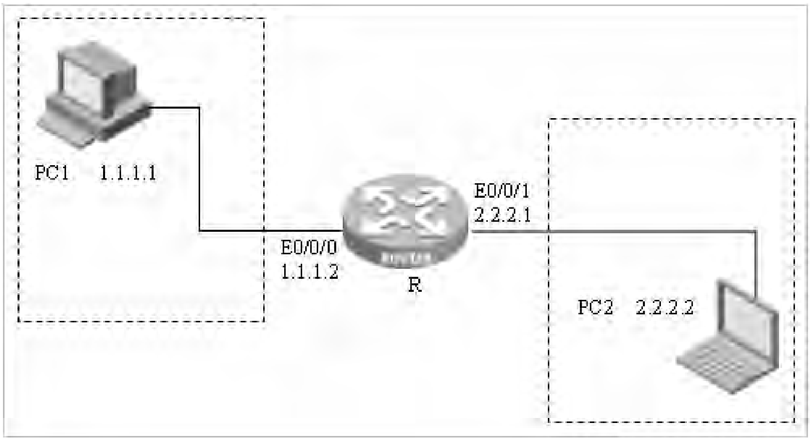


Figure 6-1 Network diagram for IP accounting configuration

III. Configuration procedure

# Enable IP accounting.

```
[3Com] ip count enable
```

# Enter system view, and configure an IP accounting rule.

```
[3Com] ip count rule 1.1.1.1 24
```

# Configure the aging time as 1,440 minutes (24 hours).

```
[3Com] ip count timeout 1440
```

# Set the maximum length of the interior hash table to 100.

```
[3Com] ip count interior-threshold 100
```

# Set the maximum length of the exterior hash table to 20.

```
[3Com] ip count exterior-threshold 20
```

# Enter the interface view of Ethernet 0/0/0; assign the interface an IP address and configure the IP Accounting to count both inbound and outbound IP packets on it.

```
[3Com] interface Ethernet 0/0/0
[3Com-Ethernet0/0/0] ip address 1.1.1.2 24
[3Com-Ethernet0/0/0] ip count inbound-packets
[3Com-Ethernet0/0/0] ip count outbound-packets
[3Com-Ethernet0/0/0] quit
```

# Enter the view of Ethernet 0/0/1 and assign it an IP address.

```
[3Com] interface Ethernet 0/0/1
[3Com-Ethernet0/0/1] ip address 2.2.2.1 24
```

# Configure static routes on PC1 and PC2 for them to reaching each other. Ping PC2 on PC1.

# Display IP accounting information.

```
[3Com] display ip count inbound-packets interior
 Inbound packets information in interior list:
  SrcIP           DstIP           Protocol  Pkts        Bytes
  1.1.1.1         2.2.2.2         ICMP      4           240
[3Com] display ip count outbound-packets interior
 Outbound packets information in interior list:
  SrcIP           DstIP           Protocol  Pkts        Bytes
  2.2.2.2         1.1.1.1         ICMP      4           240
```

Note:

The two hosts can be replaced by other types of network devices such as routers.

6.3 Displaying and Maintaining IP Accounting Configuration

Execute the **display** commands in any view to display IP accounting configuration.

Table 6-2 Display and maintain IP accounting configuration

Operation	Command	Remarks
Display configuration information	**display this**	You can execute the command in system or interface view to view the configured commands.
Display the IP accounting rule list	**display ip count rule**	You can execute the command in any view.
Display IP accounting information	**display ip count** { **inbound-packets** | **outbound-packets** } { **interior** | **exterior** | **firewall-denied** }	You can execute the command in any view.

6.4 Tips for Configuration

- When configuring an interior or exterior hash table, you need to clear the table first and then make configuration if the number of the entries in the table is greater than the configured or default value.
- The interior or exterior hash table contains information about the IP packets counted after IP accounting rules are configured. After you configure an IP accounting rule, some original rule-incompliant packets may match the rule. After that, information about these packets is to be saved in the interior hash table. The exterior table, however, possibly contains information about the packets counted with the same address before the rule is configured. The entry for these packets in the exterior hash table will be removed when the aging time expires.

Chapter 7 UDP Helper Configuration

7.1 Introduction to UDP Helper

UDP Helper functions to relay UDP broadcast packets to the specified server after converting them to unicast packets.

With UDP Helper enabled, the router decides whether to forward a received UDP broadcast packet based on its port number. If forwarding is required, the router modifies the destination IP address in the IP header and then relays the packet to the specified destination server. If not, the router passes the packet to the upper layer module. When relaying a BOOTP/DHCP response message, the router broadcasts it if the client requests that a broadcast response is desired; if otherwise, the router unicasts it.

7.2 UDP Helper Configuration

UDP Helper configuration tasks are described in the following sections:

- Enabling/Disabling UDP Helper
- Specifying by UDP Port Number which UDP Broadcast
- Configuring Destination Server

7.2.1 Enabling/Disabling UDP Helper

You can enable UDP helper to have the router forward the received UDP broadcast packets. As soon as this function is enabled, the router forwards the broadcast packets with the UDP port number 69, 53, 37, 137, 138, or 49 by default. In addition to these port numbers, you can configure the router to forward the broadcast packets with the specified UDP port number. Disabling this function disables the router to forward the broadcast packets with one of these UDP port numbers (specified or default).

Perform the following configuration in system view.

Table 7-1 Enable/disable UDP Helper

Operation	Command
Enable UDP Helper	**udp-helper enable**
Disable UDP Helper	**undo udp-helper enable**

By default, UDP Helper is disabled.

7.2.2 Specifying by UDP Port Number which UDP Broadcasts are forwarded

With UDP Helper enabled, the system by default unicasts the broadcast packets with the UDP ports listed in the following table. You can configure up to 256 UDP ports with UDP Helper.

Table 7-2 Default UDP ports

Protocol	UDP port number
Trivial file transfer protocol (TFTP)	69
Domain name system (DNS)	53
Time service	37
NetBIOS name server (NetBIOS-NS)	137
NetBIOS datagram server (NetBIOS-DS)	138
Terminal access controller access control system (TACACS)	49

Perform the following configuration in system view.

Table 7-3 Configure/disable the system to forward the UDP broadcasts with the specified UDP port number

Operation	Command
Configure the system to forward the UDP broadcasts with the specified UDP port number	**udp-helper port** { *port* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }
Disable the system to forward the UDP broadcasts with the specified UDP port number	**undo udp-helper port** { *port* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

Note that:

- Before you can specify by UDP port number which UDP broadcasts are forwarded, you must enable UDP Helper.
- The **dns**, **netbios-ds**, **netbios-ns**, **tacacs**, **tftp**, and **time** keywords represents the six default ports. When specifying a default port, DNS for example, you can specify its port number 53 directly or specifying the keyword **dns**.
- When displaying the information about UDP helper, the **display current-configuration** command displays the default UDP port numbers only when they are disabled to use UDP Helper.

7.2.3 Configuring Destination Servers

After enabling UDP helper in system view, you can configure one or multiple (up to 20) servers on an Ethernet interface to have the UDP broadcasts received on the interface forwarded to the server or servers.

Perform the following configuration in Ethernet interface view.

Table 7-4 Configure/delete the server to which UDP broadcasts are forwarded

Operation	Command
Configure the destination server to which the UDP broadcasts received on the interface are forwarded	**udp-helper server** *ip-address*
Delete the destination server to which the UDP broadcasts received on the interface are forwarded	**undo udp-helper server** [*ip-address*]

By default, no destination server is available.

7.3 Displaying and Debugging the UDP Helper Configuration

After completing the above configuration tasks, execute the **display** command in any view to view the destination servers available with UDP Helper and to verify the effect of the configurations.

Execute the **debugging** command in user view to debug UDP helper.

Table 7-5 Display and debug UDP Helper

Operation	Command
Display the destination servers associated with the specified or all Ethernet interfaces	**display udp-helper server** [**interface** *number*]
Enable UDP Helper debugging	**debugging udp-helper** { **event** | **packet** [**receive** | **send**] }
Disable UDP Helper debugging	**undo debugging udp-helper** { **event** | **packet** [**receive** | **send**] }

Chapter 8 BOOTP Client Configuration

8.1 Introduction to BOOTP Client

The bootstrap protocol (BOOTP) adopts the client/server model where the BOOTP client requests the server for an IP address.

The following is how the BOOTP client obtains an IP address from the BOOTP server:

- The BOOTP client sends a BOOTP request.
- Upon receipt of the request, the BOOTP Server sends back a reply with the allocated IP address.
- The BOOTP client obtains the IP address.

BOOTP messages are encapsulated in UDP. To ensure transmission reliability, the timeout retransmission mechanism is adopted. When the BOOTP client sends a request, a retransmission timer starts. If no reply is received when the timer times out, the client retransmits the request. The retransmission occurs every five seconds and up to three transmission attempts are allowed.

8.2 BOOTP Client Configuration

BOOTP client configuration includes only one task, which is described in the following subsection.

8.2.1 Configuring an Ethernet Interface to Obtain IP Address Using BOOTP

Perform the following configuration in Ethernet interface view.

Table 8-1 Configure the Ethernet interface to obtain IP address using BOOTP

Operation	Command
Configure the Ethernet interface to obtain IP address using BOOTP	**ip address bootp-alloc**
Disable the Ethernet interface to obtain IP address using BOOTP	**undo ip address bootp-alloc**

By default, the Ethernet interface does not use BOOTP to obtain IP address.

8.3 Displaying and Debugging BOOTP Client Configuration

After completing the above configuration, execute the **display** command in any view to display and verify your BOOTP configuration.

Table 8-2 Display and debug the BOOTP client configuration

Operation	Command
Display BOOTP client information	**display bootp client** [**interface** *interface-type interface-number*]

Chapter 9 DHCP Configuration

9.1 DHCP Overview

9.1.1 Introduction to DHCP

We are in a world where the scales of networks are ever-growing and their configurations are more and more complex, computers (such as laptop computers and wireless networks) are likely to move, and the available IP addresses are far from adequate for the ever-increasing number of computers. Dynamic Host Configuration Protocol (DHCP) was introduced in such a background.

Like Bootstrap Protocol (BOOTP), DHCP adopts the client/server communications model. In this model, it is client that requests the server for configurations, such as the assigned IP address, subnet mask, and default GateWay (GW). The server will return the configuration information appropriate to the request in accordance with the configured policy. Both BOOTP and DHCP packets are encapsulated with UDP and in the structures that are highly similar.

BOOTP is running in a relatively static environment in which each host has a fixed network connection and, for each host, administrators configure a BOOTP file that will keep the same for a relatively long time.

Compared to BOOTP, DHCP is improved in two aspects. Firstly, DHCP allows computers to obtain all the desired configuration information by using only one message; secondly, it allows computers to rapidly and dynamically obtain IP addresses rather than statically specifying an address for each host.

9.1.2 IP address allocation in DHCP

1) IP address allocation policy

The time durations different types of hosts occupying IP addresses are different. For example, servers are more likely to use fixed IP addresses for a long time, some hosts perhaps need to use some dynamic IP addresses for a long period of time too, but some individuals only need to use temporarily assigned IP addresses for a short period of time.

Commensurate with these demands, a DHCP server provides three types of IP address allocation policies:

- Manual allocation, with which fixed IP addresses are assigned to a small amount of special hosts such as World Wide Web (WWW) servers.

- Auto-allocation, with which fixed IP addresses are assigned to some hosts connected to networks for the first time and these hosts are allowed to use the addresses for a long period of time.
- Dynamic allocation, with which some addresses are “leased” to client hosts. In this case, the clients need to request for new addresses upon the expiration of the leases. In fact, the addresses assigned to most client hosts are dynamic addresses.

2) IP address allocation order

A DHCP server selects an IP address for a client in the following order:

- The static IP address bound with the MAC address of the client in the database of the DHCP server.
- The client’s previous IP address, that is, the address requested in the “Requested IP Addr Option” carried in the DHCP_Discover packet sent by the client.
- A new address allocated from the server's DHCP pool of available addresses. This address is the one found first in the address pool.
- If the DHCP server does not find an available address, it will look outdated leased IP address and then conflicting IP address to find a valid one for assignment. If the attempt fails, the server will report error.

9.2 DHCP Server

9.2.1 Application environment for DHCP server

DHCP servers are well-suited to the network where:

- The network size is large, manual configuration is not an easy job, and it is hard to centralize the management on the entire network.
- The number of IP addresses available to the hosts on the network is far from adequate and it is impossible to assign a fixed IP address to each host. So the hosts, being too many, have to obtain dynamic IP addresses from a DHCP server in this case. In addition, limitation is placed on the number of concurrent users.
- On networks, most hosts are not assigned fixed IP addresses except of a few of them.

9.2.2 Fundamentals of DHCP server

As shown in the following figure, a typical DHCP application network usually comprises a DHCP server and multiple clients (such as PCs and laptop computers).

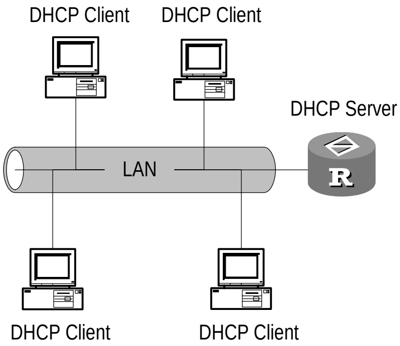


Figure 9-1 Network diagram for a DHCP server application

In order to obtain a valid dynamic IP address, a DHCP client should exchange different information with the server in different stages, three usual situations are:

1) First network access of DHCP client

In this case, the DHCP client should undergo four stages in order to set up a connection with a DHCP server.

- Discover stage where the DHCP client is searching for a DHCP server. In this stage, the client broadcast a DHCP_Discover packet on the network and only DHCP servers respond to it.
- Offer stage where DHCP servers offer IP addresses to the client. Upon receipt of the DHCP_Discover packet from the client, each DHCP server sends a DHCP_Offer packet carrying an unassigned IP address selected from its IP address pool to the client with other settings. To guarantee that the offered IP address is unique, each of them does an ARP probe before that.
- Selecting stage where the DHCP client picks one IP address out of all the offers. If the client receives offers from multiple DHCP servers, it only accepts the one reaching first. Then, it broadcasts a DHCP_Request packet containing the IP address, which was assigned and wrapped in the DHCP_Offer packet by DHCP server, to all the DHCP servers.
- Final check stage where the DHCP client checks the offered IP address. After receiving a DHCP_ACK packet, the client broadcasts an ARP packet destined to the offered IP address. If no response is received after a specified period of time, the client uses the IP address.
- Except for the selected DHCP server, all other DHCP servers can allocate their offered IP addresses to other requesting clients.

2) Non-first network access of DHCP client

If it is not the first time for the DHCP client to access the network, it should undergo the following procedure in order to set up a connection with a DHCP server.

- When a DHCP client that has a successful access record accesses the network again, it only needs to broadcast a DHCP_Request packet containing the IP address assigned to it the last time instead of sending a DHCP_Discover packet.

- Upon the receipt of the DHCP_Request packet, the DHCP server sends back a DHCP_ACK packet allowing the client to use the requested address if it is still unallocated.
- If the DHCP server has allocated that IP address to some other DHCP client or it is not available to the client for other reasons, the DHCP server sends back a DHCP_NAK packet. Upon the receipt of the packet, the client may send a new DHCP_Discover packet requesting a new IP address.

3) Renew the IP address lease

DHCP server takes back the dynamic IP address allocated to DHCP client when the lease expires. If DHCP client still wants to use this address, it should renew the IP address lease.

In practice, when the DHCP client starts or is at the half of the lease limit, it can send a DHCP_Request packet to DHCP server to complete lease renewal. If the current IP address is still valid, DHCP server returns DHCP_ACK packet to notify DHCP client that it has renewed the IP address lease.

4) Configure PC

Use the **ipconfig**/**release** command under DOS environment or run [winipcfg/release] at GUI (graphic user interface) to release an existing IP address. Then the user PC sends DHCP_Release packet to DHCP server. Use the **ipconfig** /**renew** command under DOS environment or run [winipcfg/renew] at GUI to request for new IP address. Now the user PC sends the DHCP_Discover packet to DHCP server.

You can also use the **ipconfig**/**renew** command on the user PC or run [winipcfg /renew] at GUI to renew the IP address lease.

The following figure presents the procedures described above:

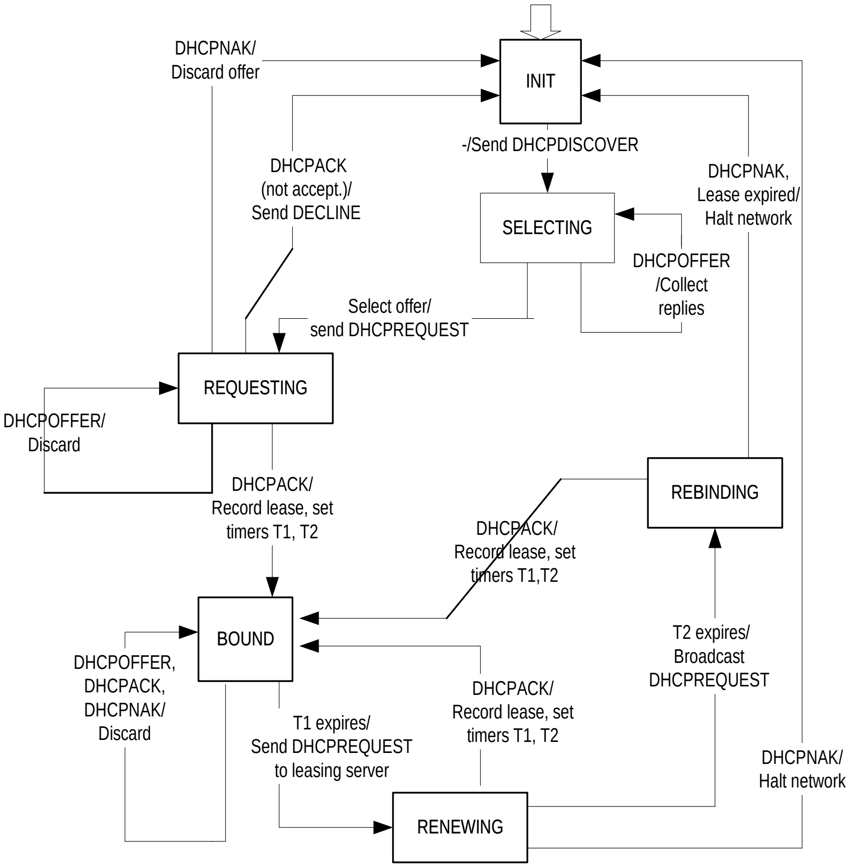


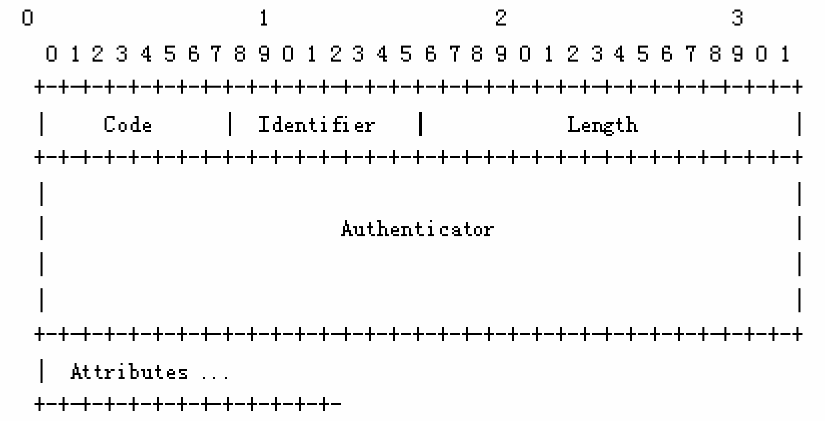
Figure 9-2 DHCP client state transit

9.2.3 Introduction to DHCP Accounting

DHCP accounting enables a DHCP server to notify the RADIUS server of the start or end of accounting when assigning or reclaiming a lease. The cooperation of the DHCP server and RADIUS server implements the network accounting function, and at the same time improves the network security to a certain degree.

I. Structure of the DHCP accounting packet

The interactive operations between the DHCP server and the RADIUS server are based on two types of packets: accounting start request and accounting stop request. The two types of packets have the similar structure, and the only difference lies in the Attributes field. The following figure illustrates the packet structure:



```
 0                   1                   2                   3
  0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |     Code      |  Identifier   |            Length             |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |                                                               |
 |                         Authenticator                         |
 |                                                               |
 |                                                               |
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
 |  Attributes ...
 +-+-+-+-+-+-+-+-+-+-+-+-+-+-
```

Figure 9-3 Structure of the DHCP accounting packet

- Code: One byte for identifying the type of the DHCP accounting packet. A value of 4 indicates an accounting start request, while a value of 5 indicates an accounting stop request. If the Code field of an accounting packet is not valid, the packet is discarded.
- Identifier: One byte for matching requests and responses. The RADIUS server checks this field for duplicate requests from the same IP address and UDP port of a client.
- Length: Two bytes for identifying the length of the accounting packet.
- Authenticator: 16 bytes for identifying the information between the RADIUS server and client.

II. Fundamental of DHCP accounting

After you complete AAA authentication and RADIUS configuration on a router with the DHCP server function enabled, the DHCP server acts as a RADIUS client. For the authentication process of the DHCP server acting as a RADIUS client, refer to the “Introduction to the RADIUS Protocol” section of the "Security” part in this manual. The following describes only the interactive accounting operations between the DHCP server and the RADIUS server.

- After sending a DHCP_ACK packet with the IP configuration parameters to the DHCP client, the DHCP server sends an accounting start request to the specified RADIUS server. The RADIUS server processes the accounting start request, makes a record, and sends a response to the DHCP server.
- Once reclaiming a lease for some reason, the DHCP server sends an accounting stop request to the RADIUS server immediately. The RADIUS server processes the accounting stop request, stops the recording for the DHCP client, and sends a response to the DHCP server. A lease can be reclaimed for an expired lease, a release request from the DHCP client, a manual reclamation operation, an address pool removal operation, and the like.

- If the RADIUS server of the specified domain is unreachable for some reason, the DHCP server sends up to three DHCP accounting start requests (including the first sending attempt) at regular intervals. If the three start requests bring no response from the RADIUS server, the DHCP server does not send start requests any more.

9.2.4 Option 82 Support on the DHCP Server

Option 82 is a relay agent information option in the DHCP packet. When a request packet from a DHCP client travels through a DHCP relay on its way to the DHCP server, the DHCP relay inserts the option 82 field into the request packet. Option 82 includes many sub-options, but the DHCP server supports only sub-option 5 at present. When the DHCP relay adds the IP address of a segment into sub-option 5 of option 82, the DHCP server can assign an IP address or the configuration information according to option 82.

I. Basic concepts for option 82

1) Options

Options is a length-variable field in the DHCP packet for carrying information such as part of the lease information and packet type. It can include up to 255 options and must comprise at least one option.

2) Option 82

Option 82, also known as relay agent information option, is a part of the Options field of DHCP packet. According to RFC3046, option 82 lies before option 255 and after the other options. Option 82 can include up to 255 sub-options and must comprise at least one sub-option. Up to now, the frequently used sub-options in option 82 are sub-option 1, sub-option 2, and sub-option 5.

3) Sub-option 1

As a sub-option of option 82, sub-option 1 represents the agent circuit ID, namely Circuit ID. It holds the VLAN-ID and MAC address of the switch port for the DHCP client, which usually you must configure on the DHCP relay.

Generally, sub-option 1 and sub-option 2 must be used in conjunction to identify information about the DHCP source end.

4) Sub-option 2

Sub-option 2 is also a sub-option of option 82 and represents the remote agent ID, namely Remote ID. It holds the MAC address of the DHCP relay, which usually you must configure on the DHCP relay.

Generally, sub-option 1 and sub-option 2 must be used in conjunction to identify information about the DHCP source end.

5) Sub-option 5

Sub-option 5, another sub-option of option 82, represents link selection. It holds the IP address added by the DHCP relay, so that the DHCP server can assign an IP address on the same segment as the address.

📖 **Note:**

Currently, DHCP from 3Com Corporation implements only part of the functions of option 82: The DHCP server supports only sub-option 5 in option 82, and the DHCP relay supports only sub-options 1 and 2 in option 82.

II. Operating mechanism of option 82 support on the DHCP server

Sub-option 5 of option 82 for DHCP server operates on these principles:

- On a network with a DHCP relay, the DHCP relay forwards the DHCP request packet broadcasted by a DHCP client to the DHCP server.
- Upon receiving a request packet forwarded by the DHCP relay, the DHCP server determines whether sub-option 5 of option 82 is present in the packet. If the sub-option is present, the DHCP server looks up the local address pools, assigns an IP address on the same segment as that in sub-option 5 to the client, and responds with a packet with option 82.
- After receiving the response from the DHCP server, the DHCP relay strips off option 82 and forwards the resulted packet to the DHCP client.

III. Protocols and standards

The protocols related with option 82 for DHCP server include these:

- RFC2131 Dynamic Host Configuration Protocol
- RFC3527 Link Selection sub-option

9.2.5 BIMS Option Support on the DHCP Server

BIMS option for DHCP server enables a DHCP server to notify a DHCP client of the information about the branch intelligent management system (BIMS) server when assigning an IP address, making the DHCP client be able to use the BIMS server for software backup and upgrade after obtaining an IP address. The code of the BIMS option is 217.

I. Structure of the BIMS Option packet

The BIMS option is added into the Options field of a response generated by the DHCP server for a DHCP client. Since DHCP clients from different manufacturers process DHCP responses differently, the DHCP server adds the BIMS option to both

DHCP_OFFER and DHCP_ACK packets. The structure of the BIMS option packet is as follows:

```
Code      Len     IP:port:sharekey
+-------+------+------+------+------+------+--...-+------+
|  217  |   N  |  i1  |  i2  |  i3  |  i4  | ...|  iN  |
+-------+------+------+------+------+------+--...-+------+
```

Figure 9-4 Structure of the BIMS option packet

The BIMS option packet has a structure similar to those of other option packets. It also contains the Code field for identifying the number of the option and the Len field for identifying the length of the option packet.

The i1 to iN fields mainly carry the IP address, protocol port, and shared key of the BIMS server, which are represented by a string. For example, if the IP address of the BIMS server is 192.168.1.1, the port number is 80, and the shared key is abcdefg, then these fields carry the string of 192.168.1.1.80.abcdefg.

II. Fundamental of BIMS Option for DHCP Server

1) A DHCP client sends a request to the DHCP server for an IP address and configuration parameters.
2) When receiving a request, the DHCP server checks the locally configured address pools. You can enable the BIMS option feature for a global address pool or interface address pool of the DHCP server. If the address to be assigned to the client is from an address pool for which BIMS option is enabled, the DHCP server encapsulates the IP address, protocol port, and shared key of the BIMS server together with the IP configuration parameters in the response.
3) When receiving the response with the BIMS option information from the DHCP server, the DHCP client resolves the BIMS option information to obtain the IP address, protocol port, and shared key of the BIMS server. After that, the client periodically sends connection requests to the BIMS server for software backup and upgrade.

9.2.6 Introduction to Option 184

Option 184 is an RFC reserved option, and the information it carries can be customized. 3Com defines four proprietary sub-options for this option, enabling the DHCP server to encapsulate the information required by a DHCP client in the response packet to the client. The four sub-options of option 184 mainly carry information about voice. The following lists the sub-options and the carried information:

- Sub-option 1: IP address of the network call processor (NCP-IP).
- Sub-option 2: IP address of the alternate server (AS-IP).

- Sub-option 3: Voice VLAN configuration.
- Sub-option 4: Fail-over call routing.

I. Meanings of the sub-options for option 184

- NCP-IP

The NCP-IP sub-option carries the IP address of the network call processor (NCP). When used in option 184, this sub-option must be the first sub-option, that is, sub-option 1.

The IP address of the NCP server carried by sub-option 1 of option 184 is intended for identifying the server acting as the network call controller and used for application download.

- AS-IP

The AS-IP sub-option carries the IP address of the alternate server (AS), and is the second sub-option of option 184, that is, sub-option 2. The AS-IP sub-option takes effect only when sub-option 1 (that is, the NCP-IP sub-option) is defined.

The alternate NCP server identified by sub-option 2 of option 184 acts as the backup of the NCP server and is used only when the IP address carried by the NCP-IP sub-option is unreachable or invalid.

- Voice VLAN configuration

The voice VLAN configuration sub-option carries the ID of the voice VLAN and the flag indicating whether the voice VLAN identification function is enabled. This sub-option is the third sub-option of option 184, that is, sub-option 3.

The sub-option 3 of option 184 comprises two parts, which carry the previously mentioned two items respectively. A flag value of 0 indicates that the voice VLAN identification function is not enabled, in which case the information carried by the VLAN ID part will be neglected. A flag value of 1 indicates that the voice VLAN identification function is enabled.

- Fail-over call routing

The fail-over call routing sub-option carries the IP address for fail-over call routing and the associated dial number. This sub-option is the fourth sub-option of option 184, that is, sub-option 4.

The IP address for fail-over call routing and the dial number in sub-option 4 of option 184 refer to the IP address and dial number of the session initiation protocol (SIP) peer. When the NCP server and alternate NCP server (if configured) are unreachable, a SIP user can use the configured IP address and dial number of the peer to establish a connection and communicates with the peer SIP user.

🕮 **Note:**

For the configurations specifying to add sub-option 2, sub-option 3, and sub-option 4 in the response packets to take effect, you must configure the DHCP server to add sub-option 1.

II. Operational mechanism of using option 184 on DHCP server

The DHCP server encapsulates the information for option 184 to carry in the response packets sent to the DHCP clients. Supposing that the DHCP clients are on the same segment as the DHCP server, the operational mechanism of option 184 support on DHCP server is as follows:

1) A DHCP client sends to the DHCP server a request packet carrying option 55, which indicates the client requests the configuration parameters of option 184.
2) The DHCP server checks the request list in option 55 carried by the request packet, and then adds the sub-options of option 184 in the Options field of the response packet sent to the DHCP client.

🕮 **Note:**

Only when the DHCP client specifies in option 55 of the request packet that it requires option 184, does the DHCP server add option 184 in the response packet sent to the client.

9.2.7 DHCP Address Allocation Support of WAN Interfaces

The traditional DHCP client function can only be implemented on Ethernet interfaces, while all the current functions of DHCP server, DHCP relay, and DHCP client can be implemented on WAN interfaces encapsulating PPP, HDLC, or FR. The DHCP-enabled WAN interfaces include synchronous/asynchronous serial interface and E1 interface.

The following describes the operational procedure of the DHCP server and DHCP client based on the encapsulated link layer protocol.

I. Enabling DHCP address allocation on a WAN interface encapsulating PPP

With PPP encapsulated and DHCP enabled, an interface starts with PPP negotiation, and after achieving negotiation success, performs DHCP packet interaction. The following lists the detailed procedure:

1) After the LCP negotiation over the PPP link succeeds, the local client (the DHCP client) sends a DHCP-Discover request packet to the peer (the DHCP server), which the DHCP server discards.
2) During IPCP negotiation, the local client uses the IP address of another interface or an address that is all 0s to negotiate with the peer. After the IPCP negotiation succeeds, the DHCP client broadcasts the DHCP request packet over the PPP link. For the address allocation procedure, refer to section 9.2.2 "Fundamentals of DHCP server".
3) After obtaining an IP address, the DHCP client fills the IP address to the corresponding WAN interface and notifies the PPP module that the local address has changed. Then, the local PPP module performs the IPCP negotiation again to notify the peer of the IP address change.

II. Enabling DHCP address allocation on a WAN interface encapsulating FR

The operational procedure of DHCP on an FR link is similar to that on Ethernet. However, since an FR interface may have multiple logical channels, when an FR interface is used as DHCP client to apply for an IP address, the following happen:

- If the FR interface is configured to allow dynamic address mapping, the DHCP client can broadcast the DHCP request packet directly to perform normal DHCP negotiation and obtain an IP address.
- If the FR interface is configured with static address mapping, the **broadcast** keyword must be configured at the same time, so that the DHCP request packet can be broadcasted over multiple logical channels and the DHCP client can obtain an IP address.

III. Enabling DHCP address allocation on a WAN interface encapsulating HDLC

When the link layer protocol is HDLC, once the DHCP client initiates a DHCP request, the DHCP server can assign an IP address to the client directly.

9.3 DHCP Relay

The early Dynamic Host Configuration Protocol (DHCP) is only applicable to the case where DHCP server and client are in the same sub-net, but not to the trans-segment case. To achieve dynamic host configuration, it is required to configure a DHCP server for every segment, as obviously uneconomical.

DHCP relay can solve this problem. With DHCP relay, the client in a LAN can communicate with the DHCP server in another sub-net and get IP address successfully. That is, DHCP clients in several sub-nets can share one DHCP server, as is significant for saving cost and centralized management.

You may use a host or router as a DHCP relay simply by running a DHCP relay agent program on it.

9.3.1 Principle of DHCP Relay

The following figure illustrates DHCP relay networking.

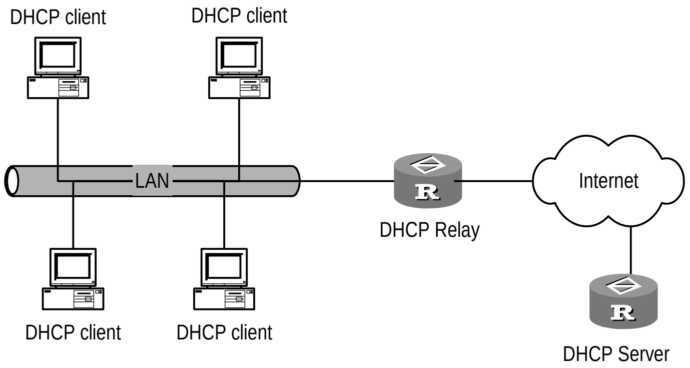


Figure 9-5 Network diagram for DHCP relay

DHCP relay works on this principle:

- When DHCP client starts and runs DHCP initialization, it sends configuration request packet to the local network.
- If there is a DHCP server in the network, it begins DHCP configurations without DHCP relay.
- If not, the local network processes the packet and forwards it to the specified DHCP server in another sub-net.
- The DHCP server undertakes configurations according to the information from the client and sends the configuration information through DHCP relay back to the client. Till now, dynamic configuration for the client ends is completed. In practice, multiple message exchange processes may be required to finish client configuration.

It can be seen that DHCP relay supports transparent transmission of DHCP broadcast messages and can transmit broadcast messages from DHCP client (or server) transparently to the DHCP server (or client) in another sub-net.

In real network, DHCP relay function is often implemented at a specific interface of a router. So you should configure IP relay address for the interface to specify a target DHCP server.

9.3.2 Option 82 Support on the DHCP Relay

Option 82 is a relay agent information option in the DHCP packet.

When a request packet with option 82 from a DHCP client reaches a DHCP relay on its way to the DHCP server, the DHCP relay may drop it, forward it with its option 82 information intact, or forward it with its original option 82 information replaced.

Option 82 provides many sub-options. Among them, only sub-option 1 and sub-option 2 are available on the DHCP relay. Option 82 allows the address information of the DHCP client and the DHCP relay such as MAC address and VLAN ID, to be recorded on the DHCP server. In conjunction with other software, it may implement DHCP address assignment restriction and accounting.

I. Operating mechanism of option 82 support on the DHCP relay

When obtaining an IP address through a DHCP relay, the DHCP client goes through four phases, discovery, offer, selecting, and final check, as it would directly through a DHCP server. This section however, describes only the operating mechanism of option 82 support on the DHCP relay.

The following is how option 82 support is operating on the DHCP relay:

1) The DHCP client broadcasts a request when it is initialized.
2) If no DHCP server is present on the local network, the DHCP relay connected to the network checks the packet for the option 82 field. If the packet does not carry the option 82 field, the DHCP relay inserts the option 82 field into the packet and forwards it with the MAC address and VLAN ID of the switch port connected to the DHCP client, and the MAC address of the DHCP relay itself. If the packet carries option 82 information, the DHCP relay does one of the following depending on the adopted strategy:

- Drop the packet.
- Forward the packet with its option 82 information intact.
- Forward the packet with its option 82 information being replaced with that of the DHCP relay.
- When the DHCP server receives the request, it records the option 82 information and then sends a response carrying DHCP configuration and option 82 information back to the DHCP relay.
- The DHCP relay sends the received response to the DHCP client with option 82 information removed.

Note:

To accommodate the DHCP request processing mechanisms of different DHCP relay vendors, the DHCP relay with option 82 support enabled inserts option 82 information into all DHCP requests, whether they are DHCP_DISCOVER or DHCP_Request.

II. Protocols and standards

The DHCP relay supports option 82 in compliance with the following protocols:

- RFC 2131 Dynamic Host Configuration Protocol (DHCP)
- RFC 3046 DHCP Relay Agent Information Option

9.4 DHCP Common Configuration

DHCP common configurations refer to those configurations suitable for both DHCP server and DHCP relay. The configuration tasks include

- Enable/disable DHCP services
- Configure pseudo-DHCP server detection

9.4.1 Enabling/Disabling DHCP

For both DHCP server and DHCP relay, DHCP configurations can take effect only after DHCP is enabled.

Perform the following configurations in the system view.

Table 9-1 Enable/disable DHCP

Operation	Command
Enable DHCP.	**dhcp enable**
Disable DHCP.	**undo dhcp enable**

By default, DHCP is enabled.

Note:

DHCP can operate normally only after you correctly set the system clock.

9.4.2 Configuring Pseudo-DHCP Server Detection

Pseudo-DHCP servers are unauthorized DHCP servers. Upon the request for IP address from a DHCP client, a pseudo-DHCP server might communicate with the client and may allocate incorrect IP address to the client.

You can configure pseudo-DHCP server detection to record IP address and interface information of DHCP server. Then the administrator can easily find and deal with the pseudo-DHCP server.

Perform the following configurations in system view.

Table 9-2 Configure pseudo-DHCP server detection

Operation	Command
Enable pseudo-DHCP server detection.	**dhcp server detect**
Disable pseudo-DHCP server detection.	**undo dhcp server detect**

By default, pseudo-DHCP server detection is disabled.

9.5 DHCP Server Configuration

DHCP server configuration tasks include

- Setting interfaces to operate in DHCP server mode
- Adding DHCP address pool
- Defining allocation mode of DHCP address pool
- Excluding IP address from auto allocation
- Defining IP address lease expiry limit
- Configuring domain name for DHCP client
- Configuring DNS (Domain Name Server) IP address for DHCP client
- Configuring NetBIOS IP address for DHCP client
- Defining NetBIOS node type for DHCP client
- Configuring DHCP customization items
- Configuring egress gateway router for DHCP client
- Configuring ping packet transfer in DHCP server
- Clearing DHCP information

Note:

Differences between global address pool and interface address pool:

- The global address pool is created with **dhcp server ip-pool** command in system view and it takes effect within the scope of this router.
- The interface address pool is established automatically when the Ethernet interface is configured with valid unicast IP address and the **dhcp select interface** command is configured; it is effective only in the interface. Its address segment range is the segment for the Ethernet interface. The commands related to interface address pool can be configured only when the interface address pool exists.

9.5.1 Setting Interfaces to Operate in DHCP Server Mode

When the router receives a DHCP packet with itself being the destination, the router handles the packet depending on the specified operating mode. When operating in DHCP server mode, the router forwards the packet to the local DHCP server; when operating in relay mode, the router forwards the packet to an external DHCP server.

Perform the following configuration in interface view to have the current interface operate in DHCP server mode.

Table 9-3 Set the current interface to operate in DHCP server mode

Operation	Command
Send DHCP packets to the local DHCP server and allocate addresses from the global address pool	**dhcp select global** [**subaddress**]
Send DHCP packets to the local DHCP server and allocate addresses from the interface address pool	**dhcp select interface**
Restore the default	**undo dhcp select**

Note:

These commands must be performed on an Ethernet interface (subinterface), virtual Ethernet interface, synchronous/asynchronous serial interface encapsulated with PPP, HDLC or frame relay, or E1 interface.

Perform the following configuration in the system view to have the specified interfaces operate in DHCP server mode.

Table 9-4 Set multiple interfaces to operate in DHCP server mode

Operation	Command
Send DHCP packets to the local DHCP server and allocate addresses from the global address pool	**dhcp select global** [**subaddress**] { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] **|** **all** }
Send DHCP packets to the local DHCP server and allocate addresses from the interface address pool	**dhcp select interface** { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] **|** **all** }
Resets the default	**undo dhcp select** { **interface** *interface-type interface-number* [**to** *interface-type interface-number* **|** **all** }

By default, **dhcp select global** applies. Currently DHCP server is available on following interfaces:

- Ethernet interface (subinterface)
- Virtual Ethernet interface
- Synchronous/asynchronous serial interface encapsulated with PPP, HDLC, or frame relay
- E1 interface

🕮 **Note:**

To use interface address pools for address allocation, you must configure the **dhcp select interface** command.

You may configure the **subaddress** keyword to allow the DHCP server to assign a DHCP client an IP address belonging to a subaddress segment for the Ethernet interface. This IP address is selected from the global address pool corresponding to the subaddress segment. When subaddress allocation is enabled, the Ethernet interface on the DHCP server must be assigned a subaddress located in the subaddress segment from which subaddresses are selected for DHCP clients. This is to ensure that the main address and the IP address assigned to a DHCP client are located in different network segments.

9.5.2 Adding Global DHCP Address Pool

DHCP server allocates IP addresses from the address pool. When DHCP client originates DHCP requests to DHCP server, the server will choose a proper address pool according to a certain algorithm and select a free IP address, which, along with other parameters (for example DNS IP address, address lease limit), is sent to the client. With V 2.41, a DHCP server by far can be configured with 128 global address pools.

The address pools in DHCP server is in tree structure: the native segment address as root, sub-net addresses as branch, addresses bound to the clients as leaf nodes. This structure guarantees configuration inheritance: the sub-net (son node) inherits the configurations of the native segment (father node); the client (grandson node) inherits the configurations of the sub-net. For those common parameters, for example domain name, you can just configure them at the native segment or sub-net. You can view the structure of the address pools with the **display dhcp server tree** command. The order for those address pools at the same level is defined by creation time.

Perform the following configurations in the system view.

Table 9-5 Add global DHCP address pool

Operation	Command
Adds DHCP address pool or enter DHCP address pool view	**dhcp server ip-pool** *pool-name*
Deletes DHCP address pool	**undo dhcp server ip-pool** *pool-name*

By default, no global DHCP address pool is created.

9.5.3 Defining Allocation Mode of DHCP Address Pool

You can select static address binding or dynamic address binding accordingly, but you can only choose one of them for a given DHCP address pool.

For dynamic address allocation mode, you should specify address range. Static address binding can be deemed as a special DHCP address pool with only one address.

I. Configuring static address binding for global address pool

Some DHCP clients may require a fixed IP address, i.e., binding the client MAC address or identifier to an IP address. Then when the DHCP client with this MAC address or identifier requests for an IP address, DHCP server will find and allocate the bound IP address to the client.

Perform the following configurations in the DHCP address pool view.

Table 9-6 Configure static address binding

Operation	Command
Configure static IP address binding	**static-bind ip-address** *ip-address* [**mask** *netmask*]
Delete static IP address binding	**undo static-bind ip-address**
Configure static client MAC address or identifier binding	**static-bind** { **mac-address** *mac-address* | **client-identifier** *client-identifier* }
Delete static client MAC address or identifier binding	**undo static-bind** { **mac-address** | **client-identifier**}

By default, no binding is configured and the client MAC address/identifier is set as Ethernet.

Note:

The command **static-bind ip-address** must be used along with the **static-bind** { **mac-address | client-identifier**} command. If you use the commands repeatedly, the new configuration will overwrite the previous one.

II. Configuring static address binding for interface address pool

Perform the following configurations in Ethernet interface (or subinterface) view.

Table 9-7 Configure static address binding for interface address pool

Operation	Command
Configure a static address binding for the address pool of the current interface	**dhcp server static-bind ip-address** *ip-address* { **mac-address** *mac-address* | **client-identifier** *client-identifier* }
Delete a static address binding	**undo dhcp server static-bind** { **ip-address** *ip-address* | **mac-address** *mac-address* | **client-identifier** *client-identifier* }

Among all the bindings of an interface, each IP address, MAC address, and client identifier must be unique. In addition, the client identifier and the corresponding MAC address are mutually exclusive, that is, an IP address can only be bound to a MAC address or client identifier, but not both.

III. Configuring dynamic address allocation

For the dynamic addresses (including permanent ones or those lease limit dynamic ones), you should configure them with address pool range. Currently only one address segment can be set to an address pool, which is defined by the mask.

Perform the following configurations in the DHCP address pool view.

Table 9-8 Configure IP address range for dynamic allocation

Operation	Command
Configure IP address range for dynamic allocation	**network** *ip-address* [**mask** *netmask*]
Delete dynamic IP address range	**undo network**

By default, no DHCP address pool is available for dynamic allocation.

If you use the command repeatedly, the new configurations will overwrite the previous ones.

9.5.4 Excluding IP Address from Auto Allocation

In configuring address allocation by DHCP server, you should exclude those in-use IP addresses. Otherwise, one IP address may be allocated to two hosts, which will cause address conflict.

Perform the following configurations in the system view.

Table 9-9 Exclude IP address from auto allocation

Operation	Command
Forbid auto allocation of an IP address	**dhcp server forbidden-ip** *low-ip-address* [*high-ip-address*]
Allow auto allocation of the IP address	**undo dhcp server forbidden-ip** *low-ip-address* [*high-ip-address*]

By default, all addresses in the DHCP address pool will be automatically allocated.

Using this command repeatedly, you can exclude multiple IP addresses from being allocated.

9.5.5 Defining IP Address Lease Expiry Limit

DHCP server can assign different lease duration limit for different address pools, but the same lease duration limit for the addresses in the same address pool.

Address lease duration limit cannot be renewed automatically.

The system provides different configuration modes for different types of address pools.

I. Global DHCP address pool

Perform the following configurations in the DHCP address pool view.

Table 9-10 Configure lease expiry limit for global DHCP address pool

Operation	Command
Configures expiry limit for dynamic IP address lease	**expired** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }
Resets the lease expiry limit to the default value	**undo expired**

II. Interface DHCP address pool

Perform the following configurations in Ethernet interface (or subinterface) view.

Table 9-11 Configure lease expiry limit for interface DHCP address pool

Operation	Command
Configures expiry limit for dynamic IP address lease	**dhcp server expired** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }
Resets the lease expiry limit to the default value	**undo dhcp server expired**

III. Multiple interface DHCP address pools

You can also configure lease limit for DHCP address pool on multiple interfaces at one blow.

Perform the following configurations in the system view.

Table 9-12 Configure lease expiry limit for DHCP address pool on multiple interfaces

Operation	Command
Configures expiry limit for dynamic IP address lease	**dhcp server expired** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number* | **all** }
Resets the lease expiry limit to the default value	**undo dhcp server expired** { **interface** *interface-type interface-number* [**to** *interface-type interface-number* | **all** }

By default, an IP address lease expires after one day.

🕮 **Note:**

For some DHCP configuration items, the system provides different configuration modes for different types of DHCP address pools. You can configure these items respectively in the global DHCP address pool, interface DHCP address pool and multiple interface DHCP address pools.

These configuration tasks include: Configuring domain name for DHCP client, configuring DNS IP address for DHCP client, configuring NetBIOS IP address for DHCP client, defining NetBIOS node type for DHCP client and configuring DHCP customization items.

Currently, the leasing valid period specified by this command cannot exceed the year of 2106.

9.5.6 Configuring Domain Names for DHCP Clients

On a DHCP server, you may configure domain names that DHCP clients should use when obtaining the DNS service on a per-address pool basis.

Perform the following configuration in DHCP address pool view to configure the global DHCP address pool.

Table 9-13 Configure DHCP client domain name in global DHCP address pool

Operation	Command
Configures a domain name to DHCP client	**domain-name** *domain-name*
Delete the domain name to DHCP client	**undo domain-name**

Perform the following configurations in Ethernet interface (or subinterface) view to configure the interface DHCP address pool.

Table 9-14 Configure domain name to DHCP client in interface DHCP address pool

Operation	Command
Configures a domain name to DHCP client	**dhcp server domain-name** *domain-name*
Delete the domain name to DHCP client	**undo dhcp server domain-name**

Perform the following configurations in the system view to configure multiple interface DHCP address pools.

Table 9-15 Assign domain name to DHCP client in multiple interface DHCP address pools

Operation	Command
Configures a domain name to DHCP client	**dhcp server domain-name** *domain-name* { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] **|** **all** }
Delete the domain name to DHCP client	**undo dhcp server domain-name** *domain-name* { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] **|** **all** }

By default, no domain name is allocated to DHCP client.

9.5.7 Configuring DNS IP Address for DHCP Client

When the host accesses the Internet through domain name, it should translate the domain name into IP address, which is implemented by Domain Name System (DNS). To access DHCP client successfully into the Internet, DHCP server ought to assign DNS IP address at the time allocating IP address to the client.

A maximum of eight DNS addresses by far can be configured in a DHCP address pool.

Perform the following configurations in the DHCP address pool view to configure global DHCP address pool.

Table 9-16 Configure DNS IP address in global DHCP address pool

Operation	Command
Configures a DNS IP address to DHCP client	**dns-list** *ip-address* [*ip-address*]
Delete the DNS IP address to DHCP client	**undo dns-list** { *ip-address* **| all** }

Perform the following configurations in Ethernet interface (or subinterface) view to configure interface DHCP address pool.

Table 9-17 Configure DNS IP address in interface DHCP address pool

Operation	Command
Configure a DNS IP address to DHCP client	**dhcp server dns-list** *ip-address* [*ip-address*]
Delete the DNS IP address to DHCP client	**undo dhcp server dns-list** { *ip-address* | **all** }

Perform the following configurations in the system view to configure multiple interface DHCP address pools.

Table 9-18 Configure DNS IP address in multiple interface DHCP address pools

Operation	Command
Add a DNS server to the DNS server list of the DHCP client	**dhcp server dns-list** *ip-address* [*ip-address*] { **interface** *interface-type interface-number* [**to** *interface-type interface-number* | **all** }
Remove the specified DNS server from the DNS server list of the DHCP client	**undo dhcp server dns-list** { *ip-address* | **all** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number* | **all** }

By default, no IP address of DNS server is configured.

9.5.8 Configuring NetBIOS IP Address for DHCP Client

For those clients running on Microsoft operating system, WINS (Windows Internet Naming Service) server is required to translate host name into IP address for the hosts using NetBIOS protocol. So most Windows client may require WINS settings.

A maximum of eight NetBIOS addresses currently can be configured in a DHCP address pool.

Perform the following configurations in the DHCP address pool view to configure global DHCP address pool.

Table 9-19 Configure NetBIOS IP address in global DHCP address pool

Operation	Command
Configures a NetBIOS address to DHCP client	**nbns-list** *ip-address* [*ip-address*]
Deletes the NetBIOS address to DHCP client	**undo nbns-list** { *ip-address* **|** **all** }

Perform the following configurations in Ethernet interface (or subinterface) view to configure interface DHCP address pool.

Table 9-20 Configure NetBIOS IP address to DHCP client in interface

Operation	Command
Configures a NetBIOS address to DHCP client	**dhcp server nbns-list** *ip-address* [*ip-address*]
Deletes the NetBIOS address to DHCP client	**undo dhcp server nbns-list** { *ip-address* **|** **all** }

Perform the following configurations in the system view to configure multiple interface DHCP address pools.

Table 9-21 Configure NetBIOS IP address to DHCP client in multiple interface DHCP address pools

Operation	Command
Configures a NetBIOS address to DHCP client	**dhcp server nbns-list** *ip-address* [*ip-address*] { **interface** *interface-type* *interface-number* [**to** *interface-type interface-number*] **|** **all** }
Deletes the NetBIOS address to DHCP client	**undo dhcp server nbns-list** { *ip-address* **|** **all** } { **interface** *interface-type* *interface-number* [**to** *interface-type interface-number*] **|** **all** }

By default, no NetBIOS IP address is configured to DHCP client.

9.5.9 Defining NetBIOS Node Type for DHCP Client

Mapping must be established between the host name and IP address when DHCP client uses NetBIOS protocol for communications over Wide Area Network (WAN). In terms of mapping establishment mode, NetBIOS node can be divided as

- b-node: b here stands for broadcast, that is, the node gets mapping through broadcast.
- p-node: p here stands for peer-to-peer. The node gets mapping by communicating with the NetBIOS server.

- m-node: m here stands for mixed. It is the p-node embraces part of the broadcast attributes.
- h-node: h here stands for hybrid. It is b-node for which peer-to-peer communication is available.

Perform the following configurations in the DHCP address pool view to configure DHCP address pool.

Table 9-22 Define NetBIOS node type in global DHCP address pool

Operation	Command
Defines NetBIOS node type for DHCP client	**netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** }
Resets NetBIOS node type to the default value	**undo netbios-type**

Perform the following configurations in Ethernet interface (or subinterface) view to configure interface DHCP address pool.

Table 9-23 Define NetBIOS node type in interface DHCP address pool

Operation	Command
Defines NetBIOS node type for DHCP client	**dhcp server netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** }
Resets NetBIOS node type to the default value	**undo dhcp server netbios-type**

Perform the following configurations in the interface view to configure multiple interface DHCP address pools.

Table 9-24 Define NetBIOS node type in multiple interface DHCP address pools

Operation	Command
Defines NetBIOS node type for DHCP client	**dhcp server netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }
Resets NetBIOS node type to the default value	**undo dhcp server netbios-type** { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

By default, h-node is configured for DHCP client.

9.5.10 Configuring DHCP Customization Items

With further development of DHCP technology, new optional configuration items may arise. Then you can add in custom way these items into DHCP server attribute table.

Perform the following configurations in the DHCP address pool view to configure global DHCP address pool.

Table 9-25 Configure DHCP customization items

Operation	Command
Adds DHCP customization items	**option** *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }
Deletes DHCP customization items	**undo option** *code*

Perform the following configurations in Ethernet interface (or subinterface) view to configure interface DHCP address pool.

Table 9-26 Configure DHCP customization items

Operation	Command
Adds DHCP customization items	**dhcp server option** *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* }
Deletes DHCP customization items	**undo dhcp server option** *code*

Perform the following configurations in the interface view to configure multiple interface DHCP address pools.

Table 9-27 Configure DHCP customization items

Operation	Command
Adds DHCP customization items	**dhcp server option** *code* { **ascii** *ascii-string* | **hex** *hex-string* | **ip-address** *ip-address* } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }
Deletes DHCP customization items	**undo dhcp server option** *code* { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

9.5.11 Configuring Egress Gateway Router for DHCP Client

DHCP client must use an egress gateway for data transmission and receiving when accessing the server or host with the IP address not in the segment.

Perform the following configurations in the DHCP address pool view.

Table 9-28 Configure egress gateway router for DHCP client

Operation	Command
Configures egress gateway router for DHCP client	**gateway-list** *ip-address* [*ip-address*]
Deletes the egress gateway router	**undo gateway-list** { *ip-address* **|** **all** }

By default, no egress gateway router is configured to DHCP client.

A maximum of eight egress gateway addresses currently can be configured in a DHCP.

📖 **Note:**

To configure multiple egress gateway addresses, give out the ip-address parameter one by one.

9.5.12 Configuring ping Packet Transfer in DHCP Server

To prevent IP address conflict, DHCP server will check whether an address has been allocated before allocating it to the client.

You can initiate IP address check with the command **ping**. If no response is sent back, then continue to send ping packets till the maximum ping packets allowed are sent. If there is still no response sent back with the preset time limit, then you can conclude that this IP address is free. This ensures the client a unique IP address.

Perform the following configurations in the system view.

Table 9-29 Configure ping packet transfer in DHCP server

Operation	Command
Configures maximum number of ping packet for transfer in DHCP server	**dhcp server ping packets** *number*
Resets the maximum number of ping packet to the default value	**undo dhcp server ping packets**
Configures time limit to receive ping response	**dhcp server ping timeout** *milliseconds*
Resets time limit to receive ping response to the default value	**undo dhcp server ping timeout**

By default, two ping packets can be transferred and 500 milliseconds are set for DHCP server to receive ping response.

The DHCP server detects address collisions by sending pings, while the DHCP client does that by sending ARP packets.

9.5.13 Configuring DHCP Accounting

When DHCP accounting is enabled, the DHCP server sends accounting packets to the RADIUS accounting server in the specific domain when issuing and releasing leases.

In this case, the RADIUS server records information about use of IP addresses, but does not really perform accounting.

I. Configuration prerequisites

Before configuring DHCP accounting, perform the following configuration:

- Complete the related configuration on the DHCP server and client, ensuring that the DHCP server can assign IP addresses to clients.
- Complete the configuration related to domain and RADIUS accounting server. That is, configure the RADIUS scheme for the specified domain, and configure the RADIUS server in the RADIUS scheme.

For configuration of domain and RADIUS accounting server, refer to the “Security” part of this manual.

II. Configuring DHCP accounting in system view

Table 9-30 Configure DHCP accounting in system view

Operation	Command	Remarks
Enter system view	**system-view**	—
Configure the interfaces to work in DHCP server mode and assign addresses from specified interface address pools	**dhcp select interface** { **all** | **interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	Required
Enable DHCP accounting for addresses from specified interface address pool and configure the domain for DHCP accounting	**dhcp server accounting domain** *domain-name* { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }	Required
Enter interface view	**interface** *interface-type interface-number*	To create interface address pools, you must configure IP addresses for the interfaces involved in the above commands.
Configure the IP address of the interface	**ip address** *ip-address net-mask*	

📖 **Note:**

- This mode applies to the scenario that the DHCP server allocates IP addresses from interface address pools.
- In this mode, you can configure a range of interfaces, and therefore can enable DHCP accounting on multiple interfaces at a time.

III. Configuring DHCP accounting in interface view

Table 9-31 Configure DHCP accounting in interface view

Operation	Command	Remarks
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	Required
Configure the IP address of the interface	**ip address** *ip-address net-mask*	Required
Configure the interface to work in DHCP server mode and assign addresses from the interface address pools	**dhcp select interface**	Required
Enable DHCP accounting for addresses from the interface address pools and configure the domain for DHCP accounting	**dhcp server accounting domain** *domain-name*	Required

📖 **Note:**

- This mode applies to the scenario where the DHCP server allocates IP addresses from interface address pools.
- In this mode, you can enable DHCP accounting in interface view. Therefore, this mode applies when you want to enable DHCP accounting on a single interface.

IV. Configuring DHCP accounting in global DHCP address pool view

Table 9-32 Configure DHCP accounting in global DHCP address pool view

Operation	Command	Remarks
Enter system view	**system-view**	—

Operation	Command	Remarks
Configure specified interfaces to work in DHCP server mode and assign addresses from the global DHCP address pool	**dhcp select global** [**subaddress**] { **all** | **interface** *interface-type interface-number* [**to** *interface-type interface-number*]}	Required
Enter DHCP address pool view	**dhcp server ip pool** *pool-name*	—
Configure the IP addresses for dynamic allocation	**network** *ip-address* [**mask** *netmask*]	
Enable DHCP accounting for addresses in the DHCP address pool and configure the domain for DHCP accounting	**accounting domain** *domain-name*	By default, DHCP accounting is not enabled.

Note:

This mode applies to the scenario where the DHCP server allocates IP addresses from the global DHCP address pool.

9.5.14 Configuring BIMS Option Support on the DHCP Server

I. Configuration prerequisites

Before configuring the feature of BIMS option for DHCP server, complete the following tasks:

- Enable the DHCP server function and configure the address pools on the router.
- Configure the DHCP clients.
- Ensure that the DHCP clients, DHCP server, and BIMS server are reachable.

II. Configuring BIMS option

The following table describes the BIMS option configuration tasks.

Table 9-33 Configure BIMS option

Operation	Command	Remarks
Enter system view	**system-view**	—

Operation	Command	Remarks
Enable and configure BIMS option in system view	**dhcp server bims-server ip** *ip-address* **port** *port-number* **sharekey** *key* { **interface** *interface-type interface-number* **to** *interface-type interface-number* | **all** }	Required. These are three alternative ways of configuring BIMS options.
Enable and configure BIMS option in interface view	**dhcp server bims-server ip** *ip-address* [**port** *port-number*] **sharekey** *key* **undo dhcp server bims-server**	
Enable and configure BIMS option in global DHCP address pool view,	**dhcp server ip-pool** *pool-name*	
	bims-server ip *ip-address* **port** *port-number* **sharekey** *key*	

Note:

- If you configure BIMS option for a global address pool, the DHCP server sends the BIMS option information together with the lease when assigning an IP address from the global address pool to a DHCP client.
- If you configure BIMS option for an interface, the DHCP server sends the BIMS option information together with the lease when assigning an IP address from the interface address pool to a DHCP client.
- If you specify the **all** keyword in the **dhcp server bims-server ip** command, the DHCP server sends the BIMS option information together with the lease when assigning an IP address from any of the interface address pools to a DHCP client.

9.5.15 Configuring Option 184 Support on the DHCP Server

You may configure suboptions of option 184 for the DHCP server in system view, interface view, or DHCP address pool view. Whichever view you select, you must configure interface address pools for involved interfaces.

I. Configuration prerequisites

Before configuring option 184 support on the DHCP server, make sure that:

- The network parameters, and address pool and address lease allocation policies are configured.
- The DHCP client is reachable to the DHCP server.

II. Configuring option 184 in system view

Table 9-34 Configure option 184 for the DHCP server in system view

Operation	Command	Remarks
Enter system view	**system-view**	—
Configure specified interfaces to operate in DHCP server mode and assign addresses from specified interface address pools	**dhcp select interface** { **all** | **interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	Required
Configure suboption NCP-IP of option 184	**dhcp server voice-config ncp-ip** *ip-address* { **all** | **interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	Required
Configure suboption AS-IP of option 184	**dhcp server voice-config as-ip** *ip-address* { **all** | **interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	Optional This suboption is available only after you configure suboption NCP-IP.
Configure suboption Voice VLAN Configuration of option 184	**dhcp server voice-config voice-vlan** *vlan-id* { **enable** | **disable** } { **all** | **interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	Optional This suboption is available only after you configure suboption NCP-IP.
Configure suboption Fail-Over Routing of option 184	**dhcp server voice-config fail-over** *ip-address dialer-string* { **all** | **interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	Optional This suboption is available only after you configure suboption NCP-IP.
Enter interface view	**interface** *interface-type interface-number*	Repeat these two steps to assign IP address to each involved interface. Otherwise, your address pool creation may fail.
Assign an IP address to the interface	**ip address** *ip-address net-mask*	

Note:

Configure option 184 in system view when the DHCP server uses interface address pools to assign addresses.

This approach allows you to configure option 184 on multiple interfaces at the same time.

III. Configuring option 184 in interface view

Table 9-35 Configure option 184 for the DHCP server in interface view

Operation	Command	Remarks
Enter system view	**system-view**	—
Enter interface view	**interface** *interface-type interface-number*	Required
Assign an IP address to the interface	**ip address** *ip-address net-mask*	Required
Configure the interface to operate in DHCP server mode and assign addresses from its address pool	**dhcp select interface**	Required
Configure suboption NCP-IP of option 184	**dhcp server voice-config ncp-ip** *ip-address*	Required
Configure suboption AS-IP of option 184	**dhcp server voice-config as-ip** *ip-address*	Optional This suboption is available only after you configure suboption NCP-IP.
Configure suboption Voice VLAN Configuration of option 184	**dhcp server voice-config voice-vlan** *vlan-id* { **enable** | **disable** }	Optional This suboption is available only after you configure suboption NCP-IP.
Configure suboption Fail-Over Routing of option 184	**dhcp server voice-config fail-over** *ip-address dialer-string*	Optional This suboption is available only after you configure suboption NCP-IP.

📖 **Note:**

Configure option 184 in interface view when the DHCP server uses an interface address pool to assign addresses.

This approach allows you to configure option 184 on a single interface.

IV. Configuring option 184 in DHCP global address pool view

Table 9-36 Configure option 184 for the DHCP server in global address pool view

Operation	Command	Remarks
Enter system view	**system-view**	—
Configure specified interfaces to operate in DHCP server mode and assign addresses from a global address pool	**dhcp select global** [**subaddress**] { **all** | **interface** *interface-type interface-number* [**to** *interface-type interface-number*] }	Required
Enter DHCP address pool view	**dhcp server ip pool** *pool-name*	Required
Configure an IP address range for dynamic address allocation	**network** *ip-address* [**mask** *netmask*]	Required
Configure suboption NCP-IP of option 184	**voice-config ncp-ip** *ip-address*	Required
Configure suboption AS-IP of option 184	**voice-config as-ip** *ip-address*	Optional This suboption is available only after you configure suboption NCP-IP.
Configure suboption Voice VLAN Configuration of option 184	**voice-config voice-vlan** *vlan-id* { **enable | disable** }	Optional This suboption is available only after you configure suboption NCP-IP.
Configure suboption Fail-Over Routing of option 184	**voice-config fail-over** *ip-address dialer-string*	Optional This suboption is available only after you configure suboption NCP-IP.

🕮 **Note:**

Configure option 184 in DHCP global address pool view when the DHCP server uses a global address pool to assign addresses.

9.5.16 Configuring Option 82 Support on the DHCP Server

I. Configuration prerequisites

Before configuring option 82 support on the DHCP server, make sure that:

- The DHCP server function is enabled on your device and the network parameters of the device are configured.
- The network parameters, and address pool and address lease allocation policies are configured for the DHCP server.
- The DHCP server device is reachable.

For more information, refer to the part discussing DHCP.

II. Enabling option 82 support on the DHCP server

Table 9-37 Configure option 82 support on the DHCP server

Operation	Command	Remarks
Enter system view	**system-view**	—
Enable option 82 support on the DHCP server	**dhcp server relay information enable**	Required By default, option 82 support is enabled on the DHCP server.

9.5.17 Clearing DHCP Information

Use the **display dhcp server ip-in-use** command in any views to display dynamic address binding information of the address pool. You can delete the information using the corresponding command.

Use the **display dhcp server conflict** command in any views to display DHCP address conflict information. You can delete the information using the corresponding command.

Use the **display dhcp server statistics** command in any views to display DHCP server information. You can delete the information using the corresponding command.

Perform the following configurations in user view.

Table 9-38 Clear DHCP information

Operation	Command
Clear binding information of a specific IP address	**reset dhcp server ip-in-use ip** *ip-address*
Clear dynamic address binding information of the global address pool	**reset dhcp server ip-in-use pool** [*pool-name*]
Clear dynamic address binding information of the interface address pool	**reset dhcp server ip-in-use interface** [*interface-type interface-number*]
Clear binding information of all address pools	**reset dhcp server ip-in-use all**
Clear conflict information of a specific IP address	**reset dhcp server conflict** *ip-address*

Operation	Command
Clear conflict information of all address pool	**reset dhcp server conflict all**
Clear statistical information in DHCP server	**reset dhcp server statistics**

9.6 DHCP Relay Configuration

DHCP relay configuration tasks include:

- Setting interfaces to operate in DHCP relay mode
- Specifying external DHCP server addresses
- Configuring DHCP server load sharing from DHCP relay
- Releasing DHCP client IP address from DHCP relay
- Clearing DHCP relay information

9.6.1 Setting Interfaces to Operate in DHCP Relay Mode

When the router receives a DHCP packet with itself being the destination, the router handles the packet depending on the specified operating mode. When operating in DHCP server mode, the router forwards the packet to the local DHCP server; when operating in relay mode, the router forwards the packet to an external DHCP server.

Perform the following configuration in interface view to have the current interface operate in DHCP relay mode.

Table 9-39 Set the current interface to operate in DHCP relay mode

Operation	Command
Relay DHCP packets to an external DHCP server for address allocation	**dhcp select relay**
Restore the default	**undo dhcp select**

Note:

These commands must be performed on an Ethernet interface (subinterface), virtual Ethernet interface, synchronous/asynchronous serial interface encapsulated with PPP, HDLC or frame relay, or E1 interface.

Perform the following configuration in the system view to have the specified interfaces operate in DHCP relay mode.

Table 9-40 Set multiple interfaces to operate in DHCP relay mode

Operation	Command
Relay DHCP packets to an external DHCP server for address allocation	**dhcp select relay** { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] **|** **all** }
Resets the default	**undo dhcp select** { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] **|** **all** }

By default, **dhcp select global** applies.

Currently DHCP relay is available on following interfaces:

- Ethernet interface (subinterface)
- Virtual Ethernet interface
- Synchronous/asynchronous serial interface encapsulated with PPP, HDLC, or frame relay
- E1 interface

Note:

When a PC wants to obtain an IP address through the DHCP relay on an Ethernet subinterface on the router, the PC needs to connect to the router through a switch. In this case, you need to make proper link configuration on the switch beforehand.

9.6.2 Specifying External DHCP Servers

When receiving a DHCP broadcast, the interface with DHCP relay enabled relays the DHCP broadcast to the specified external DHCP server.

Perform the following configuration in interface view to specify an external DHCP server address to which the received DHCP broadcasts are to be forwarded.

Table 9-41 Specify an external DHCP server address on the current interface

Operation	Command
Specify an external DHCP server address on the current interface	**ip relay address** *ip-address*
Delete one or all external DHCP server addresses on the current interface	**undo ip relay address** { *ip-address* | **all** }

Perform the following configuration in system view to specify an external DHCP server address to which the DHCP broadcasts received on the specified interfaces are to be forwarded.

Table 9-42 Configure an external DHCP server address for multiple interfaces

Operation	Command
Specify an external DHCP server address for the interfaces in the specified range	**ip relay address** *ip-address* [**interface** *interface-type interface-number* [**to** *interface-type interface-number* | **all**]
Remove an external DHCP server address for the interfaces in the specified range	**undo ip relay address** { *ip-address* | **all** } { **interface** *interface-type interface-number* [**to** *interface-type interface-number*] | **all** }

📖 **Note:**

Since the packets sent by the DHCP client are broadcast in some stages, the corresponding interface must support broadcast.

Up to 20 external DHCP server addresses can be configured on an interface.

9.6.3 Configuring DHCP Server Load Sharing for DHCP Relay

You can use DHCP relay to configure several DHCP servers and share traffic load between them.

When multiple DHCP servers are configured, the DHCP Relay can distribute among them requests from the clients using the HASH algorithm and thus achieve load sharing.

Perform the following configurations in the system view.

Table 9-43 Configure DHCP server load sharing

Operation	Command
Configures DHCP server load sharing	**ip relay address cycle**
Cancel DHCP server load sharing	**undo ip relay address cycle**

By default, no load sharing between DHCP servers is available.

9.6.4 Releasing Client IP Address by DHCP Relay

Sometimes you may release the IP address of a client by DHCP relay.

Perform the following configurations in interface view or system view.

Table 9-44 Release client IP address from DHCP relay

Operation	Command
Requests DHCP server to release client IP address	**dhcp relay release** *client-ip mac-address*
Requests a specific DHCP server to release client IP address	**dhcp relay release** *client-ip mac-address server-ip*

If no DHCP server is specified, in system view, the release request will be sent to all DHCP servers; while in interface view, the release request will be sent to the current interface.

🕮 **Note:**

After receiving an IP address release request from the DHCP relay, the DHCP server releases the IP address from the IP-in-use address pool and moves it to the lease-expired queue. Normally, this address will experience some time before participating in allocation again. For the client, however, this address is not released and will be used until its lease really expires.

Release packets take effect only when the server uses MAC addresses to identify users. When the DHCP server function is deployed on a router, you can use the **display dhcp server ip-in-use** command to display the related information. If the words “Hardware address” are displayed, the server is using MAC addresses to identify users; if the words “Client identifier/Hardware address” are displayed, the server is using client identifiers to identify users.

9.6.5 Configuring Option 82 Support on the DHCP Relay

I. Configuration prerequisites

Before configuring option 82 support on the DHCP relay, make sure that:

- The DHCP relay function is enabled on your device and the network parameters of the device are configured.
- The network parameters, and address pool and address lease allocation policies are configured for the DHCP relay.
- The DHCP relay device is reachable.

For more information, refer to the part discussing DHCP.

II. Configuring option 82 support on the DHCP relay

Table 9-45 Configure option 82 support on the DHCP relay

Operation	Command	Remarks
Enter system view	**system-view**	—
Enable option 82 support on the DHCP relay	**dhcp relay information enable**	Required
Configure a strategy for handling packets with option 82 on the DHCP relay	**dhcp relay information strategy** { **drop** | **keep** | **replace** }	Required By default, the DHCP relay uses the replace strategy when handling a request with option 82.

9.6.6 Clearing DHCP Relay Information

Use the command **display dhcp relay statistics** in any views to view DHCP relay information. The information can certainly be cleared out.

Perform the following configuration in user view.

Table 9-46 Clear DHCP relay information

Operation	Command
Clears DHCP relay information	**reset dhcp relay statistics**

9.7 DHCP Client Configuration

When configuring the DHCP client, you only need to perform one command to have an interface to get IP address from DHCP. Currently, DHCP is available only on the following interfaces:

- Ethernet interface or subinterface
- Synchronous/asynchronous serial interface encapsulated with PPP, HDLC, or frame relay
- E1 interface

Perform the following configurations in interface view.

Table 9-47 Configure static IP and MAC address binding

Operation	Command
Enable DHCP client to get local IP address	**ip address dhcp-alloc**
Disable DHCP client	**undo ip address dhcp-alloc**

By default, DHCP client is disabled.

Note the following:

- After configured to obtain an IP address through DHCP, an interface cannot be configured with any subaddress. That is, the command **ip address dhcp-alloc** is in conflict with the command **ip address** *ip-address mask* **sub**, so you can only use one of them.
- When one interface on a DHCP client goes up after obtaining an IP address from a DHCP server configured with the **gateway-list** command, a default route entry appears in the routing table on the client, with the next hop being the gateway specified by the command. If the DHCP client is connected to multiple DHCP servers configured with different gateways, multiple equal-cost default routes may appear in its routing table with their next hops being different gateways, for example,

```
[Router] display ip routing-table
Routing Table: public net
Destination/Mask   Protocol    Pre  Cost      Nexthop       Interface
0.0.0.0/0           DHCPDEF    255    0      23.23.0.2     Ethernet2/1.1

                                              30.30.0.3       Serial3/0:0
```

- When an interface with frame relay encapsulation is functioning as the DHCP client, the interface adopts frame relay dynamic address mapping or broadcast-mode frame relay static address mapping.
- Currently, virtual Ethernet interfaces support DHCP server but not DHCP client.

9.8 Displaying and Debugging DHCP

When the aforementioned configurations are completed, use the **display** command in any views to show DHCP running status, for the purpose of checking configuration information.

Using the **debugging** command in user view, you can enable DHCP debugging.

I. Displaying and debugging DHCP server

Table 9-48 Display and debug DHCP

Operation	Command
Display free address information in DHCP address pool	**display dhcp server free-ip**
Display in-conflict DHCP address information	**display dhcp server conflict** { **ip** *ip-address* | **all** }

Operation	Command
Display expired leases in DHCP address pool	**display dhcp server expired** { **ip** *ip-address* | **pool** [*pool-name*] | **interface** [*interface-type interface-number*] **all** }
Display DHCP address binding information	**display dhcp server ip-in-use** { **all** | **ip** *ip-address* | **pool** [*pool-name*] | **interface** [*interface-type interface-number*] }
Display DHCP server information	**display dhcp server statistics**
Display tree architecture information about DHCP address pool	**display dhcp server tree** { **pool** [*pool-name*] | **interface** [*interface-type interface-number*] | **all** }
Enable DHCP server debugging	**debugging dhcp server** { **error** | **events** | **packets** }
Disable DHCP server debugging	**undo debugging dhcp server** { **events** | **packets** | **error** }
Delete the information of DHCP dynamic address binding	**reset dhcp server ip-in-use** { **ip** *ip-address* | **pool** [*pool-name*] | **interface** [*interface-type interface-number*] | **all** }
Delete the statistics of DHCP address conflict	**reset dhcp server conflict** { *ip-address* | **all** }
Delete the statistics of the DHCP server	**reset dhcp server statistics**

📖 **Note:**

The lease information is not saved in the DHCP server's Flash when you execute the save command. So there is not any lease information in the configuration files when the system restarts or when you use the reset dhcp server ip-in-use command to delete the lease information. If a client requests lease renewal at this time, the system will not permit it but require the client to apply for the IP address again.

II. Displaying and debugging DHCP relay

Table 9-49 Display and debug DHCP relay

Operation	Command
Display the IP information of the interface of DHCP relay	**display ip interface** [*interface-type interface-number*]
Display the statistics of DHCP relay	**display dhcp relay statistics**

Operation	Command
Display the DHCP relay address of the interface	**display dhcp relay address** [**interface** *interface-type interface-num* **| all**]
Display IP-to-MAC address associations for DHCP clients obtaining IP addresses through the DHCP relay	**display dhcprelay-security**
Enable the DHCP relay debugging	**debugging dhcp relay** { **all** | **error** | **event** | **packet** [**client mac** *mac-address*] }
Disable the DHCP relay debugging	**undo debugging dhcp relay** { **all** | **error** | **event** | **packet** [**client mac** *mac-address*] }

III. Displaying and debugging DHCP client

Table 9-50 Display and debug DHCP client

Operation	Command
Display the statistics of DHCP client	**display dhcp client** [**verbose**]
Enable the DHCP client debugging	**debugging dhcp client** { **error | event | packet** | **all** }
Disable the DHCP client debugging	**undo debugging dhcp client** { **error | event | packet | all** }

9.9 DHCP Configuration Examples

9.9.1 DHCP Server Configuration Example

There are two types of DHCP networking modes: one is that both DHCP server and DHCP client are in the same sub-net and they exchange signals using DHCP. The second is that DHCP server and DHCP client are in different sub-nets, which requires DHCP relay agent to achieve IP address allocation. The configuration details are the same in both networking modes.

I. Network requirements

DHCP server allocates dynamic IP address to DHCP client which is in the same sub-net. The address pool segment 10.1.1.0/24 is divided into two sub-segments: 10.1.1.0/25 and 10.1.1.128/25. The two Ethernet interface of DHCP server are with the addresses 10.1.1.1/25 and 10.1.1.129/25.

For the segment 10.1.1.0/25, the address lease limit is 10 days and 12 hours; the domain name is huawei.com; the DNS address is 10.1.1.2; no NetBIOS is configured; the egress router address is 10.1.1.126. For the segment 10.1.1.128/25, the address limit is 5 days; the DNS address is 10.1.1.2; the NetBIOS address is 10.1.1.4; the egress router address is 10.1.1.254.

II. Networking topology

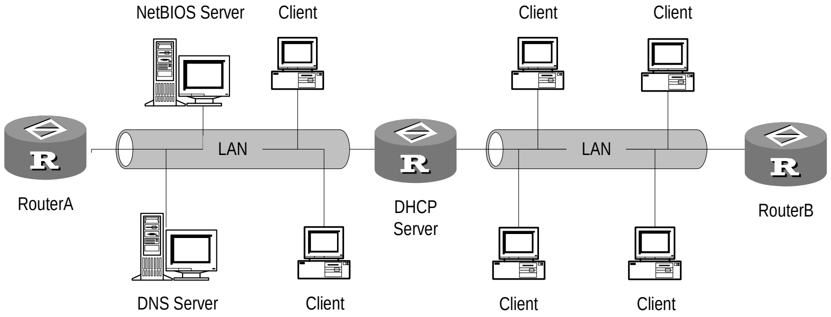


Figure 9-6 DHCP server and client in the same sub-net

III. Configuration procedure

# Enable DHCP

```
[3Com] dhcp enable
```

# Configure specified interfaces to operate in DHCP server mode and allocate IP addresses from a global address pool.

```
[3Com] dhcp select global interface ethernet 0/0/0 to ethernet 0/0/1
```

# Forbid auto allocation of IP addresses (including DNS address, NetBIOS address and egress gateway address)

```
[3Com] dhcp server forbidden-ip 10.1.1.2
[3Com] dhcp server forbidden-ip 10.1.1.4
[3Com] dhcp server forbidden-ip 10.1.1.126
[3Com] dhcp server forbidden-ip 10.1.1.254
```

# Configure common attributes for DHCP address pool 0 (address pool range, domain name and DNS address).

```
[3Com] dhcp server ip-pool 0
[3Com-dhcp-0] network 10.1.1.0 mask 255.255.255.0
[3Com-dhcp-0] domain-name huawei.com
[3Com-dhcp-0] dns-list 10.1.1.2
[3Com-dhcp-0] quit
```

# Configure attributes for DHCP address pool 1 (address pool range, egress gateway address and address lease limit)

```
[3Com] dhcp server ip-pool 1
[3Com-dhcp-1] network 10.1.1.0 mask 255.255.255.128
[3Com-dhcp-1] gateway-list 10.1.1.126
```

```
[3Com-dhcp-1] expired day 10 hour 12
```

# Configure attributes for DHCP address pool 2 (address pool range, egress gateway address, NetBIOS address and address lease limit).

```
[3Com] dhcp server ip-pool 2
[3Com-dhcp-2] network 10.1.1.128 mask 255.255.255.128
[3Com-dhcp-2] expired day 5
[3Com-dhcp-2] nbns-list 10.1.1.4
[3Com-dhcp-2] gateway-list 10.1.1.254
```

9.9.2 DHCP Relay Configuration Example

I. Network requirements

The segment for DHCP client is 10.110.0.0 and that for DHCP server is 202.38.0.0. A router which supports DHCP relay function is required for forwarding DHCP messages, so that DHCP client can request configuration information (for example IP address) successfully from DHCP server.

DHCP server is configured with an IP address pool whose segment is 10.110.0.0, so the IP addresses can be allocated to the DHCP clients on this segment. DHCP server is also configured with routes to the segment 10.110.0.0.

II. Networking topology

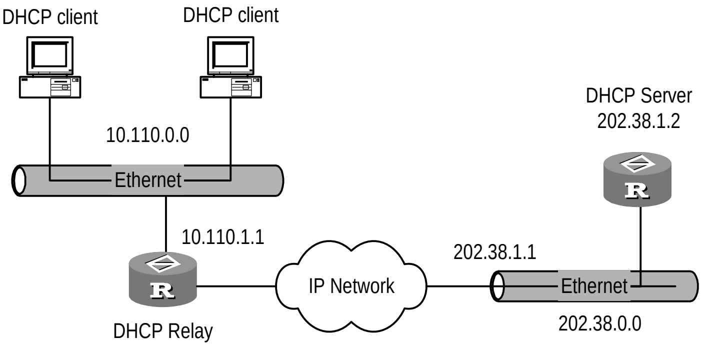


Figure 9-7 DHCP relay configuration

III. Configuration procedure

Configurations on the router:

# Enable DHCP services

```
[3Com] dhcp enable
```

# Enter an interface where DHCP relay function has been enabled, configure IP address and mask for it, and ensure that the interface and DHCP client are in the same segment.

```
[3Com] interface ethernet 6/0/0
```

```
[3Com-Ethernet6/0/0] ip address 10.110.1.1 255.255.0.0
```

# Configure IP relay address for the interface to specify the target DHCP server.

```
[3Com-Ethernet6/0/0] dhcp select relay
[3Com-Ethernet6/0/0] ip relay address 202.38.1.2
```

Configurations on DHCP server will not be mentioned here.

9.9.3 DHCP Client Configuration Example

Two types of DHCP client configurations are mentioned here: one is that the Ethernet gets dynamic IP address, the other is that the Ethernet sub-interface gets dynamic IP address (supporting VLAN).

I. Ethernet interface as DHCP client

1) Network requirements

The interfaces Ethernet0/0/0 and Ethernet2/0/0 of the router RTA are connected respectively into LAN1 and LAN2, which are respectively configured with DHCP server 1 and DHCP server 2. The segment for LAN1 is 200.254.0.0/16 and that for LAN2 is 172.10.0.0/16. The configuration task is to make the two interfaces get IP addresses through DHCP.

2) Networking topology

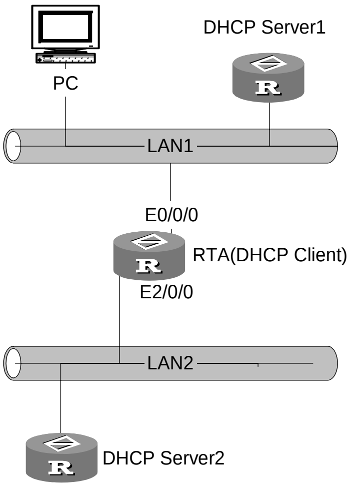


Figure 9-8 Main interface as DHCP client

3) Configuration procedure

The configuration of both DHCP server and client are mentioned.

# Configure server1

```
[server1] dhcp enable
[server1] interface ethernet0/0/0
[server1-Ethernet0/0/0] ip address 200.254.0.1 16
```

```
[server1] dhcp server ip-pool 1
[server1-dhcp1] network 200.254.0.0 mask 255.255.0.0
```

# Configure server2

```
[server2] dhcp enable
[server2] interface ethernet0/0/0
[server2-Ethernet0/0/0] ip address 172.10.0.1 16
[server2] dhcp server ip-pool 2
[server2-dhcp2] network 172.10.0.0 mask 255.255.0.0
```

# Configure Ethernet0/0/0 getting dynamic IP address though DHCP

```
[client] interface ethernet0/0/0
[client-Ethernet0/0/0] ip address dhcp-alloc
```

# Configure Ethernet2/0/0 getting dynamic IP address through DHCP

```
[client] interface ethernet2/0/0
[client-Ethernet2/0/0] ip address dhcp-alloc
```

II. Ethernet sub-interface as DHCP client

1) Network requirements

DHCP servers 1 and 2 are respectively in VLAN10 and VLAN20. The configuration task is to create sub-interfaces and configure getting dynamic IP addresses respectively from the two DHCP servers.

2) Networking diagram

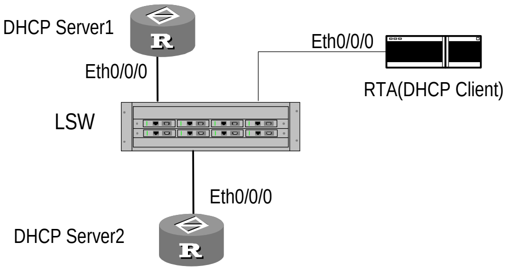


Figure 9-9 Sub-interface as DHCP client

3) Configuration procedures

Configure LAN Switch first (it is not detailed here) and make sure that DHCP servers 1and 2 can be respectively connected into VLAN10 and VLAN 20. Then configure RTA interface as Trunk interface which enables transparent transmission of messages for VLAN 10 and VLAN 20.

The configurations of DHCP server1 and server2 are similar to those in above example, so the configurations of DHCP client are listed.

# Configure the sub-interface which gets IP address from DHCP server1.

```
[client] interface ethernet0/0/0.1
```

```
[client-Ethernet0/0/0.1] vlan-type dot1q vid 10
[client-Ethernet0/0/0.1] ip addr dhcp-alloc
```

# Configure the sub-interface which gets IP address from DHCP server2.

```
[client] interface ethernet0/0/0.2
[client-Ethernet0/0/0.2] vlan-type dot1q vid 20
[client-Ethernet0/0/0.2] ip addr dhcp-alloc
```

9.9.4 DHCP Accounting Configuration Example

I. Network requirements

As shown in Figure 9-10,

- The DHCP server is connected to the DHCP client and the RADIUS server through interface Ethernet1/0/0 and Ethernet1/0/1 respectively.
- The IP address of the RADIUS server is 10.1.2.2/24.
- DHCP accounting is enabled on the DHCP server. The global DHCP address pool is 10.1.1.0 and domain 123 is assigned to the pool for DHCP accounting.

It is required that the RADIUS accounting server could track IP address use of the DHCP client.

II. Network diagram

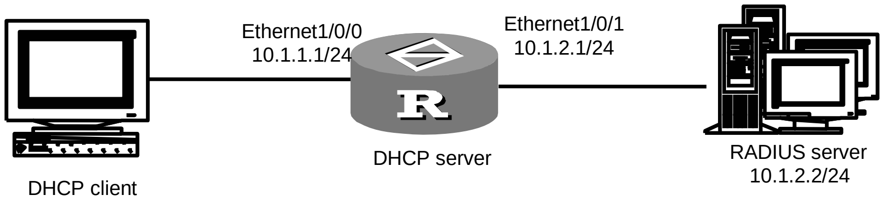


Figure 9-10 Network diagram for DHCP accounting

III. Configuration procedure

# Configure DHCP server network parameters.

```
<3Com> system-view
[3Com] interface Ethernet 1/0/0
[3Com-Ethernet1/0/0] ip address 10.1.1.1 255.255.255.0
[3Com-Ethernet1/0/0] quit
[3Com] interface Ethernet 1/0/1
[3Com-Ethernet1/0/1] ip address 10.1.2.1 255.255.255.0
[3Com-Ethernet1/0/1] quit
```

# Enable DHCP server.

```
[3Com] dhcp enable
[3Com] dhcp select global interface ethernet 1/0/0 to ethernet 1/0/1
```

# Create a domain, create a RADIUS scheme, and associate them for DHCP accounting.

```
[3Com] radius scheme 123
[3Com-radius-123] primary authentication 10.1.2.2
[3Com-radius-123] quit
[3Com] domain 123
[3Com-isp-123] scheme radius-scheme 123
[3Com-isp-123] quit
```

# Configure an address pool for the DHCP server.

```
[3Com] dhcp server ip-pool test
[3Com-dhcp-pool-test] network 10.1.1.0 mask 255.255.255.0
```

# Configure DHCP accounting and assign domain 123 to the pool just created.

```
[3Com-dhcp-pool-test] accounting domain 123
```

9.9.5 Option 184-Supported DHCP Server Configuration Example

I. Network requirements

Figure 9-11 presents a scenario, where

- 3Com VCX is functioning as the DHCP client, 3Com Router is functioning as the DHCP server.
- 3Com Router supports option 184 when assigning addresses from global address pools. The suboption NCP-IP of option 184 is set to 3.3.3.3, AS-IP to 2.2.2.2, voice VLAN state to enable and ID to 1, Fail-Over IP to 1.1.1.1 and fail-over dial string to 99*.

II. Network diagram

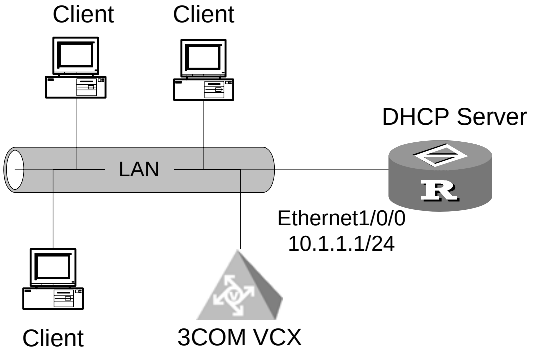


Figure 9-11 Network diagram for option 184 support on the DHCP server

III. Configuration procedure

1) Configure the DHCP client (on 3Com VCX)

Enable DHCP client, and configure it to request all suboptions of option 184 when requesting an address.

2) Configure the DHCP server

```
<3Com> system-view
[3Com] dhcp enable
[3Com] dhcp select global interface ethernet 1/0/0
[3Com] dhcp server ip-pool 123
[3Com-dhcp-pool-123] network 10.1.1.1 mask 255.255.255.0
[3Com-dhcp-pool-123] voice-config as-ip 2.2.2.2
[3Com-dhcp-pool-123] voice-config ncp-ip 3.3.3.3
[3Com-dhcp-pool-123] voice-config voice-vlan 1 enable
[3Com-dhcp-pool-123] voice-config fail-over 1.1.1.1 99*
[3Com-dhcp-pool-voice] quit
```

9.9.6 Option 28-Supported DHCP Relay Configuration Example

I. Network requirements

As shown in Figure 9-12, two DHCP clients on 10.110.1.0 obtain IP addresses from a DHCP server through a DHCP relay.

Do the following on the DHCP relay:

- Configure option 82 support
- Use the keep strategy to handle DHCP requests with option 82.

II. Network diagram

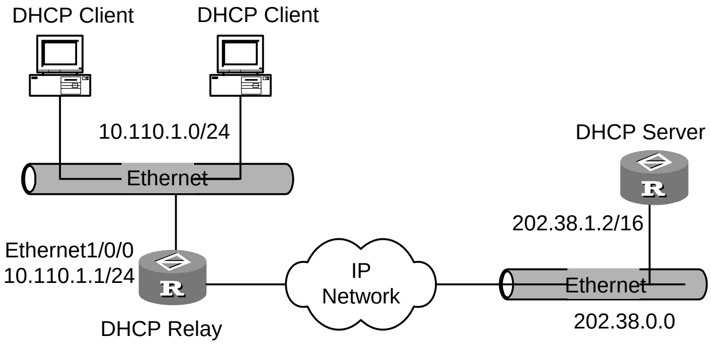


Figure 9-12 Network diagram for option 82 support on DHCP relay

III. Configuration procedure

This example assumes that the DHCP relay and the DHCP server are reachable to each other.

1) Configure the DHCP relay

# Enable DHCP.

```
<3Com> system-view
[3Com] dhcp enable
```

# Configure the DHCP relay interface, and assign it an IP address belonging to the same network segment.

```
[3Com] interface ethernet 1/0/0
[3Com-Ethernet1/0/0] dhcp select relay
[3Com-Ethernet1/0/0] ip address 10.110.1.1 255.255.255.0
```

# Specify a DHCP server to the DHCP relay interface.

```
[3Com-Ethernet1/0/0] ip relay address 202.38.1.2
[3Com-Ethernet1/0/0] quit
```

# Enable option 82 support on the frame relay and specify the strategy for handling packets with option 82 to keep.

```
[3Com] dhcp relay information enable
[3Com] dhcp relay information strategy keep
```

2) Configure the DHCP server

Omitted

9.9.7 DHCP Configuration Example for the Serial Interface using PPP

I. Network requirements

As shown in Figure 9-13,

- A DHCP relay uses interface Serial 2/0/1 to connect to interface Serial 2/0/1 on a DHCP client and uses interface Serial 2/0/0 to connect to a DHCP relay, both across PPP links.
- The DHCP server uses the address pool with the segment 20.20.0.0/24 for address assignment.

Perform configuration to allow interface Serial 2/0/0 on the DHCP client to obtain IP address from the DHCP server through the DHCP relay.

II. Network diagram

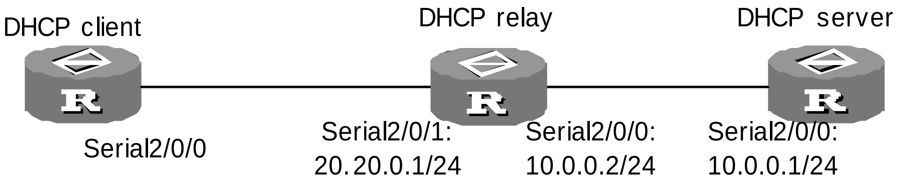


Figure 9-13 Network diagram for the DHCP support on the serial interface using PPP

III. Configuration procedure

1) Configure the DHCP server

```
<3Com> system-view
[3Com] dhcp enable
[3Com] dhcp select global interface serial 2/0/0
[3Com] dhcp server ip-pool 1
[3Com-dhcp-pool-1] network 20.20.0.0 mask 255.255.255.0
[3Com-dhcp-pool-1] gateway-list 20.20.0.1
[3Com-dhcp-pool-1] domain-name huawei.com
[3Com-dhcp-pool-1] quit
[3Com] interface serial 2/0/0
[3Com-serial2/0/0] link-protocol ppp
[3Com-serial2/0/0] ip address 10.0.0.1 255.255.255.0
[3Com-serial2/0/0] quit
[3Com] ip route 0.0.0.0 0.0.0.0 10.0.0.2
```

2) Configure the DHCP relay

```
<3Com> system-view
[3Com] dhcp enable
[3Com] interface seral 2/0/0
[3Com-serial2/0/0] link-protocol ppp
[3Com-serial2/0/0] ip address 10.0.0.2 255.255.255.0
[3Com-serial2/0/0] quit
[3Com] interface serial 2/0/1
[3Com-serial2/0/1] link-protocol ppp
[3Com-serial2/0/1] ip address 20.20.0.1 255.255.255.0
[3Com-serial2/0/1] ip relay address 10.10.0.1
[3Com-serial2/0/1] dhcp select relay
[3Com-serial2/0/1] quit
```

3) Configure the DHCP client

```
<3Com> system-view
```

```
[3Com] dhcp enable
[3Com] interface serial 2/0/0
[3Com-serial2/0/0] link-protocol ppp
[3Com-serial2/0/0] ip address dhcp-alloc
[3Com-serial2/0/0] quit
```

Chapter 10 IP Performance Configuration

10.1 Configuring Maximum Transmission Unit (MTU)

MTU size of the interface decides whether the IP packets on the interface need to be fragmented.

Table 10-1 Configure MTU of the interface

Operation	Command
Configure MTU of the interface	**mtu** *mtu-size*
Restore to the default value of the interface MTU	**undo mtu**

The default value of the interface MTU is 1500 bytes when using Ethernet_II frame format.

10.2 Configuring TCP Packet Fragmentation

The parameter of TCP packet fragmentation determines whether the TCP packets are to be fragmented.

Perform these commands in interface view.

Table 10-2 Configure TCP packets fragmentation

Operation	Command
Enable TCP packet fragmentation	**tcp mss** *value*
Disable the TCP packet fragmentation	**undo tcp mss**

By default, TCP packets are not fragmented.

10.3 Configuring TCP Attributes

TCP attributes that can be configured include:

- syn timer: When sending the syn packets, TCP starts the syn timer. If response packets are not received before syn timeout, the TCP connection will be terminated. The range of syn timer timeout time is 2 to 600 seconds, and the default is 75 seconds.
- fin timer: When the TCP connection state turns from FIN_WAIT_1 to FIN_WAIT_2, fin timer will be started. If FIN packets are not received before fin timer timeout, the

TCP connection will be terminated. The range of fin is 76 to 3600 seconds and the default of fin is 675 seconds.

- The receiving/sending buffer size of connection-oriented Socket: The range is 1 to 32 KB and the default is 8 KB.

Perform the following configuration in the interface view.

Table 10-3 Configure TCP attributes

Operation	Command
Configure syn timer time for TCP connection establishment	**tcp timer syn-timeout** *time-value*
Restore syn timer time for TCP connection establishment to default value	**undo tcp timer syn-timeout**
Configure FIN_WAIT_2 timer time of TCP	**tcp timer fin-timeout** *time-value*
Restore FIN_WAIT_2 timer time of TCP to default value	**undo tcp timer fin-timeout**
Configure Socket receiving/sending buffer size of TCP	**tcp window** *window-size*
Restore Socket receiving/sending buffer size of TCP to default value	**undo tcp window-**

10.4 Configuring the Sending of ICMP Redirect Messages

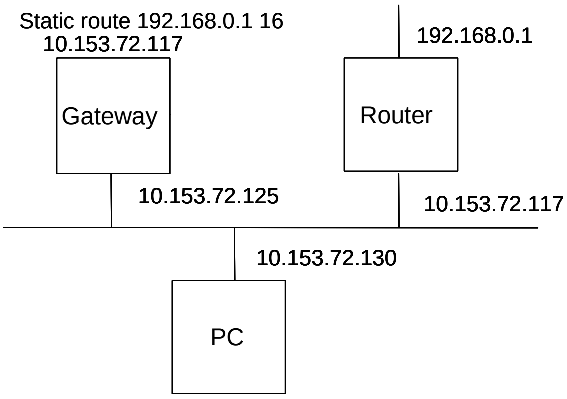


Figure 10-1 Network diagram for configuring the sending of ICMP Redirect messages

As shown in the above figure, when the PC wants to send a packet to the Router, it first sends the packet to the Gateway. With the sending of ICMP Redirect messages disabled, the Gateway forwards the packet directly to the Router. With the function enabled, the Gateway sends back an ICMP Redirect message to redirect the PC to the Router.

Perform the following configuration in system view.

Table 10-4 Configure the sending of ICMP Redirect messages

Operation	Command
Enable the sending of ICMP Redirect messages	**icmp redirect send**
Disable the sending of ICMP Redirect messages	**undo icmp redirect send**

By default, the sending of ICMP Redirect messages is enabled.

10.5 Displaying and Debugging IP Performance

After the above configuration, execute the **display** command in all views to display the running of the IP Performance, and to verify the effect of the configuration.

Execute the **reset** command in user views to clear the running statistic information.

Execute the **debugging** command in user view for the debugging of IP Performance.

Table 10-5 Display and debug of IP performance

Operation	Command
Show TCP connection state	**display tcp status**
Show TCP traffic statistic information	**display tcp statistics**
Show information on the IP layer interface table.	**display ip interface** [*interface-type interface-number*]
Show information on the FIB of interface cards.	**display fib**
Output rows that include the string defined by *text* from the cache in regular expressions.	**display fib** [**|** { **begin** | **include** | **exclude** } *text*]
Show the filtered FIB information.	**display fib acl** *acl-number*
Show FIB entries by destination address.	**display fib** *dest-addr1* [*dest-mask2*] [**longer**]
Show FIB entries with destination addresses in the range *dest-addr1 dest-mask1* to *dest-addr2 dest-mask2*.	**display fib** *dest-addr1 dest-mask1 dest-addr2 dest-mask2*
Show in certain format FIB entries that are filtered in by the rules in the specified IP-prefix list.	**display fib ip-prefix** *listname*
Show the total number of FIB entries.	**display fib statistics**
Enable IP information debugging	**debugging ip packet**
Enable ICMP debugging.	**debugging ip icmp**
Enable TCP information debugging	**debugging tcp packet**
Clear IP statistics.	**reset ip statistics**

Operation	Command
Enable UDP information debugging	**debugging udp packet**
Disable UDP connection debugging.	**undo debugging udp packet**
Clear TCP traffic statistics.	**reset tcp statistics**
Show information on all the current socket interfaces in the system.	**display ip socket**
Disable TCP connection debugging.	**undo debugging tcp packet**
Enable TCP event debugging	**debugging tcp event**
Disable TCP event debugging.	**undo debugging tcp event**
Show UDP traffic statistics.	**display udp statistics**
Clear UDP traffic statistics.	**reset udp statistics**

10.6 Configuring Broadcast Forwarding on an Interface

10.6.1 Configuring Broadcast Forwarding on an Interface

Normally routers do not forward layer 2 broadcasts. You may however configure them to do that for special applications, cross-network wake on LAN (WOL) for example, to forward Wakeup frames to a specified network.

Perform the following configuration in interface view.

Table 10-6 Configure broadcast forwarding on the interface

Operation	Command
Configure broadcast forwarding on the current interface	**ip forward-broadcast** [*acl-number*]
Disable broadcast forwarding on the current interface	**undo ip forward-broadcast**

By default, the router does not forward broadcasts.

10.6.2 Configuration Example for Implementing Remote WOL with Routers

I. Network requirements

PC 1 is installed with wakeup software, magic packet.exe for example, in order to wake up all PCs on the remote network segment 192.168.1.0/24.

Configure to ensure that:

- The 192.168.1.0/24 segment is reachable to PC 1.

- All PCs on 192.168.1.0/24 support remote wakeup and the wakeup function must work with power supplies, network adapters, and main boards.
- Enable broadcast forwarding on interface Ethernet 1/0/1 on the router.
- Ensure that only the Wakeup frames from the 192.168.2.1 segment are forwarded to the 192.168.1.0/24 segment.

II. Network diagram

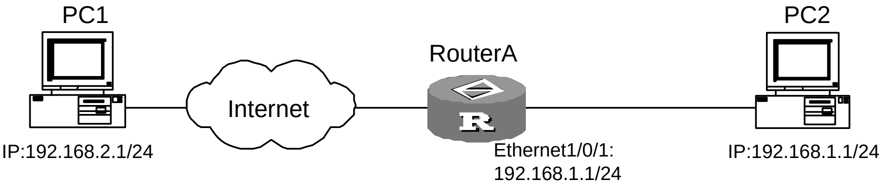


Figure 10-2 Network diagram for implementing remote WOL with routers

III. Configuration procedure

Configure Router A:

```
<RouterA> system-view
[RouterA] interface Ethernet1/0/1
[RouterA-Ethernet1/0/1] ip address 192.168.1.2 24
[RouterA-Ethernet1/0/1] ip forward-broadcast 2100
[RouterA-Ethernet1/0/1] quit
[RouterA] acl number 2100
[RouterA-acl-basic-2100] rule 1 permit source 192.168.2.1 0
[RouterA-acl-basic-2100] rule 2 deny source any
```

10.7 Configuring Unicast Fast Forwarding

10.7.1 Brief Introduction to Unicast Fast Forwarding

Message forwarding efficiency is a key feature evaluating router performance. According to regular flow, when a message arrives, the router will copy it from the interface memory to the main CPU. The CPU specifies the network ID from the IP address, consults with the routing table to get the best path for forwarding the message, and encapsulates a link layer frame header for the message. The resulted frame is then copied to the output queue via DMA (Direct Memory Access), and during this process the main system bus is passed twice. This process can be repeated for message forwarding.

In the unicast fast forwarding, cache is used to process messages. After the first message is forwarded by searching routing table, corresponding exchange information is generated in the cache, and forwarding of the following same messages can be realized by directly searching the cache. This practice simplifies the queuing of IP messages, and cuts down the route finding time and improves forwarding throughput of IP messages. Since the forwarding table in the cache has been optimized, much quicker searching speed can be obtained.

The unicast fast forwarding implemented by V 2.41 provides:

- Unicast fast forwarding on all types of high-speed link interfaces (including subinterfaces), such as Ethernet, synchronous PPP, frame relay, and HDLC.
- Unicast fast forwarding in presence of normal firewall.
- Unicast fast forwarding in presence of ASPF firewall.
- Unicast fast forwarding when NAT is configured.
- Unicast fast forwarding when GRE is in use.
- Significantly improved forwarding efficiency.

The performance of unicast fast forwarding sometimes will be affected by some characteristics such as message queue management and message header compression. Unicast fast forwarding is not conducted for fragmented messages.

10.7.2 Configuring Unicast Fast Forwarding

You can disable fast-forwarding as needed. For example, if load balance is required when forwarding packets, fast-forwarding must be disabled in the forwarding direction of the interface.

Perform the following configuration in interface view.

Table 10-7 Enable/disable unicast fast forwarding on an interface

Operation	Command
Enable unicast fast forwarding in both directions of the interface	**ip fast-forwarding**
Enable unicast fast forwarding on the inbound interface	**ip fast-forwarding inbound**
Enable unicast fast forwarding on the outbound interface	**ip fast-forwarding outbound**
Disable unicast fast forwarding on the interface	**undo ip fast-forwarding**

By default, unicast fast forwarding is enabled in the input/output directions of the interface.

⚠ **Caution:**

To have an interface participate in load balancing, you must disable fast forwarding on it in the forwarding direction.

If fast-forwarding is configured on an interface, the debugging information of the IP packets on the interface will not be displayed, namely, the **debugging ip packet** command does not work.

10.7.3 Displaying and Debugging Unicast Fast Forwarding

Table 10-8 Display and debug unicast fast forwarding

Operation	Command
Display contents in the unicast fast forwarding cache	**display ip fast-forwarding cache**
Clear contents in the unicast fast forwarding cache	**reset ip fast-forwarding cache**

When fast-forwarding on the same interface is configured, ICMP redirect messages will not be sent again when IP messages pass the same interface. Otherwise, ICMP reorientation messages needs to be sent while messages are forwarded.

10.8 Multicast Fast Forwarding Configuration

10.8.1 Introduction to Multicast Fast Forwarding

Packet forwarding efficiency is a critical index for evaluating the performance of a router. Normally, when a router receives a packet, it copies the packet from the buffer of the interface to the main CPU. The CPU determines the ID of the destination network, looks it up in the routing table for the optimal route, encapsulates the packet with a link layer frame header, and then copies the resulted frame from the DMA to the output queue. This procedure uses the bus of the main system twice. The router repeats this procedure to forward each packet.

Fast forwarding employs a cache to handle packets based on data stream technology. Almost all data on the Internet is based on data stream, and a data stream represents a specific application between two specified hosts on the Internet. For example, an FTP operation transfers a file. A data stream is usually described with a 5-tuple, including the source IP address, source port number, destination IP address, destination port number, and protocol number.

For the first packet of a data stream, the router looks up the routing table for the routing decision, while for the subsequent packets of the stream, it looks up the cached fast forwarding table, which is optimized. This greatly reduces the IP packet queuing procedure, decreases the route lookup time and improves the forwarding throughput of IP packets.

The multicast fast forwarding function has the following features:

- Supports high speed link interfaces of various types, including Ethernet, ATM, synchronous PPP, FR, and HDLC.
- Supports environments with packet filtering firewalls.
- Supports environments in which QoS is configured.
- Improves packet forwarding efficiency dramatically.

10.8.2 Configuring Multicast Fast Forwarding

Enable multicast fast forwarding as needed.

Perform the following configuration in interface view.

Table 10-9 Enable/disable multicast fast forwarding on an interface

Operation	Command
Enable multicast fast forwarding on an interface	**ip multicast-fast-forwarding**
Disable multicast fast forwarding on an interface	**undo ip multicast-fast-forwarding**

By default, multicast fast forwarding is disabled on an interface.

10.8.3 Displaying and Debugging Multicast Fast Forwarding

Table 10-10 Display and debug multicast fast forwarding

Operation	Command
Display information about the multicast fast forwarding table.	**display ip multicast-fast-forwarding cache** [*multicast-group*]
Clear the contents in the multicast fast forwarding cache	**reset ip multicast-fast-forwarding cache**

10.9 IP Performance Configuration Troubleshooting

Fault 1: TCP and UDP are established on IP to provide the transmission of data packets. The problem is that TCP and UDP cannot work normally.

Troubleshooting: In the event of such a fault, you can enable the corresponding debugging information output to view the debugging information.

- Use the command **debugging udp** to enable the UDP debugging information output to trace the UDP packet. When the router sends or receives UDP packets, the content format of the datagram can be displayed in real time. You can locate the problem from the contents of the datagram.

The following are the UDP packet formats:

```
*0.348541898-SOCKET-8-UDPINI:UDP packet information :
Incoming UDP datagram:
source IP address:   172.16.101.70
source port:   138
destination IP address:   172.16.255.255
destination port:   138
The length of UDP packet:   209
```

- Use the command **debugging tcp packet** to enable the TCP debugging information output to trace the TCP packets. Two TCP packet formats are available for selection. One is to debug and trace the receiving and sending of all the TCP packets of the TCP connection that take this device as one end. The operations are as follows:

```
[3Com] info-center enable
[3Com] quit
<3Com> debugging tcp packet
```

Then the TCP packets received or sent can be checked in real time. Specific packet formats are as follows:

```
*0.348623498-SOCKET-8-OUTBAND:TCP packet information :
TCP output packet:
source IP address:   172.16.201.1
source port:   23
destination IP address:   172.16.105.148
destination port:   1031
packet sequence number:   4818317
ACK sequence number:   3644122
The packet flags:  ACK  PUSH
The total length of IP packet:   436
The length of TCP header:   20
```

The other is to debug and trace the packets with SYN, FIN or RST flags being set.

Operations are as follows:

```
[3Com] info-center enable
[3Com] quit
<3Com> debugging tcp event
```

Then the TCP packets received or sent can be checked in real time, and the formats are similar to those mentioned above.

Chapter 11 NAT Configuration

11.1 NAT Overview

As described in RFC1631, Network Address Translation (NAT) is to translate the IP address in IP data packet header into another IP address, which is mainly used to implement private network accessing external network in practice. NAT can reduce the depletion speed of IP address space via using several public IP addresses to represent multiple private IP addresses.

Note:

Private address denotes the address of network or host on intranet, whereas public address denotes the universal unique IP address on Internet.
IP addresses that RFC1918 reserves for private and private use are.
Class A: 10.0.0.0 to 10.255.255.255 (10.0.0.0/8)
Class B: 172.16.0.0 to 172.31.255.255 (172.16.0.0/12)
Class C: 192.168.0.0 to 192.168.255.255 (192.168.0.0/16)
IP addresses in the above three ranges will not be assigned in the Internet, so they can be used in the intranet by a company or enterprise with no need for requesting ISP or register center.

A basic NAT application is shown in the following figure.

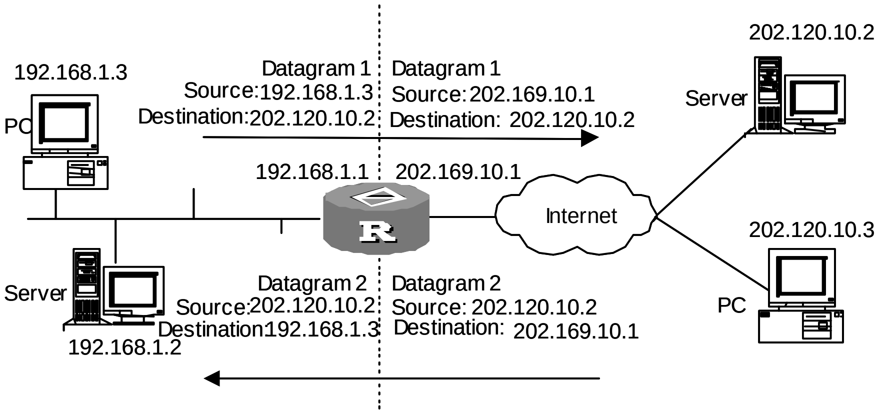


Figure 11-1 Network diagram for basic processes of address translation

NAT server such as the Router is located at the joint between private network and public network. When the internal PC at 192.168.1.3 sends the data packet1 to the external server at 202.120.10.2, the data packet will traverse the NAT server. The NAT server checks the contents in the packet header. If the destination address in the header is an extranet address, the server will translate the source address 192.168.1.3 into a valid public address on the Internet 202.169.10.1, then forward the packet to the external server and record the mapping in the network address translation list. The external server sends the response packet2 (The destination is 202.169.10.1) to the NAT server. After inquiring the network address translation list, the NAT server replaces the destination address in packet2 header with the original private address 192.168.1.3 of the internal PC.

The above mentioned NAT process is transparent for terminals such as the PC and server in the above figure. NAT “hides” the private network of an enterprise because the external server regards 202.169.10.1 as the IP address of the internal PC without the awareness of the existence of 192.168.1.3.

The main benefit NAT offers is the easy access to the outside resources for the intranet hosts while maintaining the privacy of the inner hosts.

- Since it is necessary to translate the IP address translation of data packets, the header of the data packet related to IP address cannot be encrypted. For example, encrypted FTP connection is forbidden to be used. Otherwise, FTP port cannot be correctly translated.
- Network debugging becomes more difficult. For instance, while a certain internal network host attempts to attack other networks, it is hard to point out which computer is malicious, for the host IP address is shielded.
- NAT has little impact on the performance of the network for the 10Mbit/s bandwidth links, for the bottleneck is the data transfer circuit. When the baud rate is over 10Mbits/s, NAT will cause some certain effects upon the performance of the route.

11.2 Functions Provided by NAT

11.2.1 Many-to-Many Address Translation and Address Translation Control

Based on the above figure, the source address of the intranet will be translated into an appropriate extranet address (the public address of the outbound interface on the NAT server in the above figure) via NAT. In this way, all the hosts in the intranet share one extranet address when they access the external network. In other words, only one host can access the external network at a time when there are many access requirements, which is called “one-to-one address translation”.

An extended NAT implements the concurrent access, that is, multiple public IP addresses are assigned to a NAT server. The NAT server assigns a public address IP1 to a requesting host, keeps a record in the address translation list and forwards the data packet, then assigns another public address IP2 to another request host and so on. This is called “many-to-many address translation”.

🕮 **Note:**

The number of public IP addresses on the NAT server is far less than the number of hosts in the intranet because not all hosts will access the extranet at one time. The public IP address number is determined based on the maximum number of intranet hosts at the rush hour of the network.

In practice, it may be required that only some intranet hosts can access the Internet (external network). In other words, the NAT server will not translate source IP addresses of those unauthorized hosts, which is called address translation control.

Router implements many-to-many address translation and address translation control via address pool and ACL respectively.

- Address pool: A set of public IP addresses for address translation. A client should configure an appropriate address pool according to its valid IP address number, internal host number as well as the actual condition. An address will be selected from the pool as the source address during the translation process.
- ACL-based address translation: Only the data packet matching the ACL rule can be translated, which effectively limits the address translation range and allows some specific hosts to access Internet.

11.2.2 NAPT

There is another way to implement the concurrent access, that is, Network Address Port Translation (NAPT), which allows the map from multiple internal addresses to an identical public address. Therefore, it can be called as “many-to-one address translation” or address multiplex informally.

NAPT maps IP addresses and port numbers of data packets form various internal addresses to an identical public address with different port numbers. In this way, different internal addresses can share an identical public address.

The fundamentals of NAPT are shown in the following figure.

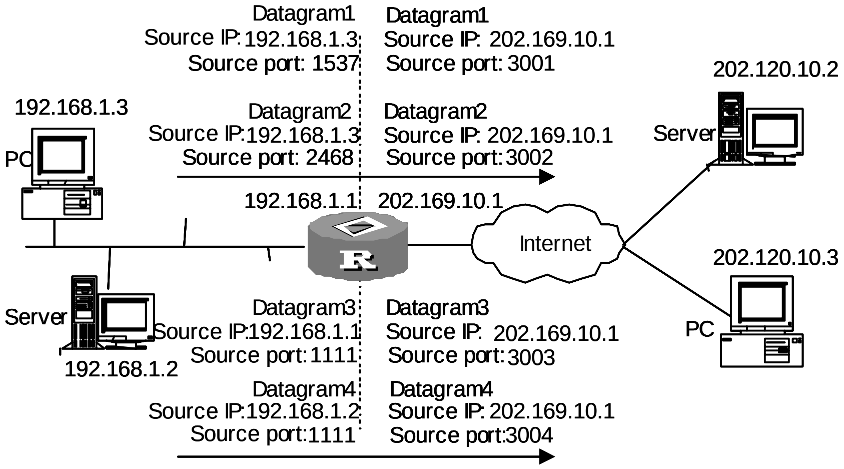


Figure 11-2 NAPT allowing multiple internal hosts to share a public address

As shown in the above figure, four data packets from internal addresses arrive at the NAT server. Among them, packet1 and packet2 come from the same internal address with different source port number, pakcet3 and packet4 come from different internal addresses with an identical source port number. After the NAT mapping, all the 4 packets are translated into an identical public address with different source port numbers, so they are still different from each other. As for the response packets, the NAT server can also differentiate these packets based on their destination addresses and port numbers and forward the response packets to the corresponding internal hosts.

11.2.3 Static Net-to-Net NAT

Static net-to-net NAT maps an internal network address range to a public network address range. This approach to NAT only involves the net ID portion of the IP address. The host ID portion remains unchanged after address translation.

Static net-to-net NAT allows an internal host to access an external network through and to be accessed at its associated public address.

Static net-to-net NAT creates direct mapping between internal host addresses and public network addresses, and implements the function similar to NAT server.

However, static net-to-net NAT requires a large IP address space since it holds a one-to-one mapping between internal host addresses and public network addresses. To save IP address resources, you can use it with conventional static or dynamic NAT but should note to avoid address conflicts.

11.2.4 Bidirectional NAT

In comparison to conventional NAT which translates only the source or destination address, bidirectional NAT translates both addresses. It is suitable for the situation where the addresses of the hosts on your intranet overlap.

As shown in Figure 11-3, the addresses of the internal host PC 1 and the host PC 3 overlap. Normally, if PC 1 or PC 2 sends a packet to PC 3, the packet will be forwarded to PC 1 instead of the intended destination.

To ensure correct forwarding, you may configure bidirectional NAT on Router A on the basis of conventional NAT. By mapping an overlapping address pool to a temporary address pool, you can have the router translate the overlapping address into a unique temporary address.

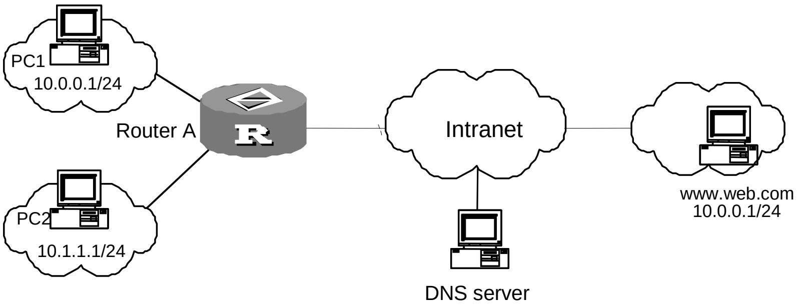


Figure 11-3 Bidirectional NAT implementation

To configure bidirectional NAT on Router A, do the following:

Step 1: Configure conventional NAT, for example, many-to-many address translation.

Configure a NAT address pool with the range of 200.0.0.1 to 200.0.0.100, and apply it to the WAN interface.

Step 2: Map an overlapping address pool to a temporary address pool, for example, 10.0.0.0 to 3.0.0.0, both with a 24-bit subnet mask.

The following are the translation conventions:

- Temporary address = Start address of the temporary address pool + (overlapping address – start address of the overlapping address pool)
- Overlapping address = Start address of the overlapping address pool + (temporary address – start address of the temporary address pool)

When PC 2 uses the domain name of PC 3 to access PC 3, packets are processed as follows:

1) PC 2 sends a DNS request for resolving www.web.com. The DNS server on the private network processes the request and sends a DNS response to Router A. Router A checks the response, and finds out that the resolved address 10.0.0.1 is an overlapping address; then it translates this address to its corresponding temporary address 3.0.0.1. After that, Router A translates the destination address

in the DNS response following the conventional NAT procedures and sends the DNS response to PC 2.

2) PC 2 initiates an access to 3.0.0.1, the temporary address for www.web.com. When Router A receives this request, it first translates the source address following the conventional NAT procedures, and then translates the destination address, which is temporary, to 10.0.0.1, the corresponding overlapping address.
3) Router A sends the request out its outgoing interface, and the request is forwarded across the WAN hop by hop to PC 3.
4) When receiving the response from PC 3, Router A checks it and finds out that the source address 10.0.0.1 is an overlapping address. The router then translates this address to its corresponding temporary address, 3.0.0.1. After translating the destination address following the conventional NAT procedures, Router A sends the response back to PC 2.

11.2.5 Internal Server

NAT can “shield” internal hosts via hiding the architecture of the intranet. However, there are times that you want to permit some hosts on external networks to access some hosts on the intranet, such as a WWW server or a FTP server. You can flexibly add servers on the intranet via NAT, for example, you can use 202.169.10.10 as the external address of the WWW server and 202.110.10.11 as the external address of the FTP server. Even 202.110.10.12:8080 can be used as the external address of the WWW server. Moreover, NAT can provide multiple identical servers such as WWW servers for external clients.

The NAT function on 3Com Series Routers provides some servers on the intranet for some hosts on external networks. When a client on an external network accesses a server on the intranet, the NAT device translates the destination address in the request packet into a private address on the internal server and translates the source address (a private address) in the response packet into a public address.

11.2.6 Easy IP

Easy IP is to use the public IP address of an interface as the source address after the address translation. It also controls the address translation based on ACL.

11.2.7 NAT Support for ALG

Network translation may result in malfunction of many application protocols. These protocols are NAT-sensitive. Some of their packets require special treatment on the IP address and port number in the valid payload, to ensure normal subsequent protocol interaction.

Application level gateway (ALG) of NAT is a common approach to NAT traversal. It substitutes the IP address and port number in payload according to address translation rules. For the involved protocol, this is transparent. So far, V 2.41's NAT ALG implementation supports point to point tunneling protocol (PPTP), DNS, FTP, Internet locator service (ILS), NetBIOS over TCP/IP (NBT), session initiation protocol (SIP), and H.323.

11.2.8 Multi-Instance of MPLS VPN NAT Supported

NAT multi-instance function offers a solution that allow not only the VPN users to access the Internet from inner network, but also the MPLS VPN users to access the Internet through a single gateway, as well as the users from different VPNs to use the same private address. When an MPLS VPN user wants to access the Internet, NAT translates the IP address and the port of the internal host into external IP address and port and records the MPLS VPN information (such as protocol type and route identifier RD) about the user. When the packet is sent back, NAT restores the external IP address and port to the IP address and port of the internal host, and recognizes the MPLS VPN user. No matter what kind of NAT it is, PAT or NO-PAT, multi-instance will be supported.

V 2.41 NAT supports the multi-instance of internal server, and provides the outside network with the access to the hosts within MPLS VPN. For example, the WWW server in VPN1 uses the address of 10.110.1.1 as the inner address, on the other hand, uses the address of 202.110.10.20 as the outer address. Using the outer address (202.110.10.20), the Internet users can get the WWW service provided by MPLS VPN1.

11.3 NAT Configuration

NAT configuration includes:

- Configure address pool
- Configure NAT
- Configure Easy IP
- Configure static NAT
- Configure many-to-many NAT
- Configure NAPT
- Configure internal server
- Configure NAT ALG
- Configuring NAT entries for domain names
- Configure NAT effective time (optional)

11.3.1 Configuring Address Pool

The address pool is a collection of some consecutive IP addresses, while internal data packet needs to access external network via NAT, a certain address in the address pool will be chosen as the source address. Perform the following configurations in the system view.

Table 11-1 Configure address pool

Operation	Command
Define an address pool	**nat address-group** *group-number start-addr end-addr*
Delete an address pool	**undo nat address-group** *group-number*

📖 **Note:**

An address pool is irremovable while this address pool has set up the association with a certain access control list for NAT.
If easy IP is the one and only function supported by the router, the address of the interface will be used plainly as the translated IP address, no NAT pool needed.

11.3.2 Configuring NAT

The NAT is accomplished by associating address pool with ACL. The association creates a relationship between such IP packets, characterized in the ACL, and that addresses, defined in the address pool. When a packet is transferred from inner network to outer network, first, the packet is filtered by the ACL to let it out, then the association between the ACL and address pool is used to find an address, which will later serve actually as the translated address.

The configuration of ACL is discussed in relevant sections.

The configuration varies from kinds to kinds of NAT.

I. Easy IP

The NAT command without the **address-group** parameter functions as the **nat outbound** *acl-number* command, implementing the "easy-ip" feature. When performing address translation, the IP address of the interface is used as the translated address and the ACL can be used to control which addresses can be translated.

Perform the following configuration under the interface view.

Table 11-2 Configure Easy IP

Operation	Command
Add association for access control list and address pool	**nat outbound** *acl-number*
Delete association for access control list and address pool	**undo nat outbound** *acl-number*

Suppose that you directly take the interface address as the public network address after NAT. If you change the interface address in order to visit the external network, you must use the **reset nat session** command to clear the original NAT address mapping entry, otherwise, the NAT entry can neither be deleted automatically, nor be deleted by the command **reset nat**.

II. Using the IP address of a loopback interface for address translation

Perform the following configuration in interface view.

Table 11-3 Use the IP address of a loopback interface for address translation

Operation	Command
Associate an ACL with a Loopback interface	**nat outbound** *acl-number* **interface** *interface-type interface-number*
Remove the association of the ACL to the loopback interface	**undo nat outbound** *acl-number* **interface** *interface-type interface-number*

The IP address of the specified loopback interface is used to substitute for the source addresses of the packets matching the ACL.

III. Configuring static NAT

1) Configure a one-to-one static NAT entry

Perform the following configuration in system view.

Table 11-4 Configure a one-to-one static NAT entry

Operation	Command
Configure a static one-to-one private-to-public NAT entry	**nat static** *ip-addr1 ip-addr2*
Delete an existing static one-to-one private-to-public NAT entry	**undo nat static** *ip-addr1 ip-addr2*

2) Configure static net-to-net NAT

In comparison to conventional static NAT, static net-to-net NAT only involves the net ID portion of the IP address. The host ID portion remains unchanged after address translation.

Perform the following configuration in system view.

Table 11-5 Configure a static net-to-net NAT map

Operation	Command
Create a static net-to-net NAT map entry	**nat static net-to-net** *inside-start-address inside-end-address* **global** *global-address mask*
Delete a static net-to-net NAT map entry	**undo nat static net-to-net** *inside-start-address inside-end-address* **global** *global-address mask*

The static NAT entries configured using the **nat static net-to-net** command must not conflict with those configured using the **nat static** command.

3) Applying static NAT on the interface

Table 11-6 Apply static NAT on the interface

Operation	Command
Apply static NAT on the interface	**nat outbound static**

IV. Configuring many-to-many NAT

The many-to-many NAT is accomplished by associating the ACL with the NAT pool.

Perform the following configuration under the interface view.

Table 11-7 Configure many-to-many NAT

Operation	Command
Add association for access control list and address pool	**nat outbound** *acl-number* [**address-group** *group-number* [**no-pat**]]
Delete association for access control list and address pool	**undo nat outbound** *acl-number* [**address-group** *group-number* [**no-pat**]]

V. Configuring NAPT

While associating the ACL and NAT pool, the selected **no-pat** parameter denotes that only the IP address but the port information is translated, i.e. not using NAPT function; whereas the omit of the **no-pat** parameter denotes using the NAPT function.

By default, the NAPT function is active.

Perform the following configuration in interface view.

Table 11-8 Configure NAPT

Operation	Command
Add association for access control list and address pool	**nat outbound** *acl-number* [**address-group** *group-number*]
Delete association for access control list and address pool	**undo nat outbound** *acl-number* [**address-group** *group-number*]

VI. Configuring NAT Multi-instance

Easy IP, many-to-many NAT and NAPT whatsoever all support the configuration of NAT multi-instance. And all the works to be done to support **MPLS VPN** is to add **vpn–instance** *vpn-instance-name* option into the **rule** command in ACL view to show clearly which MPLS VPN user needs translation,

11.3.3 Configuring Bidirectional NAT

Perform the following configuration in system view.

Table 11-9 Configure a bidirectional NAT entry

Operation	Command
Configure a bidirectional NAT entry, mapping an overlapping address pool to a temporary address pool	**nat overlapaddress** *number overlappool-startaddress temppool-startaddress* { **pool-length** *pool-length* | **address-mask** *mask* }
Remove a bidirectional NAT entry	**undo nat overlapaddress** *number*

11.3.4 Configuring Internal Server

By configuring internal server, the related external address and port can be mapped into the internal server, thus enabling the function of external network accessing the internal server.

The mapping table for internal server and external network is configured by the **nat server** command.

The information user needs to provide includes external address, external port, internal server address, internal server port and the protocol type of the service.

If the internal server belongs to a MPLS VPN, it is necessary to specify the *vpn-instance-name.* Otherwise the internal server will be regarded to be in an ordinary VPN rather than a MPLS VPN,

Perform the following configuration in the interface view.

Table 11-10 Configure internal server

Operation	Command
Add an internal server	**nat server** [*acl-number*] [**vpn-instance** *vpn-instance-name*] **protocol** *pro-type* **global** *global-addr* [*global-port*] **inside** *host-addr* [*host-port*] **nat server** [*acl-number*] [**vpn-instance** *vpn-instance-name*] **protocol** *pro-type* **global** *global-addr global-port* 1 *global-port2* **inside** *host-addr1 host-addr2 host-port*
Delete an internal server	**undo nat server** [*acl-number*] [**vpn-instance** *vpn-instance-name*] **protocol** *pro-type* **global** *global-addr* [*global-port*] **inside** *host-addr* [*host-port*] **undo nat server** [*acl-number*] [**vpn-instance** *vpn-instance-name*] **protocol** *pro-type* **global** *global-addr global-port1 global-port2* **inside** *host-addr1 host-addr2 host-port*

Note:

While either one of the *global-port* and *inside-port* being defined as “any”, the other one must either be defined as “any” or not be defined.

11.3.5 Configuring NAT ALG

Perform the following configuration in system view.

Table 11-11 Configure NAT ALG

Operation	Command
Configure NAT ALG	**nat alg** { **dns | ftp | h323 | ils | nbt | pptp | sip** }
Disable NAT ALG	**undo nat alg** { **dns | ftp | h323 | ils | nbt | pptp | sip** }

By default, NAT ALG is enabled.

11.3.6 Configuring NAT Entries for Domain Names

Given an internal network that has no DNS server, you may configure NAT entries for domain names to allow internal hosts to identify and access internal servers (such as FTP and WWW) by domain name.

Perform the following configuration in system view.

Table 11-12 Configure a NAT entry for a domain name

Operation	Command
Map a domain name to a triplet of external IP address, port number, and protocol type	**nat dns-map** *domain-name global-addr global-port* [**tcp** | **udp**]
Delete the NAT entry for a domain name	**undo nat dns-map** *domain-name*

You may configure up to 16 NAT entries for domain names.

11.3.7 Configuring Address Translation Lifetimes

Since the Hash table used by NAT will not exist forever, the user can configure the lifetime of the Hash table for protocols such as TCP, UDP and ICMP respectively. If the Hash table is not used in the set time, the connection as well as the table it uses will be outdated.

For example, the user with the IP address 10.110.10.10 sets up an external TCP connection using port 2000, and NAT assigned corresponding address and port for it, but in a defined time, this TCP connection is not in use, the system will delete this connection.

Perform the following configuration in the system view.

Table 11-13 Configure address translation lifetime values

Operation	Command
Configure address translation lifetime values	**nat aging-time** { **default** | { **dns** | **ftp-ctrl** | **ftp-data** | **icmp** | **pptp** | **tcp** | **tcp-fin** | **tcp-syn** | **udp** } *seconds* }

If the **nat aging-time default** command is configured, the default address translation lifetime values of the system apply.

Following are the default address translation lifetime values for different protocols:

DNS: 60 seconds

FTP control link: 7200 seconds

FTP data link: 240 seconds

PPTP: 86400 seconds

TCP: 86400 seconds

TCP FIN (or RST)/SYN connection: 60 seconds

UDP: 300 seconds

ICMP: 60 seconds

11.4 Displaying and Debugging NAT

After the above configuration, execute the **display** command in all views to display the running of the NAT configuration, and to verify the effect of the configuration.

Execute the **reset** command in user views to clear the running.

Execute the **debugging** command in user view for the debugging of NAT.

Table 11-14 Display and debug NAT

Operation	Command
Check NAT status	**display nat** { **address-group** | **aging-time** | **all** | **outbound** | **server** | **statistics** | **session** [**vpn-instance** *vpn-instance-name*] [**slot** *slot-number*] [**destination** *ip-addr*] [**source global** *global-addr* | **source inside** *inside-addr*] }
Enable the debugging of NAT	**debugging nat** { **alg** | **event** | **packet** [**interface** { *interface-type interface-number*] }
Disable the debugging of NAT	**undo debugging nat** { **alg** | **event** | **packet** [**interface** *interface-type interface-number*] }
Clear NAT mapping table	**reset nat**{ **log-entry** | **session slot** *slot-number* }

11.5 NAT Configuration Example

11.5.1 Typical NAT Configuration

I. Network requirements

An enterprise is connected to WAN by the address translation function of router. It is required that the enterprise can access the Internet via serial 3/0/0 of the router, and provide www, ftp and smtp services to the outside, as well as two WWW servers. The internal network address of the enterprise is 10.110.0.0/16.

The internal ftp server address is 10.110.10.1. The internal www server1 address is 10.110.10.2. The internal www server 2 address is 10.110.10.3. The internal smtp server address is 10.110.10.4. It is expected to provide uniform server IP address to the outside. Internal network segment 10.110.10.0/24 may access Internet, but PC on other segments cannot access Internet. External PC may access internal server. The enterprise has six legal IP addresses from 202.38.160.100 to 202.38.160.105.

Choose 202.38.160.100 to be the external IP address of the enterprise, and www server2 uses 8080 port to the outside.

II. Network diagram

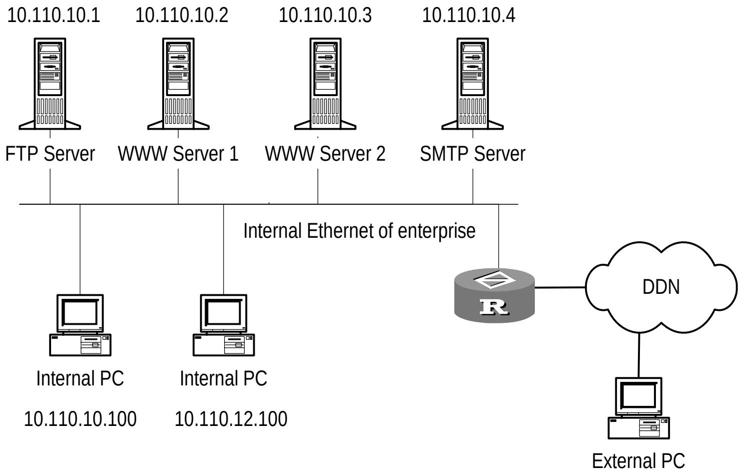


Figure 11-4 Network diagram for NAT configuration

III. Configuration procedure

# Configure address pool and access control list.

```
[3Com] nat address-group 1 202.38.160.101 202.38.160.105
[3Com] acl number 2001
[3Com-acl-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[3Com-acl-basic-2001] rule deny source 10.110.0.0 0.0.255.255
```

# Allow address translation of segment at 10.110.10.0/24

```
[3Com-Serial3/0/0] nat outbound 2001 address-group 1
```

# Set internal ftp server

```
[3Com-Serial3/0/0] nat server protocol tcp global 202.38.160.100 inside
10.110.10.1 ftp
```

# Set internal www server 1

```
[3Com-Serial3/0/0] nat server protocol tcp global 202.38.160.100 inside
10.110.10.2 www
```

# Set internal www server 2

```
[3Com-Serial3/0/0] nat server protocol tcp global 202.38.160.100 8080 inside
10.110.10.3 www
```

# Set internal smtp server

```
[3Com-Serial3/0/0] nat server protocol tcp global 202.38.160.100 inside
10.110.10.4 smtp
```

11.5.2 Configuration Example of NAT Using IP Address of Loopback Interface

I. Network requirements

As shown in Figure 11-5, the intranet accesses the Internet through the serial interface 3/0/0 on the 3Com router; the internal network segment 10.110.10.0/24 can access the Internet, but other network segments cannot; the internet network segment uses the Loopback interface address 202.38.160.106 as the converted address. The intranet provides WWW, FTP and SMTP services to the outside, and the three servers use the same public address 202.38.160.100.

II. Network diagram

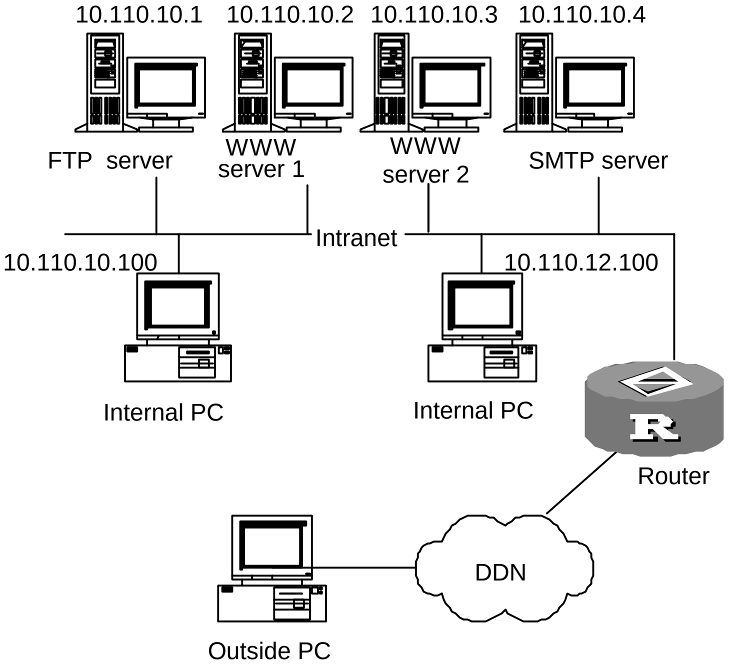


Figure 11-5 Configuration network diagram

III. Configuration procedure

# Configure an ACL.

```
[3Com] acl number 2001
[3Com-acl-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[3Com-acl-basic-2001] rule deny source 10.110.0.0 0.0.255.255
[3Com-acl-basic-2001] quit
```

# Configure the loopback interface.

```
[3Com] interface loopback0
[3Com-LoopBack0] ip address 202.38.160.106
```

```
[3Com-LoopBack0] quit
```

# Configure the internal FTP server.

```
[3Com] interface Serial3/0/0
[3Com-Serial3/0/0] nat server protocol tcp global 202.38.160.100 inside
10.110.10.1 ftp
```

# Configure the internal WWW server 1.

```
[3Com-Serial3/0/0] nat server protocol tcp global 202.38.160.100 inside
10.110.10.2 www
```

# Configure the internal WWW server 2.

```
[3Com-Serial3/0/0] nat server protocol tcp global 202.38.160.100 8080 inside
10.110.10.3 www
```

# Configure the internal SMTP server.

```
[3Com-Serial3/0/0] nat server protocol tcp global 202.38.160.100 inside
10.110.10.4 smtp
```

# Associate the ACL with the loopback interface.

```
[3Com-Serial3/0/0] nat outbound 2001 interface loopback 0
```

11.5.3 Static Net-to-Net NAT Configuration Example

I. Network requirements

As shown in the following diagram, two private networks, Network A and Network B, are connected to the Internet through Router A and Router B respectively. The addresses of both networks are 10.1.1.0/24.

On Network A,

- Router A provides access to the Internet through the WAN interface with IP address 201.1.1.1/24.
- The IP address of PC 1 is 10.1.1.2 and its public IP address on Router A is 211.2.1.2.

On Network B,

- Router B provides access to the Internet through the WAN interface with IP address 201.2.2.2/24.
- The IP address of PC 2 is 10.1.1.2, the same as that of PC 1 on Network A. The public IP address of PC 2 on Router B is 211.2.2.2.

To enable the two private networks to access the Internet and to enable PC 1 and PC 2 to access each other with their respective public addresses, do the following on Router A and Router B:

- On Router A create a static net-to-net NAT entry, translating network address 10.1.1.0/24 to 211.2.1.0/24; and configure dynamic routing, ensuring the route to 211.2.2.0/24 is reachable.
- Likewise, on Router B create a static net-to-net NAT entry, translating network address 10.1.1.0/24 to 211.2.2.0/24; and configure dynamic routing, ensuring the route to 211.2.1.0/24 is reachable.

II. Network diagram

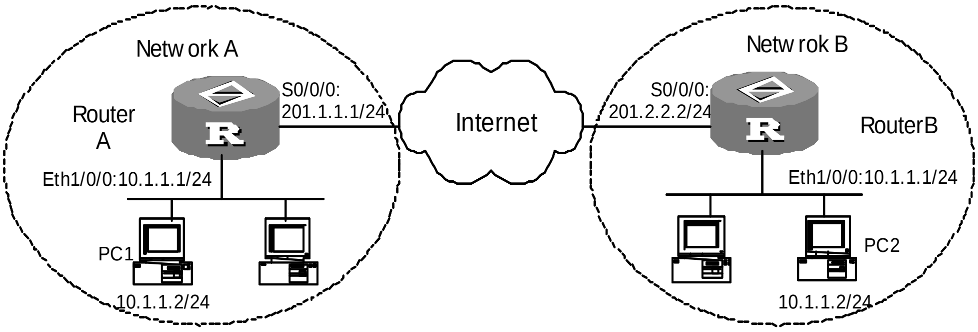


Figure 11-6 Network diagram for static net-to-net NAT

III. Configuration procedure

1) Configure Router A

# Create a static net-to-net NAT entry.

```
[RouterA] nat static net-to-net 10.1.1.1 10.1.1.254 global 211.2.1.0
255.255.255.0
```

# Enable static net-to-net NAT on interface Serial0/0/0.

```
[RouterA] interface serial0/0/0
[RouterA-Serial0/0/0] ip address 201.1.1.1 255.255.255.0
[RouterA-Serial0/0/0] nat outbound static
[RouterA-Serial0/0/0] quit
```

# Configure interface Ethernet1/0/0.

```
[RouterA] interface Ethernet1/0/0
[RouterA-Ethernet1/0/0] ip address 10.1.1.1 255.255.255.0
```

# Configure dynamic routing, ensuring the 211.2.2.0 network segment is reachable.

Omitted

2) Configure Router B

# Create a static net-to-net NAT entry.

```
[RouterB] nat static net-to-net 10.1.1.1 10.1.1.255 global 211.2.2.0
255.255.255.0
```

# Enable static net-to-net NAT on interface Serial0/0/0.

```
[RouterB] interface serial0/0/0
[RouterB-Serial0/0/0] ip address 201.2.2.2 255.255.255.0
[RouterB-Serial0/0/0] nat outbound static
[RouterB-Serial0/0/0] quit
```

# Configure interface Ethernet1/0/0.

```
[RouterB] interface ethernet1/0/0
[RouterB-Ethernet1/0/0] ip address 10.1.1.1 255.255.255.0
```

# Configure dynamic routing, ensuring the 211.2.1.0 network segment is reachable.

Omitted

11.5.4 Bidirectional NAT Configuration Example

I. Network requirements

Figure 11-7 presents a scenario where:

- Two segments of an intranet, 10.0.0.0/24 and 10.1.1.0/24, are connected to Router A. They are merged into one network segment 10.0.0.0/24.
- A DNS server is located on network 192.168.0.0/24.
- On segment 10.0.0.0/24, PC 1 is assigned the IP address 10.0.0.1, the same as that of PC 3.

Configure Router A, the DNS server, and Router B to allow PC 1 and PC 2 to access PC 3 using domain name www.web.com or IP address 3.0.0.1/24.

II. Network diagram

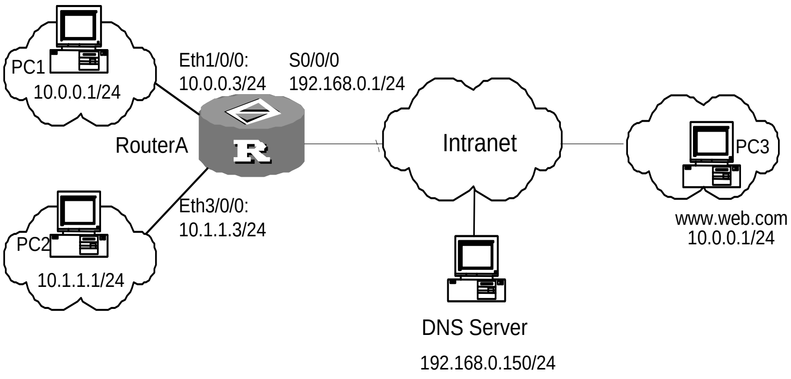


Figure 11-7 Network diagram for bidirectional NAT

III. Configuration procedure

Configure Router A

# Configure a NAT address pool.

```
[3Com] nat address-group 1 2.0.0.1 2.0.0.200
```

# Create a bidirectional NAT entry.

```
[3Com] nat overlapaddress 3 10.0.0.0 3.0.0.0 address-mask 24
```

# Configure an ACL.

```
[3Com] acl number 2000
[3Com-acl-basic-2000] rule 0 permit source 10.0.0.0 0.0.0.255
[3Com-acl-basic-2000] rule 1 permit source 10.1.1.0 0.0.0.255
[3Com-acl-basic-2000] quit
```

# On the WAN interface bind the address pool with the ACL.

```
[3Com] interface serial0/0/0
[3Com-Serial0/0/0] ip address 192.168.0.1 255.255.255.0
[3Com-Serial0/0/0] nat outbound 2000 address-group 1
```

# Assign IP addresses to LAN interfaces.

```
[3Com-Serial0/0/0] interface ethernet 1/0/0
[3Com-Ethernet1/0/0] ip address 10.0.0.3 255.255.255.0
[3Com-Ethernet1/0/0] interface ethernet 3/0/0
[3Com-Ethernet3/0/0] ip address 10.1.1.3 255.255.255.0
[3Com-Ethernet3/0/0] quit
```

# Configure static routing.

```
[3Com] ip route-static 3.0.0.0 255.255.255.0 serial0/0/0
[3Com] ip route-static 192.168.1.0 255.255.255.0 serial0/0/0
```

The IP address of the DNS server is 192.168.0.150/24.

11.5.5 Internal Servers Combined with IPSec VPN

I. Network requirements

The headquarters of a company is connected to the public network through Router 1 and to the branches through IPSec VPNs established over the public network.

All traffic between the headquarters and its branches is protected using IPSec, where manually-established SAs, the security protocol of ESP, the encryption algorithm of DES, and the authentication algorithm of SHA1-HMAC-96 are adopted.

At the headquarters, the WWW and FTP servers are located on the 10.110.10.0 segment. Router 1 provides access to these two internal servers, allowing the internal users to access using private addresses and the external users to access using public addresses.

The PCs of the headquarters and branches are located on 10.110.20.0/24 and 10.110.30.0/24 respectively. They use the address translation service provided by Router 1, accessing the Internet with the public address of interface S1/0/0.

II. Network diagram

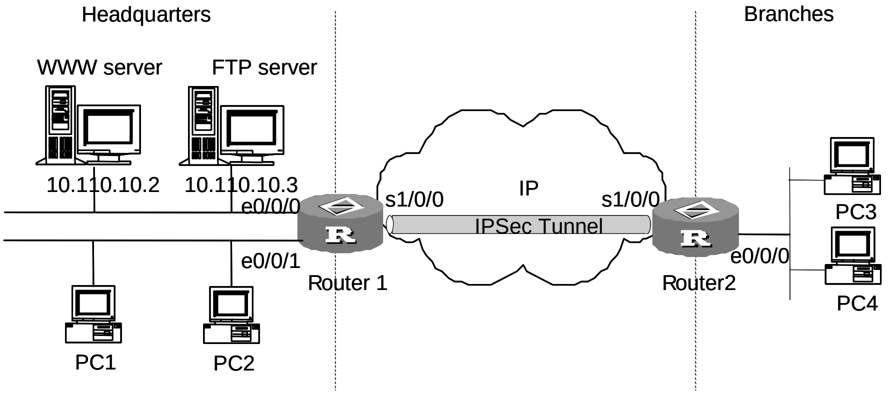


Figure 11-8 Internal servers combined with IPSec VPN

III. Configuration procedure

1) Configure Router 1

# Assign an IP address to interface Ethernet 0/0/0.

```
[3Com] interface ethernet 0/0/0
[3Com-ethernet 0/0/0] ip address 10.110.10.1 255.255.255.0
[3Com-ethernet 0/0/0] interface ethernet 0/0/1
[3Com-ethernet 0/0/1] ip address 10.110.20.1 255.255.255.0
```

# Configure an ACL to control address translation for PCs.

```
[3Com] acl number 2001
[3Com-acl-basic-2001] rule permit ip source 10.110.20.0 0.0.0.255
[3Com-acl-basic-2001] rule permit ip source 10.110.30.0 0.0.0.255
[3Com-acl-basic-2001] rule deny ip source any destination any
```

# Configure an ACL to control access to internal servers.

```
[3Com-acl-basic-2001] acl number 2002
[3Com-acl-basic-2002] rule permit ip source 10.110.10.0 0.0.0.255
[3Com-acl-basic-2002] rule deny ip source 10.110.0.0 0.0.255.255 destination
10.110.30.0 0.0.0.255
[3Com-acl-basic-2002] rule deny ip source any destination any
```

# Configure an ACL, implementing IPSec.

```
[3Com-acl-basic-2002] acl number 2003
[3Com-acl-basic-2003] rule permit ip source 10.110.0.0 0.0.255.255
destination 10.110.30.0 0.0.0.255
[3Com-acl-adv-2003] rule deny ip source any destination any
[3Com-acl-adv-2003] quit
```

# Configure Easy IP.

```
[3Com] interface Serial1/0/0
```

```
[3Com-Serial1/0/0] ip address 202.38.160.1 255.255.255.0
[3Com-Serial1/0/0] nat outbound 2001
```

# Configure the internal FTP and WWW servers.

```
[3Com-Serial1/0/0] nat server 2002 protocol tcp global 202.38.160.1 inside
10.110.10.3 ftp
[3Com-Serial1/0/0] nat server 2002 protocol tcp global 202.38.160.1 inside
10.110.10.2 www
[3Com-Serial1/0/0] quit
```

# Configure IPSec.

```
[3Com] ipsec proposal tran1
[3Com-ipsec-proposal-tran1] encapsulation-mode tunnel
[3Com-ipsec-proposal-tran1] transform esp
[3Com-ipsec-proposal-tran1] esp encryption-algorithm des
[3Com-ipsec-proposal-tran1] esp authentication-algorithm sha1
[3Com-ipsec-proposal-tran1] quit
[3Com] ipsec policy map1 10 manual
[3Com-ipsec-policy-manual-map1-10] security acl 2003
[3Com-ipsec-policy-manual-map1-10] proposal tran1
[3Com-ipsec-policy-manual-map1-10] tunnel remote 202.38.162.1
[3Com-ipsec-policy-manual-map1-10] tunnel local 202.38.160.1
[3Com-ipsec-policy-manual-map1-10] sa spi outbound esp 12345
[3Com-ipsec-policy-manual-map1-10] sa spi inbound esp 54321
[3Com-ipsec-policy-manual-map1-10] sa string-key outbound esp
[3Com-ipsec-policy-manual-map1-10] sa string-key inbound esp gfedcba
[3Com-ipsec-policy-manual-map1-10] quit
```

# Apply the IPSec policy group to interface serial 1/0/0.

```
[3Com] interface serial 1/0/0
[3Com-Serial1/0/0] ipsec policy map1
[3Com-Serial1/0/0] quit
```

# Configure a static route to Router 2.

```
[3Com] ip route-static 10.110.30.0 255.255.255.0 202.38.162.1
```

2) Configure Router 2

# Assign an IP address to interface Ethernet 0/0/0.

```
[3Com] interface ethernet 0/0/0
[3Com-ethernet 0/0/0] ip address 10.110.30.1 255.255.255.0
[3Com-ethernet 0/0/0] quit
```

# Configure an ACL, implementing IPSec.

```
[3Com] acl number 2003
```

```
[3Com-acl-basic-2003] rule permit ip source 10.110.30.0 0.0.0.255 destination
10.110.0.0 0.0.255.255
[3Com-acl-adv-2003] rule deny ip source any destination any
[3Com-acl-adv-2003] quit
```

# Configure IPSec.

```
[3Com] ipsec proposal tran1
[3Com-ipsec-proposal-tran1] encapsulation-mode tunnel
[3Com-ipsec-proposal-tran1] transform esp
[3Com-ipsec-proposal-tran1] esp encryption-algorithm des
[3Com-ipsec-proposal-tran1] esp authentication-algorithm sha1
[3Com-ipsec-proposal-tran1] quit
[3Com] ipsec policy use1 10 manual
[3Com-ipsec-policyl-manual-use1-10] security acl 2003
[3Com-ipsec-policyl-manual-use1-10] proposal tran1
[3Com-ipsec-policyl-manual-use1-10] tunnel remote 202.38.160.1
[3Com-ipsec-policyl-manual-use1-10] tunnel local 202.38.162.1
[3Com-ipsec-policyl-manual-use1-10] sa spi outbound esp 54321
[3Com-ipsec-policyl-manual-use1-10] sa spi inbound esp 12345
[3Com-ipsec-policyl-manual-use1-10] sa string-key outbound esp gfedcba
[3Com-ipsec-policyl-manual-use1-10] sa string-key inbound esp abcdefg
[3Com-ipsec-policyl-manual-use1-10] quit
```

# Assign an IP address to interface serial 1/0/0 and apply the IPSec policy group on the interface.

```
[3Com] interface serial 1/0/0
[3Com-Serial1/0/0] ip address 202.38.162.1 255.0.0.0
[3Com-Serial1/0/0] ipsec policy use1
[3Com-Serial1/0/0] quit
```

# Configure a static route to Router 1.

```
[3Com] ip route-static 10.110.0.0 255.255.0.0 202.38.160.1
```

11.5.6 Domain Name-Related NAT Configuration Example

I. Network requirements

Figure 11-9 presents a scenario where:

- On intranet 10.0.0.0/8 deployed an FTP server and a WWW server.
- The domain name is ftp.zc.com for the FTP server and www.zc.com for the WWW server. The two names can be correctly resolved by external DNS servers.
- The router uses interface Serial0/0/0 to provide access to the external network. The IP address of the serial interface is 1.1.1.1/8.

Configure NAT entries for domain names to allow internal hosts to identify and access the internal servers correctly by domain name.

II. Network diagram

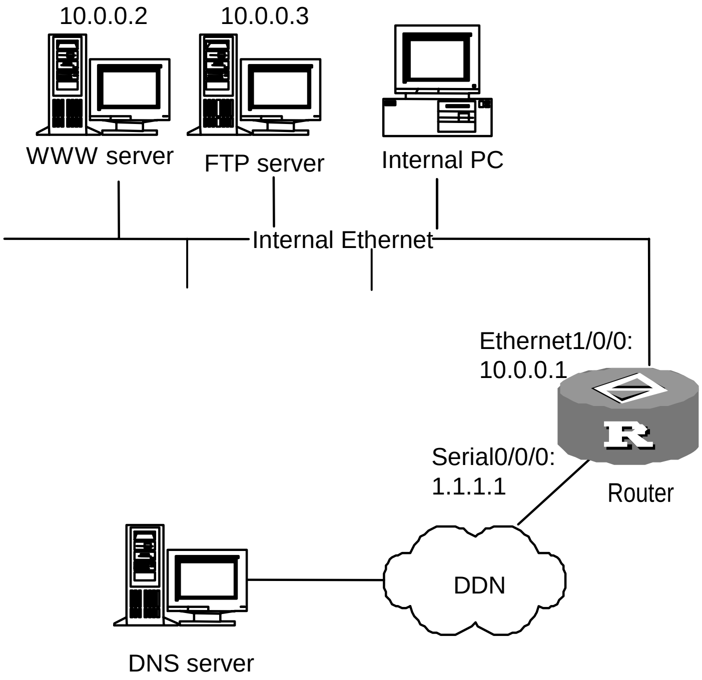


Figure 11-9 Network diagram for domain name-related NAT

III. Configuration procedure

# Configure internal FTP and WWW servers on interface Serial0/0/0.

```
[3Com] interface serial0/0/0
[3Com-Serial0/0/0] ip address 1.1.1.1 255.0.0.0
[3Com-Serial0/0/0] nat outbound 2000
[3Com-Serial0/0/0] nat server protocol tcp global 1.1.1.1 www inside 10.0.0.2
www
[3Com-Serial0/0/0] nat server protocol tcp global 1.1.1.1 ftp inside 10.0.0.3
ftp
[3Com-Serial0/0/0] quit
```

# Configure an ACL, permitting the 10.0.0.0/8 segment to access the Internet.

```
[3Com] acl number 2000
[3Com-acl-basic-2000] rule 0 permit source 10.0.0.0 0.0.0.255
[3Com-acl-basic-2000] rule 1 deny
```

# Configure interface ethernet1/0/0.

```
[3Com] interface ethernet1/0/0
[3Com-Ethernet1/0/0] ip address 10.0.0.1 255.0.0.0
```

After you complete the above configuration tasks, the outside hosts can access the two internal servers by domain name. To allow the internal hosts to access the internal servers by domain name, do the following in addition:

# Map the domain names each to a triplet of external address, port number, and protocol type.

```
[3Com] nat dns-map www.zc.com 1.1.1.1 80 tcp
[3Com] nat dns-map ftp.zc.com 1.1.1.1 21 tcp
```

11.6 Troubleshooting NAT Configuration

Fault 1: address translation abnormal

Troubleshooting: enable the debug for NAT, and refer to **debugging nat** in the **debugging** command for specific operation. According to the Debugging information displayed on the router, initially locate the failure, and then use other commands for further check. Observe the source address after translation carefully, and make sure that it is the expected address. Otherwise, it is possible the configuration of address pool is wrong. Meanwhile, make sure that there is route in the accessed network to return to the address segment defined in the address pool. Take into consideration the influence onto the NAT by the ACL of firewall and address conversion itself, and also route configuration.

Fault 2: internal server abnormal

Troubleshooting: if an external host can not access the internal server normally, check the configuration on the internal server host, or the internal server configuration on the router. It is possible that the internal server IP address is wrong, or that the firewall has inhibited the external host to access the internal network. Use the command **display acl** for further check. Refer to the firewall configuration.

Chapter 12 IP Unicast Policy Routing Configuration

12.1 IP Unicast Policy Routing Overview

IP policy routing is a mechanism in which packets are transmitted and forwarded by strategy without going through the routing table. It is a more flexible routing mechanism, compared with routing according to the destination address of data packet.

When a router is forwarding a packet, it is filtered via a **route-policy** first, deciding which packets to be forwarded and the next hop.

Policy routing is configured by the user. It is composed of a group of **if-match** clauses and a group of **apply** clauses. When some packets fully satisfy the **if-match** clauses of strategy, the **apply** clauses in the strategy are executed in a certain sequence, to complete the packet forwarding.

Route-policies are used for policy routing. One route-policy may contain multiple nodes, each consisting of multiple if-match and apply clauses.

The if-match clauses of a route-policy node define the match rules whereas its apply clauses define the actions performed on the packets filtered in by the node.

For a route-policy node, the relationship between its if-match clauses is AND for packet filtering, meaning a packet is permitted by the node only when it matches all if-match clauses.

At present, two **if-match** clauses i.e. **if-match packet-length** and **if-match acl** are provided.

The **apply** clause defines the operation of the policy. At present, there are five **apply** clauses: **apply ip-precedence**, **apply output-interface**, **apply ip-address next-hop**, **apply default output-interface**, and **apply ip-address default next-hop**. When all the if-match clauses are satisfied, the operation defined by the apply clauses are as follows:

- Configuring the priority: **apply ip-precedence**. Once configured, this clause is executed.
- Configuring the outbound interface and next hop: **apply output-interface** and **apply ip-address next-hop**, where the **apply output-interface** clause has a higher priority than the **apply ip-address next-hop** clause. When both of them are configured and valid, the system executes only the **apply output-interface** clause.
- Configuring the default outbound interface and next hop: **apply default output-interface** and **apply ip-address default next-hop**. The **apply default**

output-interface clause has a higher priority than the **apply ip-address default next-hop** clause. When both of them are configured and valid, the system executes only the **apply default output-interface** clause. Note that these two clauses are executed only when no outbound interface and next hop are configured for policy routing or the configured outbound interface and next hop are invalid, and no corresponding route is found in the routing table.

There are two kinds of policy routings: interface policy routing and local policy routing. The former is configured in interface view and performs strategic routing for packets coming through this interface, while the latter is configured in global view and performs policy routing for packets generated by this router. Generally, for the request about forwarding and security, in most cases, interface policy route will be used.

The policy routing can be used for security and load sharing.

12.2 IP Unicast Policy Routing Configuration

IP unicast policy routing configuration includes:

1) Configure a route-policy

- Establish a Route-policy
- Define match clause of policy routing
- Define apply clause of policy routing

2) Enable policy routing

- Enable/disable local policy routing
- Enable/disable policy routing on the interface

12.2.1 Configuring a Route-Policy

I. Creating a route-policy

Each route-policy comprises multiple policy nodes, each assigned a sequence number. The smaller the sequence number, the higher the priority. The policy with the highest priority is executed first.

A route-policy is made up of if-match and apply statements and can be used for route redistribution or policy routing.

Perform the following task in system view.

Table 12-1 Establish a route-policy

Operation	Command
Establish a route-policy or a policy node	**route-policy** *policy-name* { **permit** | **deny** } **node** *sequence-number*
Delete a route-policy or a policy node	**undo route-policy** *policy-name* [**permit** | **deny**] [**node** *sequence-number*]

permit means applying policy routing for the packets meeting the conditions, and **deny** means not applying policy routing for the packets meeting the conditions.

By default, no route-policy and the related node configuration is defined.

II. Defining if-match clauses for the route-policy

The if-match clauses are used for matching packets on which policy routing is to be performed. IP unicast policy routing provides two if-match clauses, **if-match packet-length** clause and **if-match acl** clause. When both of them are configured, their relationship is AND.

Perform the following task in route-policy view.

Table 12-2 Define if-match clause of policy routing

Operation	Command
Specify an IP packet length if-match clause	**if-match packet-length** *min-len max-len*
Specify an ACL matching if-match clause	**if-match acl** *acl-number*

By default, no if-match clause is defined.

III. Defining the apply clauses of the route-policy

IP unicast policy routing provides five types of apply clauses: **apply ip-precedence**, **apply output-interface**, **apply ip-address next-hop**, **apply default output-interface**, and **apply ip-address default next-hop**. One route-policy node may have multiple apply clauses. These clauses are executed in the order in which they are configured until a valid apply clause is executed.

Perform the following task in route-policy view.

Table 12-3 Define apply clause of policy routing

Operation	Command
Set packet precedence	**apply ip-precedence** *precedence*
Set packet transmitting interface	**apply output-interface** *interface-type interface-number* [*interface-type interface-number*]
Set packet next-hop	**apply ip-address next-hop** *ip-address* [*ip address*]
Set packet default transmitting interface	**apply default output-interface** *interface-type interface-number* [*interface-type interface-number*]
Set packet default next-hop	**apply ip-address default next-hop** *ip-address* [*ip address*]

The user can specify multiple next hops or set several outbound interfaces. In this case, the forwarding of packets will be shared among multiple parameters, namely, each packet is sent on each next hop or outbound interface in turn. This is only applicable to multiple parameters configured of one kind. If the outbound interfaces and next hops are both configured, only the outbound interface is set to perform the load sharing.

By default, no apply clause is defined.

12.2.2 Enabling Policy Routing

I. Enabling or Disabling Local Policy Routing

Enable or disable local policy routing in the system view. Only one local policy can be enabled.

Table 12-4 Enable/disable local policy routing

Operation	Command
Enable local policy routing	**ip local policy route-policy** *policy-name*
Disable local policy routing	**undo ip local policy route-policy** *policy-name*

By default, local policy routing is disabled.

II. Enabling or Disabling Policy Routing on the Interface

Enable or disable policy routing on a specified interface. At most one policy can be referenced on each interface.

Perform the following configuration in interface view.

Table 12-5 Enable/disable policy routing on the interface

Operation	Command
Enable policy routing on the interface	**ip policy route-policy** *policy-name*
Disable policy routing on the interface	**undo ip policy route-policy** *policy-name*

By default, policy routing is disabled on the interface.

12.3 Displaying and Debugging IP Unicast Policy Routing

After the above configuration, execute the **display** command in all views to display the running of the IP Unicast Policy Routing configuration, and to verify the effect of the configuration.

Execute the **debugging** command in user view for the debugging of IP Unicast Policy Routing.

Table 12-6 Display and debug IP unicast policy routing

Operation	Command
Show local policy routing and interface policy routing	**display ip policy**
Show the setting of the local policy routing	**display ip policy setup local**
Show the setting of the interface policy routing	**display ip policy setup interface** *interface-type interface-number*
Show the packet statistics of the local policy routing	**display ip policy statistic local**
Show the packet statistics of the interface policy routing	**display ip policy statistic interface** *interface-type interface-number*
enable the debugging of the policy routing	**debugging ip policy**

12.4 Typical Configuration of IP Unicast Policy Routing

12.4.1 Configuring Policy Routing Based on Source Address

I. Configuration requirements

Enable a policy routing named aaa, which controls all TCP packets received from Ethernet3/0/0 to be sent via the interface of serial1/0/0, whereas other packets to be forwarded based on routing table.

Node 5 denotes that Ethernet packets matched with **acl 3101** will be sent to serial1/0/0.

Node 10 denotes that any packets matched with **acl 3102** will not be processed by policy routing.

The packets from Ethernet 3/0/0 will try to match the if-match clauses of nodes 5 and 10 in turn. If nodes in **permit** mode are matched, execute corresponding apply clauses. If nodes in **deny** mode are matched, exit from policy routing.

II. Network diagram

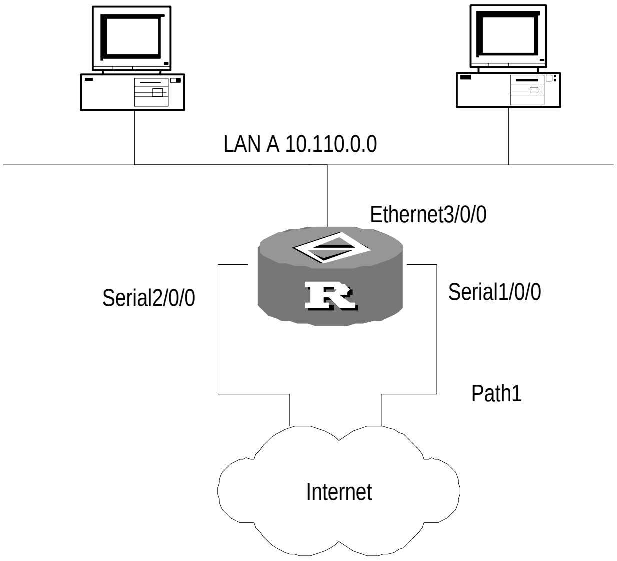


Figure 12-1 Network diagram for configuring policy routing based on source address

III. Configure procedure

# Set the default filtering method of firewall to deny.

```
[3Com] firewall default deny
```

# Define access control list:

```
[3Com] acl number 3101
[3Com-acl-adv-3101] rule permit tcp
[3Com-acl-adv-3101] quit
[3Com] acl number 3102
[3Com-acl-adv-3102] rule permit ip
[3Com-acl-adv-3102] quit
```

# Define acl 5 node to make any TCP packet matching ACL 3101 be sent to serial interface serial 1/0/0.

```
[3Com] route-policy aaa permit node 5
[3Com-route-policy] if-match acl 3101
[3Com-route-policy] apply output-interface serial 1/0/0
[3Com-route-policy] quit
```

# Define acl 10 node not to apply the policy routing to the packet matching ACL 3102.

```
[3Com] route-policy aaa deny node 10
[3Com-route-policy] if-match acl 3102
[3Com-route-policy] quit
```

# Apply policy aaa on the Ethernet interface

```
[3Com] interface ethernet 3/0/0
```

```
[3Com-Ethernet3/0/0] ip policy route-policy aaa
```

12.4.2 Configuring Policy Routing Based on Packet Size

I. Configuration requirement

Router A sends the packets of 64 to 100 bytes long through serial 2/0/0, packets of 101 to 1000 bytes long through serial 2/0/1 and those of other size should be routed normally.

Apply IP unicast policy routing lab1 on E1/2/0 of Router A. This strategy will set packet of 64 to 100 bytes long to 150.1.1.2 as the IP address of next hop and set packet of 101 to 1000 bytes long to 151.1.1.2 as the IP address of next hop. All packets of other size should be routed in the method based on the destination address

II. Network diagram

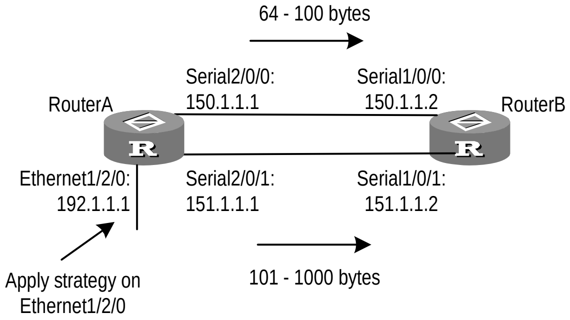


Figure 12-2 Network diagram for configuring policy routing based on packet size

III. Configure procedure

# Configure Router A:

```
[RouterA] interface ethernet 1/2/0
[RouterA-Ethernet 1/2/0] ip address 192.1.1.1 255.255.255.0
[RouterA-Ethernet 1/2/0] ip policy route-policy lab1
[RouterA] interface serial 2/0/0
[RouterA-Serial2/0/0] ip address 150.1.1.1 255.255.255.0
[RouterA] interface serial 2/0/1
[RouterA-Serial2/0/1] ip address 151.1.1.1 255.255.255.0
[RouterA] rip
[RouterA-rip] network 192.1.1.0
[RouterA-rip] network 150.1.0.0
[RouterA-rip] network 151.1.0.0
[RouterA] route-policy lab1 permit node 10
[RouterA-route-policy] if-match packet-length 64 100
[RouterA-route-policy] apply ip-address next-hop 150.1.1.2
```

```
[RouterA] route-policy lab1 permit node 20
[RouterA-route-policy] if-match packet-length 101 1000
[Router-route-policy] apply ip-address next-hop 151.1.1.2
```

# Configure Router B:

```
[RouterB] interface serial 1/0/0
[RouterB-Serial1/0/0] ip address 150.1.1.2 255.255.255.0
[RouterB] interface serial 1/0/1
[RouterB-Serial1/0/1] ip address 151.1.1.2 255.255.255.0
[RouterB] rip
[RouterB-rip] network 150.1.0.0
[RouterB-rip] network 151.1.0.0
```

Use the **debugging ip policy** command to monitor policy routing on Router A. Note: the packets of 64 bytes long match the entry item whose id number is 10 as shown in the route policy lab1, therefore they are forwarded to 150.1.1.2.

```
<RouterA> debugging ip policy
*0.483448-POLICY-8-POLICY-ROUTING:IP Policy routing success : next-hop :
150.1.1.2
```

On Router A, change the packet size to 101 bytes and monitor policy routing with the **debugging ip policy** command. Note: the packets of 101 bytes match the entry item whose serial number is 20 as shown in the route policy lab1. They are forwarded to 151.1.1.2.

```
<RouterA> debugging ip policy
*0.483448-POLICY-8-POLICY-ROUTING:IP Policy routing success : next-hop :
151.1.1.2
```

On Router A, change the packet size to 1001 bytes, and then use the **debugging ip policy** command to monitor policy routing. Note that this packet does not match any entry item in lab1, so it is forwarded in regular mode. The policy routing debugging does not output information of the forwarding packets.

Chapter 13 IP Multicast Policy Routing Configuration

13.1 Introduction to IP Multicast Policy Routing

13.1.1 Overview of IP Multicast Policy Routing

IP multicast policy routing is subsidiary and enhancement to the function that multicast forwards packets according to the routing table. It forwards multicast packets according to the policy the user specifies.

IP multicast policy routing is implemented by configuring the route-policy. The route-policy is an extension of unicast policy routing, described by a group of **if-match** and **apply** statements the user defines. The **if-match** clause defines the match rule, i.e., the filter conditions to be met to pass the current route-policy. It specifies when a multicast packet meets the match conditions the user defines, the multicast packet is not forwarded according to the usual process, but forwarded according to the action the user sets (described by the **apply** statement).

13.1.2 Concepts Related to IP Multicast Policy Routing

- route-policy

IP multicast policy routing is implemented through route-policies. Multiple route-policies can be configured on a router.

- Policy node

A policy node is a complete policy, which sets the conditions packets should match with the **if-match** command and sets the forwarding actions that should be executed to packets meeting the match conditions with the **apply** command. Each node contains at most one ACL used for defining the match conditions of packets, one ACL used for specifying the outgoing interface and one ACL used for specifying the next hop.

Multiple nodes with different conditions and actions can be configured in a route-policy. Different policy-nodes in each route-policy can be identified through an integer sequence-number.

- Match rule

Match conditions of multicast packets are described by the **if-match** clause and are set by configuring the standard or extended ACL (ranging from 2000 to 3999).

- Forwarding actions of multicast packets

Forwarding actions of multicast packets are described by the APPLY clause including setting the outgoing interface and the next hop IP address. The output interface list is specified through an interface-based ACL (ranging from 1000 to 1999). The next hop IP address list is specified through a standard ACL (ranging from 2000 to 2999).

13.1.3 Packet Forwarding Process after the IP Multicast Policy Routing is Applied

For a multicast packet, if IP multicast policy routing is configured on the incoming interface and the packet meets the match conditions of IP multicast policy routing, the packet will be forwarded according to the actions set by the policy routing. Otherwise, the packet will be forwarded according to the usual forwarding process.

13.2 Configuring IP Multicast Policy Routing

IP Multicast Policy Routing Configuration includes:

- Define a route-policy
- Define the if-match clause for IP multicast routing policy
- Define the apply clause of the route-policy
- Enable IP multicast policy routing on an interface

13.2.1 Defining a Route-Policy

Multiple policy-nodes with different conditions and actions can be configured in a route-policy. Each policy-node has its own **if-match** clauses and **apply** clauses. Their match order is specified by *sequence-number*.

Perform the following configurations in system view.

Table 13-1 Define a route-policy

Operation	Command
Define a policy-node of the route-policy	**route-policy** *policy-name* { **permit** | **deny** } **node** *sequence-number*
Remove a policy-node of the route-policy	**undo route-policy** *policy-name* [**permit** | **deny**]

When IP multicast policy routing is configured on an interface of a router, all multicast data packets that enter the router from this interface will be filtered. The filtering method is that all policy-nodes of the route-policy specified by the policy routing are processed in order of the *sequence-number* from small to large.

Note that the relationship among all parts of different *sequence-numbers* is “or”, that is, the packet pass by every node of different *sequence-number* in sequence. If packet can match if-match clause of one node, the packet will be forwarded by the apply clause of the node and not reach all the following nodes.

13.2.2 Defining the if-match Clause of the Route-Policy

An **if-match** clause defines the match rule, which is the filtering condition that should be met by the packets to pass the current route-policy.

Perform the following configurations in route-policy view.

Table 13-2 Define match conditions

Operation	Command
Set conditions that multicast packets should meet	**if-match acl** *acl-number*
Remove the match conditions set	**undo if-match acl**

If a packet meets the Match conditions specified in a policy-node, actions specified by the node will be performed. If a packet does not meet the match conditions specified in a policy-node, the next node will be detected. If a packet does not meet the conditions of all route-nodes, the packet will return to the normal forwarding flow.

The following points should be noted:

- For a node of a route-policy, the relationship among all **if-match** clauses in the same node is “and” during matching.
- Multicast policy routing only considers the configuration of **if-match acl** and **if-match interface** in a policy-node. Any other **if-match** clause does not concern forwarding of multicast policy routing.
- If no **if-match** clause is specified, all routing information will pass the filtering of the node.

13.2.3 Defining Apply Clauses for a Route-Policy

The **apply** clauses specify actions, that is, some configuration commands executed after the filter conditions specified by the **if-match** clauses have been met.

Perform the following configurations in route-policy view.

Table 13-3 Define Apply clauses

Operation	Command
Configure an outgoing interface list in a policy-node	**apply output-interface acl** *acl-number*
Remove the outgoing interface list configured	**undo apply output-interface** [**acl** *acl-number*]
Configure the next hop IP address list in a policy-node	**apply ip-address next-hop** { **acl** *acl-number* | *ip-address* [*ip-address*] }
Remove the next hop address list configured	**undo apply ip-address next-hop** [**acl** *acl-number* | *ip-address* [*ip-address*]]

Use the ACL to specify the output interface list and the next hop IP address list for IP multicast policy routing. The basic ACL (ranging from 2000 to 2999) is specified for the next hop IP address. The interface-based ACL (ranging from 1000 to 1999) is specified for the output interface list.

13.2.4 Enabling IP Multicast Policy Routing on an Interface

Perform the following configurations in interface view.

Table 13-4 Enable IP multicast policy routing on an interface

Operation	Command
Enable an IP multicast policy routing on an interface	**ip multicast-policy route-policy** *policy-name*
Remove an IP multicast policy routing on an interface	**undo ip multicast-policy route-policy** *policy-name*

When IP multicast policy routing is configured on an interface of a router, all multicast packets (excluding multicast protocol packets such as packets generated by multicast routing protocols) entering the router on the interface will be filtered.

The filter method is as follows: All policy nodes of the route-policy specified by the policy routing are filtered in order of sequence number from small to large. If a packet meets the if-match conditions specified in a policy-node, actions specified by the node will be executed. If a packet does not meet the if-match conditions specified in a policy-node, the next node will be detected. If a packet does not meet the conditions of any policy nodes, the packet will return to the normal forwarding process.

13.3 Displaying and Debugging IP Multicast Policy Routing

After the above configuration, execute **display** command in all views to display the running of IP Multicast Policy Routing configuration, and to verify the effect of the configuration.

Execute the **debugging** command in user view for the debugging of IP Multicast Policy Routing.

Table 13-5 Display and debug IP multicast policy routing

Operation	Command
Display the multicast policy routing information	**display ip multicast-policy** [**setup interface** *interface-type interface-num* **| statistic interface** *interface-type interface-num*]
Enable the IP multicast policy routing debugging	**debugging ip multicast-policy** [*acl-number*]

Operation	Command
Disable the IP multicast policy routing debugging	**undo debugging ip multicast-policy**

Routing Protocol

Table of Contents

Chapter 1 IP Routing Protocol Overview

1.1 IP Route and Routing Table Overview

1.1.1 IP Route and Route Segment

Routers are adopted for route selection on the Internet. According to the destination address of a received packet, a router selects an appropriate route (via a network) and forwards the packet to the next router. The last router is responsible for forwarding the packet to the destination host.

For example, in Figure 1-1, from host A to host C, there are totally three networks and two routers. If a node is connected to another node through a network, there will be a route segment between these two nodes. They are thus considered adjacent in the Internet. Similarly, two routers connected to the same network are adjacent routers. The number of route segments between a router and certain host in the same network is taken as zero. In the following figure, the bold arrows represent these route segments. A router does not concern about which physical links constitute this route segment.

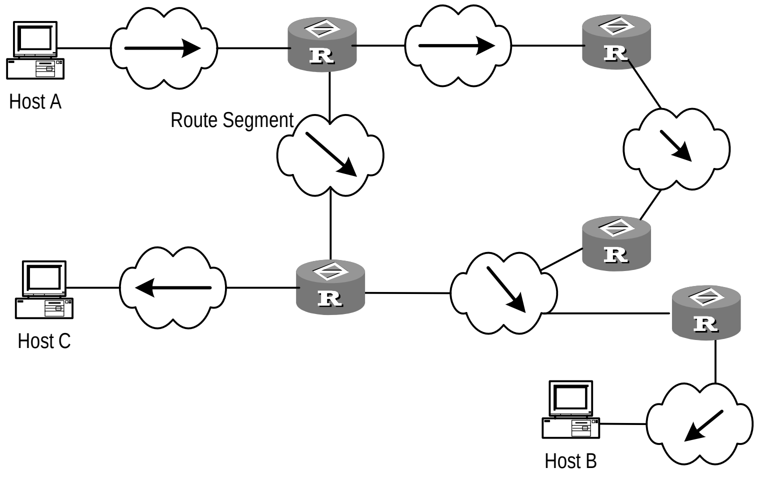


Figure 1-1 Route segment

As network size may vary greatly, the actual "lengths" of router segments may be different from each other. Therefore, for different networks, the number of route segments multiplies a weighted coefficient can measure the actual length of the path.

If a router in a network is regarded as a node in the network and a route segment in the Internet is regarded as a link in the Internet, routing in the Internet is similar to routing in a simple network. Routing through the shortest route is not always the most ideal way. For example, routing through 3 high-speed LAN route segments may be much faster than that through 2 low-speed WAN route segments.

1.1.2 Routing by Routing Table

The key for a router to forward packets is the routing table. Each router saves a routing table in its memory, and each entry of this table specifies the physical port of the router through which the packet to a subnet or a host should be sent. Therefore, it can reach the next router in this path or reach the very destination host in the directly connected network.

A routing table has the following key entries:

- Destination address: It is used to identify the destination address or the destination network of an IP packet.
- Network mask: Along with destination address, it identifies the address of the network segment where a destination host or a router resides. After performing “logical AND” between destination address and network mask, you can get the address of the network segment where a destination host or a router resides. For example, if the destination address is 129.102.8.10, the address of the network where the host or the router with the mask 255.255.0.0 is located will be 129.102.0.0. A mask consists of several consecutive “1”, represented either by dotted decimal notation or by the number of consecutive “1” in the mask.
- Output interface: It indicates through which interface an IP packet should be forwarded.
- Next hop address: It indicates the next router that an IP packet will pass through.
- Precedence added to the IP routing table for a route: There may be different next hops to the same destination. These routes may be discovered by different routing protocols, or they can be the manually configured static routes. The one with the highest precedence (the smallest numerical value) will be selected as the current optimal route.

According to different destinations, the routes fall into the following groups:

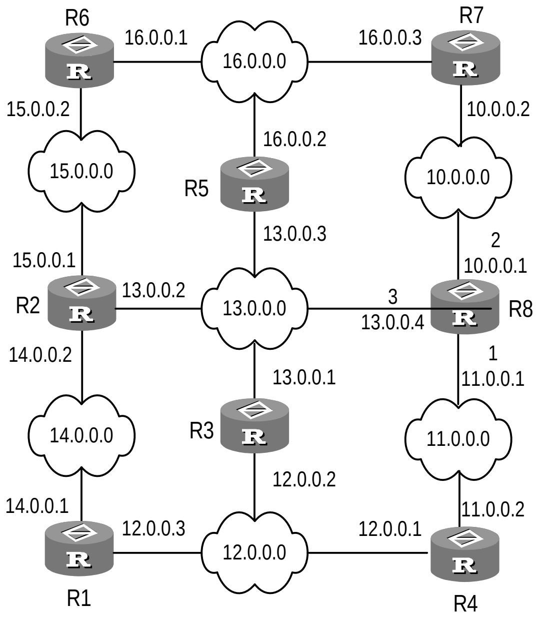
- Subnet route: Its destination is a subnet.
- Host route: Its destination is a host

In addition, according to whether the network where the destination locates is directly connected to the router, routes can be divided into the following categories:

- Direct route: The router is directly connected to the network where the destination locates.
- Indirect route: The router is not directly connected to the network where the destination locates.

In order to avoid a too huge routing table, you can set a default route. All the packets that fail to find the suitable routing entry will be forwarded through this default route.

In a complicated Internet as shown in Figure 1-2, the numbers in each network indicate its network address. The router R8 is connected with three networks, so it has three IP addresses and three physical ports. Its routing table is shown in the figure below:



Routing table of Router R8

Destination Network	Nexthop	Interface
10.0.0.0	10.0.0.1	2
11.0.0.0	11.0.0.1	1
12.0.0.0	11.0.0.2	2
13.0.0.0	13.0.0.4	3
14.0.0.0	13.0.0.2	3
15.0.0.0	10.0.0.2	2
16.0.0.0	10.0.0.2	2

Figure 1-2 Routing table

A router supports the configuration of static route as well as a series of dynamic routing protocols such as RIP, OSPF, IS-IS and BGP. Moreover, a router in operation can automatically obtain some direct routes according to interface state and user configuration.

1.2 Routing Management Policy

You can manually configure a static route to a certain destination, or configure the interaction between dynamic routing protocol and other routers in the network and find route via routing algorithm. The static routes configured by the user are managed together with the dynamic routes discovered by the routing protocol in the router. The static routes and the routes learned or configured by different routing protocols can also be shared among routing protocols.

1.2.1 Routing Protocols and Route Discovery Preference

Different routing protocols (including static routes) may discover different routes to the same destination, but not all these routes are optimal. In fact, at a certain moment, only one routing protocol can determine the current route to a specific destination. Thus, each of these routing protocols (including static routes) is assigned with a preference. When there are multiple routing information sources, the route learned by the routing protocol with the highest preference will become the current route. Table 1-1 lists the routing protocols and the default preferences (the smaller the value, the higher the preference is) of the routes discovered by them.

In the table, “0” represents a directly connected route, and “255” represents a route from an unknown source.

Table 1-1 Routing protocols and route discovery preferences

Routing Protocol or Route Type	The Preference of the Corresponding Route
DIRECT	0
OSPF	10
IS-IS	15
STATIC	60
RIP	100
OSPF ASE	150
OSPF NSSA	150
IBGP	256
EBGP	256
UNKNOWN	255

Except for direct routing, IBGP and EBGP, the preferences of various dynamic routing protocols can be manually configured to meet the user requirements. In addition, the preferences for individual static routes can be different.

1.2.2 Load Sharing and Route Backup

I. Load sharing

Load sharing supports multi-route mode, permitting to configure multiple routes that reach the same destination and use the same precedence. The same destination can be reached via multiple different paths, whose precedence is equal. When there is no route that can reach the same destination with a higher precedence, the multiple routes will be adopted. The packets are forwarded to the destination through these paths, thus implementing load sharing. This feature can however apply to the equal-cost routes of the same routing protocol. For example, you cannot balance load among static routes and OSPF routes.

Load sharing is supported by four routing protocols: static routing, OSPF, BGP, and IS-IS. The following load sharing implementations are available:

- Per-flow load sharing. When fast forwarding (the default) is enabled, the router can implement only per-flow load sharing. Suppose two equal-cost routes are available on the router. When one data flow arrives, the router forwards it on one route. When two data flows arrive, the router forwards each on one route. Likewise, the fast forwarding-enabled subinterfaces implement per-flow load sharing.

- Per-packet load sharing, implemented when fast forwarding is disabled. The router then distributes the arrived packets equally on the participating routes.
- Bandwidth-based unbalanced load sharing. When fast forwarding is disabled, the router implements per-packet load sharing to distribute load depending on the physical bandwidth of interface. You can however allocate load bandwidth to each interface. The router then distributes load on the participating interfaces depending on the ratio of their load bandwidths.

Note:

Equal-cost route load sharing is implemented based on route processing; it is meaningful only when the router makes forwarding decisions based on the routing or fast-forwarding table. When policy routing is adopted, load sharing does not work.

II. Route backup

Support route backup. When main route failed, the system will automatically switch to a backup route to improve the network reliability. In order to achieve route backup, the user can configure multiple routes to the same destination according to actual situation. One of the routes has the highest precedence and is called as main route. The other routes have descending precedence and are called as backup routes. Normally, the router sends data via main route. When the line is in failure, the main route will hide itself and the router will choose one route whose precedence is higher than others from the left routes as a path to send data. In this way, the switchover from the main route to the backup route is realized. When the main route recovers, the router will restore it and re-select route. As the main route has the highest precedence, the router will choose the main route to send data. This process is the automatic switchover from the backup route to the main route.

1.2.3 Routes Sharing Between Routing Protocols

As the algorithms of various routing protocols are different, different routing protocols may learn different routes, causing the problem of how to share the learned routes between the routing protocols. A router can redistribute the route discovered by one routing protocol to another routing protocol. Each protocol has its own route redistribution mechanism. For details, please refer to the description about "Redistributing an External Route" in the operation manual of the corresponding routing protocol.

1.3 Configuring Bandwidth-Based Unbalanced Load Sharing

In general, the technology of load sharing is to send packets evenly to different interfaces. For example, with load sharing, a flow of 3 Mbps is evenly sent to two interfaces, that is, 1.5 Mbps for each interface. This will result in low utilization on the interface with larger bandwidth and packet dropping on the interface with smaller bandwidth.

To improve bandwidth utilization, more packets should be sent to the interfaces with larger bandwidth, while fewer packets should be sent to the interfaces with less bandwidth, so as to implement unbalanced load sharing based on the interface bandwidth of the equal-cost routes. If the system supports this feature, load sharing is implemented based on physical bandwidth by default. If the user has configured specified bandwidth, load sharing will be implemented according to the specified bandwidth.

1.3.1 Enabling Bandwidth-Based Unbalanced Load Sharing

Perform the following configuration in system view.

Table 1-2 Enable bandwidth-based unbalanced load sharing

Operation	Command
Enable bandwidth-based unbalanced load sharing	**band-based-sharing**
Disable bandwidth-based unbalanced load sharing	**undo band-based-sharing**

By default, bandwidth-based unbalanced load sharing is disabled.

📖 **Note:**

As bandwidth-based unbalanced load sharing does not support per-flow load sharing, you must disable fast forwarding on the incoming or outgoing interface when using the function.

1.3.2 Assigning Bandwidth to an Interface

Perform the following configuration in interface view.

Table 1-3 Assign bandwidth to the interface

Operation	Command
Assign bandwidth to the interface	**loadbandwidth** *bandwidth*
Restore the default bandwidth of the interface	**undo loadbandwidth**

Different from physical bandwidth, the configuration of load bandwidth does not affect interface properties but load distribution. When you set the *bandwidth* argument to 0, the current interface is shut down and does not participate in load sharing. The default load bandwidth is the physical bandwidth of the interface.

1.3.3 Displaying and Debugging Bandwidth-Based Unbalanced Load Sharing

Perform the **display** command in any view and the **reset** command in user view.

Table 1-4 Display and debug bandwidth-based unbalanced load sharing

Operation	Command
Display statistics about unbalanced load sharing based on interface bandwidth	**display loadsharing ip address** *ip-address mask*
Clear statistics about unbalanced load sharing	**reset loadsharing** { **all** | **ip address** *ip-address mask* }

1.3.4 Bandwidth-Based Unbalanced Load Sharing Configuration Example

I. Network requirements

Suppose that three equal-cost routes to the destination address 10.2.1.0 /24 are available on Router A.

```
[Router A] display fib
Destination/Mask   Nexthop         Flag TimeStamp     Interface
10.2.1.0/24        10.1.1.2         GSU  t[0]           Ethernet0/0/0
10.2.1.0/24        10.1.2.2         GSU  t[0]           Atm1/0/0
10.2.1.0/24        10.1.3.2         GSU  t[0]           Serial2/0/0
```

Use the **display loadsharing ip address** command to view the current bandwidth ratio between interfaces.

```
[Router A] display loadsharing ip address 10.2.1.0 24
There are/is totally 3 route entry(s) to the same destination network.
Nexthop       Packet(s)   Bandwidth[KB]    Flow(s)    Interface
10.1.1.2      763851       100000      0          Ethernet0/0/0
```

```
10.1.2.2      1193501      155000       0           Atm1/0/0
10.1.3.2      15914        2048         0           Serial2/0/0
BandWidth:48:75:1
  Packets:47:74:1
Flows:0:0:0
```

The output indicates that load is shared on the three interfaces based on default bandwidth.

View statistics about load sharing after you configure bandwidth-based unbalanced load sharing on Router A.

II. Network diagram

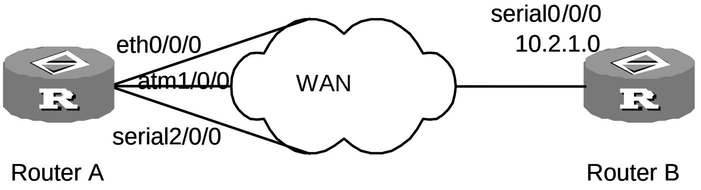


Figure 1-3 Configure bandwidth-based unbalanced load sharing

III. Configuration procedure

1) Configure Router A

# Configure bandwidth-based load sharing on three interfaces.

```
[Router A] interface ethernet 0/0/0
[Router A-Ethernet0/0/0] loadbandwidth 200
[Router A-Ethernet0/0/0] quit
[Router A] interface Atm 1/0/0
[Router A-Atm 1/0/0] loadbandwidth 100
[Router A-Atm 1/0/0] quit
[Router A] interface serial 2/0/0
[Router A-serial 2/0/0] loadbandwidth 300
[Router A-serial 2/0/0] quit
```

# View the load bandwidth ratio between the three interfaces.

```
[Router A] display loadsharing ip ad 10.2.1.0 24
There are/is totally 3 route entry(s) to the same destination network.
Nexthop       Packet(s)    Bandwidth[KB] Flow(s)     Interface
10.1.2.2      142824       100             0             Atm1/0/0
10.1.1.2      285648       200             0             Ethernet0/0/0
10.1.3.2      428472       300             0             Serial2/0/0

BandWidth:1:2:3
```

```
  Packets:1:2:3
Flows:0:0:0
```

The statistics indicates that load sharing is implemented according to the ratio of the specified bandwidths.

Chapter 2 Static Route Configuration

🕮 **Note:**

For the parameter explanation in VPN instance, refer to "MPLS" module of this manual.

2.1 Static Route Overview

2.1.1 Static Route

Static route is a special kind of route manually configured by an administrator. You can set up an interconnecting network with the static route configuration. The problem for such configuration is when a fault occurs to the network, the static route cannot change automatically to keep itself away from the node causing the fault, if without the help of the administrator.

In a relatively simple network, you only need to configure the static routes to make the router work normally. The proper configuration and usage of static routes can improve the network performance and ensure the bandwidth of important applications.

Static route also features the following attributes:

- Reachable route: A normal route is of this type. That is, an IP packet is sent to the next hop via the route marked by the destination. It is a common type of static routes.
- Unreachable route: When a static route to a destination has the "**reject**" attribute, all the IP packets to this destination will be discarded, and the originating host will be informed destination unreachable.
- Blackhole route: When a static route to a destination is of the "blackhole" attribute, all the IP packets to this destination will be discarded, and the originating host will not be informed.

The attributes "**reject**" and "**blackhole**" are usually used to control the range of reachable destinations of this router, and help troubleshooting the network.

2.1.2 Default Routing

A default route is a kind of special route, configured by static route or some dynamic routing protocols such as OSPF and IS-IS.

Simply put, a default route is a route used only when no suitable route is matched. That is to say, only when no proper route is found, will the default route be used. In a routing table, the default route is in the form of the route to the network 0.0.0.0 (with the mask 0.0.0.0). You can see whether it has been set via the output of the **display ip routing-table** command. If the destination address of a packet fails in matching any entry of the routing table, the router will select the default route to forward this packet. If there is no default route, this packet will be discarded, and an Internet Control Message Protocol (ICMP) packet will be sent to the originating host to inform that the destination host or network is unreachable.

2.2 Static Routing Configuration

Static routing configuration includes:

- Configure a static route
- Configure the default route
- Configure the priority of a static route
- Delete a static route

2.2.1 Configuring a Static Route

Perform the following configuration in system view.

Table 2-1 Configure a static route

Operation	Command
Add a static route	**ip route-static** *ip-address* { *mask* | *mask-length* } [*interface-type interface-number*] [*nexthop-address*] [**preference** *value*] [**reject | blackhole**] **ip route-static vpn-instance** { *vpn-instance-name1 vpn-instance-name2 … ip-address* } { *mask* | *mask-length* } [*interface-type interface-number* [*nexthop-address*] **| vpn-instance** *vpn-nexthop-name nexthop-address* | *nexthop-address* [**public**]] [**preference** *preference-value*] [**reject** | **blackhole**] [**tag** *tag-value*] [**description** *string*]
Delete a static route	**undo ip route-static** *ip-address* {*mask* | *mask-length* } [*interfacce-name*] [*nexthop-address*] [**preference** *value*] **undo ip route-static vpn-instance** { *vpn-instance-name1 vpn-instance-name2 … ip-address* } { *mask* | *mask-length* } [*interface-type interface-number* | **vpn-instance** *vpn-nexthop-name nexthop-address* | *nexthop-address* [**public**]] [**preference** *preference-value*]

The parameters are explained as follows:

1) VPN instance name
2) IP address and mask

An IP address is in dotted decimal format. As the “1” in a 32-bit mask is required to be consecutive, a mask can be represented either by dotted decimal notation or by mask length (namely the bits of “1” in a mask).

3) Transmitting interface or next-hop address

To configure a static route, you can either specify the *interface-name* of a sending interface or the *gateway-address* of a next-hop address. It depends on specific situation.

Virtually, it is necessary to specify the next-hop addresses of all route entries. During packet forwarding over IP, a router first finds matched route from the routing table according to the destination address of a packet. Only when the next-hop is specified, can the link layer finds corresponding link layer address via the next-hop IP address and forward the packet according to the address.

A sending interface can be specified in the following cases:

- For a point-to-point interface, when a sending interface is specified, it implicates that the next-hop address is also specified. In this case, the peer interface address connected with the interface is regarded as the next-hop address of the route. For example, in the case that SERIAL interface is encapsulated with PPP, the peer IP address can be obtained via PPP negotiation. It is unnecessary to specify the next-hop address but specifying the sending interface.
- For an NBMA interface (such as an ATM interface), which supports point-to-multipoint, it is necessary to create reroute at link layer, namely the mapping from an IP address to a link layer address, besides configuring IP routes. To configure static route in this case, you should configure the next-hop IP address rather than specify the sending interface.

4) Precedence

The **preference** can be configured differently by flexibly applying route management policies.

5) Other parameters

The attributes reject and blackhole respectively indicate the unreachable route and the blackhole route. The public attribute specifies that a public address is specified. The tag attribute specifies the tag of a static route for a routing policy. The description attribute describes the static route.

2.2.2 Configuring the Default Route

Perform the following configuration in system view.

Table 2-2 Configure the default route

Operation	Command
Configure the default route	**ip route-static** 0.0.0.0 { 0.0.0.0 | 0 } {*interface-type interface-number* | *nexthop-address* } [**preference** *value*] [**tag** *tag-value*] [**description** *string*] **ip route-static vpn-instance** *vpn-instance-name* 0.0.0.0 { 0.0.0.0 | 0 } {*interface-type interface-number* | *nexthop-address* } [**preference** *value*] [**tag** *tag-value*] [**description** *string*]
Delete the default route	**undo ip route-static** 0.0.0.0 { 0.0.0.0 | 0 } {*interface-type interface-number* | *nexthop-address*} [**preference** *value*] **undo ip route-static vpn-instance** *vpn-instance-name* 0.0.0.0 { 0.0.0.0 | 0 } {*interface-type interface-number* | *nexthop-address* } [**preference** *value*]

The meanings of parameters in the command are the same as those of the static route.

2.2.3 Deleting All Static Routes

Perform the following configuration in system view.

Table 2-3 Delete all the static routes

Operation	Command
Delete all the static routes	**delete static all**

This command can be used to delete all the static routes configured, including default routes.

2.3 Displaying and Debugging the Routing Table

After the above configuration, execute the **display** command in all views to display the running of the static route configuration, and to verify the effect of the configuration.

Table 2-4 Display and debug routing table

Operation	Command
View routing table summary	**display ip routing-table**
View routing table details	**display ip routing-table verbose**
View the route of a specified destination address	**display ip routing-table** *ip-address* [*mask*] [**longer-match**] [**verbose**]

Operation	Command
View the routes within specified range of destination addresses	**display ip routing-table** *ip-address1 mask1 ip-address2 mask2* [**verbose**]
View the routes passing the filtering of a specified standard ACL	**display ip routing-table acl** *acl-number* [**verbose**]
View the routes filtered by specified IP prefix list	**display ip routing-table ip-prefix** *ip-prefix-number* [**verbose**]
View the routes discovered by the specified protocol	**display ip routing-table protocol** *protocol* [**inactive** | **verbose|** **vpn-instance** *vpn-instance-name*]
View the tree routing table	**display ip routing-table radix**
View the statistics in a routing table	**display ip routing-table [vpn-instance** *vpn-instance-name* **] statistics**
View the summary information of the private network routing table	**display ip routing-table vpn-instance** *vpn-instance-name* [*ip-address*]
View routing table details	**display ip routing-table vpn-instance** *vpn-instance-name* [*ip-address*] **verbose**
Clear the routing table	**reset ip routing-table** [**vpn-instance** *vpn-instance-name*] **statistics protocol** *protocol-type*

2.4 Static Routing Configuration Example

I. Network requirements

In the following figure, it is required to configure static routes so as to realize interworking between any two hosts or routers.

II. Network diagram

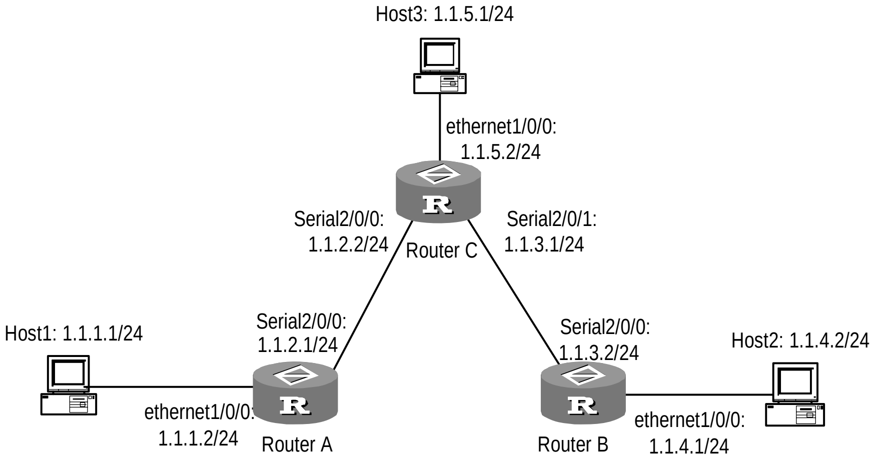


Figure 2-1 Configure static routes

III. Configuration procedure

# Configure the static route for Router A

```
[Router A] ip route-static 1.1.3.0 255.255.255.0 1.1.2.2
[Router A] ip route-static 1.1.4.0 255.255.255.0 1.1.2.2
[Router A] ip route-static 1.1.5.0 255.255.255.0 1.1.2.2
```

Or just configure the default route.

```
[Router A] ip route-static 0.0.0.0 0.0.0.0 1.1.2.2
```

# Configure the static route for Router B

```
[Router B] ip route-static 1.1.2.0 255.255.255.0 1.1.3.1
[Router B] ip route-static 1.1.5.0 255.255.255.0 1.1.3.1
[Router B] ip route-static 1.1.1.0 255.255.255.0 1.1.3.1
```

Or just configure the default route.

```
[Router B] ip route-static 0.0.0.0 0.0.0.0 1.1.3.1
```

# Configure the static route for Router C

```
[Router C] ip route-static 1.1.1.0 255.255.255.0 1.1.2.1
[Router C] ip route-static 1.1.4.0 255.255.255.0 1.1.3.2
```

Configure the default gateway of the Host 1 to be 1.1.1.2

Configure the default gateway of the Host 2 to be 1.1.4.1

Configure the default gateway of the Host 3 to be 1.1.5.2

By then, all the hosts or routers in the Figure 2-1 can mutually interwork.

2.5 Troubleshooting Static Route

Symptom 1: The router is not configured with dynamic routing protocol. Both the physical status of the interface and the link layer protocol are in UP status, but the IP packet cannot be forwarded normally.

Troubleshooting:

- Use the **display ip routing-table protocol static** command to view whether the corresponding static route is correctly configured.
- Use the **display ip routing-table** command to view whether the static route is valid.
- View whether the next-hop address is not specified or incorrectly specified on the NBMA interface.

View whether the secondary routing table of the link layer is configured correctly on the NBMA interface.

Chapter 3 RIP Configuration

Note:

For the parameter explanation of VPN instance, refer to "MPLS" module of this manual.

3.1 RIP Overview

RIP (Routing Information Protocol) is a relatively simple interior gateway protocol (IGP), and it is primarily applied to relatively small networks.

Since the implementation of RIP is comparatively simple, the impact of the cost of the protocol itself on the performance of networks is relatively small, and the configuration and maintenance of RIP is easier than that of OSPF and IS-IS, RIP is still widely used in practice.

3.1.1 Mechanism of RIP

I. Introduction to RIP

RIP is a kind of Distance-Vector (D-V) algorithm-based protocol and exchanges routing information via UDP packets. It employs Hop Count to measure the distance to the destination host, which is called Routing Cost. In RIP, the hop count from a router to its directly connected network is 0, and that to a network which can be reached through another router is 1, and so on. To restrict the time to converge, RIP prescribes that the cost is an integer ranging from 0 and 15. The hop count equal to or exceeding 16 is defined as infinite, that is to say, the destination network or the host is unreachable.

To improve performance and avoid the creation of routing loops, RIP supports both Split Horizon and Poison Reverse. Besides, RIP can also redistribute routes from other routing protocols.

II. Route database of RIP

Each router running RIP manages a route database, which contains routing entries to all the reachable destinations in the network. These routing entries contain the following information:

- Destination address: IP address of a host or a network.
- Next hop address: The address of the next router that a router will pass through for reaching the destination.
- Interface: The interface through which the IP packet should be forwarded.

- Cost: The cost for the router to reach the destination, which should be an integer in the range of 0 to 15.
- Timer: Duration from the last time that the routing entry is modified till now. The timer is reset to 0 whenever a routing entry is modified.
- Route flag: A label distinguishing routes of internal routing protocols from those of external routing protocols.

III. Timer of RIP

In RFC1058, RIP is described as controlled by three timers, Period update, Timeout and Garbage-collection,

- Timer Period update is to send all RIP routing information to all neighbors;
- If a RIP route is not updated within the time period configured on timer Timeout (namely, the local router does not receive the route update packet from the neighbor), the route will be regarded as unreachable;
- If the local router still does not receive any route update packet from the neighbor, that is, if the unreachable route is still not updated, the route will be removed from the routing table.

3.1.2 RIP Versions

Currently two RIP versions are available: RIP-1 and RIP-2.

RIP-1 is a classful routing protocol. It advertises protocol packets by broadcasting. As RIP-1 packets do not include subnet mask information, RIP can only recognize routes of natural network segments such as routes of class A, B, or C. For this reason, RIP-1 does not support route summary and discontiguous subnets.

RIP-2 is a classless routing protocol. Compared to RIP-1, it has the following advantages by supporting:

- Route tag separating internal RIP routes (routes for networks within the RIP routing domain) from external RIP routes, which may have been imported from an EGP or another IGP. You can use route tag with routing policies to manage routes flexibly.
- Subnet mask, supporting route summary and classless inter-domain routing (CIDR).
- Specified next hop, the optimal next hop address can be found on the broadcast network.
- Multicasting for sending periodic updates, reducing resource consumption.
- Authentication on RIP messages for extra security. Two methods are available: plain text and MD5.

🕮 **Note:**

RIP-2 supports both broadcasting and multicasting. By default, multicasting applies and the IP multicast address is 224.0.0.9. When RIP-2 broadcasting is running on interfaces, RIP-1 packets can also be received.

3.1.3 Trigger RIP

Trigger RIP (TRIP) is an extension of RIP on WAN circuits primarily for dial-up networks.

TRIP removes periodic updating and includes retransmission and backup routing. It adopts a new algorithm to test connectivity, ensuring that the route for a dial-up link is retained even after the link is disconnected. TRIP allows the system to disconnect links when the routing table is stable and no data is waiting for transmission. These links can be set up when the routing table changes or when data needs transmission. This greatly saves cost.

Instead of periodically broadcasting updates, TRIP sends updates only when triggered. These updates are forwarded only when acknowelegement is received. This decreases route management overheads. TRIP is suitable for dial-up networks and networks implementing traffic-based accounting.

TRIP implementation of V 2.41 supports RFC2091, RFC2082, and simple and MD5 authentication of RFC2453.

TRIP supports route summary but not equal-cost routes.

3.1.4 RIP Startup and Operation

The whole process of RIPv1 startup and running can be described as follows:

- When RIP is just enabled on a router, request packet is forwarded to a neighbor router in broadcast mode. After the neighbor router receives the packet, it will respond to the request and resend a response packet containing information in the local routing table.
- When the former router receives the response packet, it will modify its local routing table and send a modification triggering packet to the neighbor router and broadcast the route modification information. Upon receiving the modification triggering packet, the neighbor router will send it to all its neighbor routers. After a series of modification triggering broadcast, each router can get and keep the updated routing information.
- At the same time, RIP broadcasts its routing table to the adjacent routers every 30 seconds. The adjacent routers will maintain their own routing tables after receiving the packets and will select an optimal route, and then advertise the modification

information to their respective adjacent networks so as to make the updated route globally known. Furthermore, RIP uses the timeout mechanism to handle the timeout routes so as to ensure the real time and validity of the routes.

RIPv2 undergoes a similar startup and running process, except that it sends updates to the multicast address 224.0.0.9 rather than sends them as broadcasts.

RIP is adopted by most of IP router suppliers. It can be used in most of the campus networks and the regional networks that are simple yet extensive. For larger and more complicated networks, RIP is not recommended.

3.1.5 RIP Features Available in V 2.41

Currently, the following RIP features are supported in V 2.41:

- RIP-1 and RIP-2.
- RIP multi-instance, running between CE and PE of the MPLS VPN solution as an interior routing protocol of the VPN.
- Equal-cost RIP routes.
- TRIP

IPX RIP is supported on IPX-enabled centralized equipment. (For detailed information on IPX and IPX RIP, refer to the “network protocol” section of this manual.)

3.2 RIP Configuration

Before you can configure RIP, you must enable it. This however does not necessarily the case when you configure interface-related features. Note that disabling RIP can disable RIP-related interface parameters.

1) Basic RIP configuration

Basic RIP configuration includes:

- Enable RIP
- Enable RIP on a network segment

In the event of running RIP on the links that do not support broadcast/multicast packets, unicast mode should be configured for RIP packet transmission so that RIP neighbors can be set up successfully.

With respect to NBMA link networking that adopts Frame Relay subinterfaces, split horizon should even be disabled to assure the correct routing information transmission.

2) RIP route management

RIP configuration on advertising and receiving routing information is described as follows:

- Configure additional metrics
- Configure the route redistribution of RIP
- Configure route filtering

- Disable host route
- Configure route aggregation
- Configure route exchange of indirectly connected RIP neighbors
- Configure traffic share across RIP interfaces

3) RIP parameters configuration

- Configure the RIP preference
- Configure RIP timer
- Configure zero field check for RIP
- Specify RIP version of an interface

4) Security issues

In order to improve RIP security during routing information exchange as well as to control the spreading area of RIP packets, following configuration is necessary.

- Configure RIP packet authentication
- Specify the operating state of the interface

5) RIP support for MPLS VPN

- Configure multi-instance of RIP

6) Configure TRIP

3.2.1 Enabling RIP

After RIP is enabled, you can enter the RIP view.

Perform the following configuration in system view.

Table 3-1 Enable RIP and enter the RIP view

Operation	Command
Enable RIP and enter the RIP view	**rip**
Disable RIP	**undo rip**

By default, RIP is not enabled.

Most of RIP features are configured in RIP view and a few are configured in interface view. The features pre-configured in interface view will not take effect until RIP is enabled. You should note that once **undo rip** command is executed to disable RIP, the RIP related features configured on the interface will also be deleted.

3.2.2 Enabling RIP on a Network Segment

To flexibly control RIP operation, you can specify some interfaces and configure the network where they are located into RIP networks, so that these interfaces can send and receive RIP packets.

Perform the following configuration in RIP view.

Table 3-2 Enable RIP network

Operation	Command
Enable RIP on the specified network	**network** *network-address*
Disable RIP on the specified network	**undo network** *network-address*

Note that the operating network segment must be specified after RIP is enabled. RIP only operates on the specified network segment. For an interface not on the specified network segment, RIP neither receives and send routes on it nor forwards its interface route, just as the interface does not exist. The *network-address* is an enabled or disabled network address, or an IP network address on each interface.

When the command **network** is used for an address, the interface of the network with this address is enabled. For example, for **network** 129.102.1.1, you can see **network** 129.102.0.0 either using **display current-configuration** or using **display rip** command.

If RIPv1 applies, note that:

- If the destination address of the current route and the address of the sending interface do not belong to the same network (natural network segment), the route is not sent to the neighbors if it is a supernet route. If it is a subnet route, it is sent after being summarized.
- If the destination address of the current route and the address of the sending interface belong to the same network, the route is sent to the neighbors unless the destination address of the route and the interface mask are unequal.

By default, RIP is disabled on all networks.

3.2.3 Configuring Split Horizon

Split horizon means that the route received via an interface will not be sent via this interface again. It avoids the creation of routing loops to some extent. But in some special cases, split horizon must be disabled so as to get correct advertising at the cost of efficiency. Disabling the split horizon has no effect on the point-to-point connected links but is applicable on the Ethernet.

Perform the following configuration in interface view.

Table 3-3 Configure split horizon

Operation	Command
Enable split horizon	**rip split-horizon**
Disable split horizon	**undo rip split-horizon**

By default, split horizon of the interface is enabled.

3.2.4 Configuring Additional Metrics

Additional metrics is the input or output metrics added to an RIP route. It does not change the metric value of the route in the routing table, but adds a specified metric value when the interface receives or sends a route.

Perform the following configuration in interface view.

Table 3-4 Configure additional metrics

Operation	Command
Set the additional metrics of the route when the interface receives an RIP packet	**rip metricin** *value*
Disable the additional metrics of the route when the interface receives an RIP packet	**undo rip metricin**
Set the additional metrics of the route when the interface sends an RIP packet	**rip metricout** *value* [**all-route**]
Disable the additional metrics of the route when the interface sends an RIP packet	**undo rip metricout**

By default, the additional metrics added to the route when RIP sends the packet is 1. The additional routing metrics when RIP receives the packet is 0 by default.

3.2.5 Configuring the Route Redistribution of RIP

RIP allows routes from other routing protocols to be redistributed into the RIP routing table. It also allows to set the default metrics used for redistribution.

RIP can redistribute these types of routes: Direct, Static, OSPF, BGP, and IS-IS.

Perform the following configuration in RIP view.

Table 3-5 Configure the route redistribution of RIP

Operation	Command
Redistribute routes from other protocols	**import-route** *protocol* [**allow-ibgp**] [**cost** *value*] [**route-policy** *route-policy-name*]
Cancel the redistribution of routes from other protocols	**undo import-route** *protocol*
Configure the default routing cost	**default cost** *value*
Restore the default routing cost	**undo default cost**

By default, RIP does not redistribute the route information of other protocols.

When the *protocol* argument is set to BGP, the keyword **allow-ibgp** is optional. Whereas the **import-route bgp** command redistributes only EBGP routes, the **import-route bgp allow-ibgp** command redistributes IBGP routes in addition and as such, must be used with cautions.

If no metrics is specified for redistributing a route, the default metrics will be used. The default value is 1.

3.2.6 Configuring Route Filtering

While receiving, advertising, and redistributing routes, the router may filter routes according to ACL, IP-prefix list, and/or routing policy.

Perform the following configuration in RIP view.

I. Configuring RIP to filter the received routes

With the **filter-policy import** command, RIP filters the routing tables sent from neighbors. The rejected routes do not appear in the local routing table.

Table 3-6 Configure RIP to filter the received routes

Operation	Command
Filter the received routing information redistributed by the specified address	**filter-policy gateway** *ip-prefix-name* **import**
Disable RIP to filter the routing information received from the specified address	**undo filter-policy gateway** *ip-prefix-name* **import**
Filter the received global routing information	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] } **import**
Disable RIP to filter the received global routing information.	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] } **import**
Filter the received global routing information by routing policy.	**filter-policy route-policy** *route-policy-name* **import**
Disable RIP to filter the received global routing information by routing policy.	**undo filter-policy route-policy** *route-policy-name* **import**

II. Configuring RIP to filter the redistributed routes

With the **filter-policy import** command, RIP filters routes when advertising the routing table to neighbors. The matched routes are not to be advertised.

Table 3-7 Configure RIP to filter the redistributed routes

Operation	Command
Filter the redistributed routing information	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export** [*routing-protocol*]
Cancel the filtering of the redistributed routing information	**undo filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export** [*routing-protocol*]

By default, RIP will not filter the received and redistributed routing information.

You may specify the *routing-protocol* argument to have RIP filter the routes redistributed from the specified routing protocol.

For more information, refer to the "Configure Route Filtering" part in "IP Routing Policy Configuration".

3.2.7 Disabling Host Route

In some special cases, the router can receive a lot of host routes from the same segment, and these routes are of little help in route addressing but consume a lot of network resources. After host route is disabled, a router can refuse a host route it receives.

Perform the following configuration in RIP view.

Table 3-8 Disable host route

Operation	Command
Enable host route receiving	**host-route**
Disable host route receiving	**undo host-route**

By default, the router receives the host route.

3.2.8 Configuring Route Aggregation

The so-called route aggregation means that different subnet routes in the same natural network can be aggregated into one natural mask route for transmission when they are sent to the outside (i.e. other network). Route aggregation can be performed to reduce the routing traffic on the network as well as to reduce the size of the routing table.

RIP-1 only sends the route with natural mask, that is, it always sends routes in the route aggregation form. RIP-2 supports classless inter-domain routing (CIDR). To advertise all the subnet routes, the route aggregation function of RIP-2 can be disabled.

Perform the following configuration in RIP view.

Table 3-9 Configure route aggregation

Operation	Command
Enable the route aggregation function of RIP-2	**summary**
Disable the route aggregation function of RIP-2	**undo summary**

By default, RIP-2 route aggregation is enabled.

3.2.9 Configuring Route Exchange of Indirectly Connected RIP Neighbors

By default, RIP sends RIP packets to directly connected segments only. When sending a unicast packet, RIP checks if the destination is directly connected; when receiving a RIP packet, RIP checks the source address and tries to find the ingress interface. According to this kind of mechanism, when two routers are indirectly connected RIP neighbors, no RIP information exchanging can take place.

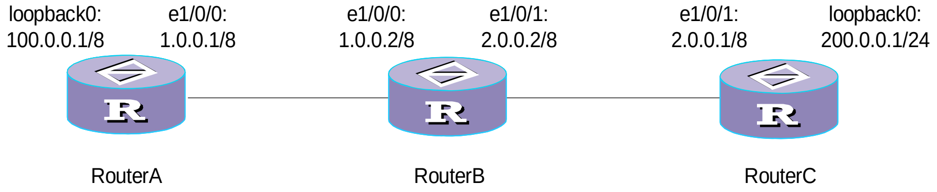


Figure 3-1 Route exchange of indirectly connected RIP neighbors

As shown in the above figure, if RouterA and RouterC are indirectly connected neighbors (only the 1.0.0.0/8 segment of RouterA and the 2.0.0.0/8 segment of RouterC are RIP-enabled, whereas RouterB is not RIP-enabled), to have RouterA and RouterC to exchange RIP routing information, configure as follows:

- Configure RouterA and RouterC to be RIP peers.
- Disable the checking of the source address of a received RIP packet.

After the above configuration, when sending unicast packets, the routers do not check the destination address for a directly connected address and removes the flag information that can prevent Router B from forwarding the packets; when receiving a RIP packet, they do not check the source address of the packet, and can use the source address and destination address of the packet to locate the ingress interface.

I. Configuring unicast of RIP packets

Generally, RIP forwards packets using broadcast or multicast addresses. To run RIP on a link not supporting broadcast packets, you must employ unicast transmission; otherwise, the RIP neighborhood cannot be established properly. You must also configure unicast of RIP packets when the routers running RIP are not directly connected neighbors.

Perform the following configuration in RIP view.

Table 3-10 Configure unicast of RIP packets

Operation	Command
Configure unicast of RIP packets	**peer** *ip-address*
Disable unicast of RIP packets	**undo peer** *ip-address*

By default, RIP does not send any packet to any unicast address.

Noted that **peer** is restricted by the operation status of the interface, which, in turn, is configured by the **rip work**, **rip output, rip input**, or **network** commands.

II. Configuring to check the source address of a RIP packet

Perform the following configuration in RIP view or RIP MBGP address family view.

Table 3-11 Configure to check the source address of a RIP packet

Operation	Command
Configure to check the source address of a RIP packet	**validate-source-address**
Disable the checking of the source address of a RIP packet	**undo validate-source-address**

This command applies to the RIP protocol both running in public networks and private networks in a MPLS VPN.

By default, the source address of a RIP packet is checked.

3.2.10 Configuring Traffic Sharing Across RIP Interfaces

You may enable traffic sharing across multiple RIP interfaces to have them share traffic equally through equal-cost routes.

Perform the following configuration in RIP view or RIP MBGP address family view.

Table 3-12 Configure traffic sharing across RIP interfaces

Operation	Command
Configure traffic sharing across RIP interfaces	**traffic-share-across-interface**
Disable traffic sharing across RIP interfaces	**undo traffic-share-across-interface**

This command applies to the RIP protocol both running in public networks and private networks in a MPLS VPN.

By default, traffic sharing across RIP interfaces is disabled. A simpler traffic sharing mechanism is supported instead.

3.2.11 Configuring the RIP Preference

Each kind of routing protocol has its own preference, by which the routing policy will select the optimal one from the routes of different protocols. The greater the preference value is, the lower the preference becomes. The preference of RIP can be set manually.

Perform the following configuration in RIP view.

Table 3-13 Set the RIP preference

Operation	Command
Set the RIP preference	**preference** *value*
Restore the default value of RIP preference	**undo preference**

By default, the preference of RIP is 100.

3.2.12 Configuring RIP Timers

It has been introduced at the beginning of this chapter that RIP has three timers, Period update, Timeout and Garbage-collection. The modification on the values of these timers will affect the convergence speed of RIP.

Perform the following configuration in RIP view.

Table 3-14 Configure RIP timers

Operation	Command
Set values for RIP timers	**timers** { **update** *update-timer-length* | **timeout** *timeout-timer-length* } *
Restore the default values	**undo timers** { **update | timeout** } *

The RIP timer values will take effect immediately after the modification.

The default value of timer Period update is 30 seconds, that of timer Timeout is 180 seconds and that of timer Garbage-collection is fixedly as 4 times as that of timer Period update, i.e., 120 seconds.

In practice, you may find that the timing length of timer Garbage-collection is not fixed. For instance, given the timer Period update is set to 30 seconds, the timing length of the timer Garbage-collection may be 90 to 120 seconds. This is because a router needs to wait for 4 update packets from the same neighbor before completely removing an unreachable route from the routing table. However, when a route changes into the unreachable state is not just the beginning of a new update period. So the actual timing length of the timer Garbage-collection is about 3 to 4 times as that of the timer Period update.

🕮 **Note:**

During the RIP timer configuration, you should take the network performance into consideration when modifying the timer value and keep consistent of configurations on all routers that run RIP to avoid adding unnecessary network traffic or causing network route oscillation.

3.2.13 Configuring Zero Field Check of an Interface Packet

As RFC1058 provides, some fields in a RIP-1 packet must be 0, and they are called zero fields. Therefore, when an interface version is set as RIP-1, the zero field check should be performed on the packet. But if the value in the zero filed is not zero, processing will be refused. As there are no zero fields in an RIP-2 packet, this configuration is invalid for RIP-2.

Perform the following configuration in RIP view.

Table 3-15 Configure zero field check of an interface packet

Operation	Command
Configure zero field check on the RIP-1 packet	**checkzero**
Disable zero field check on the RIP-1 packet	**undo checkzero**

By default, zero field check is enabled on RIP-1 packets.

3.2.14 Specifying the RIP Version of an Interface

RIP has two versions, RIP-1 and RIP-2. You can specify the version of the RIP packet processed by an interface.

RIP-1 broadcasts the packets. RIP-2 can transmit packets by both broadcast and multicast. By default, multicast is adopted for packets transmission. In RIP-2, the multicast address is 224.0.0.9. The advantage of multicast packet transmission is that it prevents RIP-disabled hosts from receiving RIP broadcast packets. In addition, it also helps RIP-1-enabled hosts to avoid mistakenly receiving and processing routes with subnet masks of RIP-2. When RIP-2 is enabled on an interface, RIP-1 packets can also be received.

Perform the following configuration in interface view.

Table 3-16 Specify the RIP version of an interface

Operation	Command
Specify the interface version as RIP-1	**rip version 1**
Specify the interface version as RIP-2	**rip version 2** [**broadcast** | **multicast**]
Restore the default operating RIP version on an interface	**undo rip version** { **1** | **2** }

By default, the interface receives and sends RIP-1 packets. When the interface RIP version is set to RIP-2, the interface will transmit packets in multicast mode.

3.2.15 Configuring RIP Packet Authentication

RIP-1 does not support packet authentication. But when the interface operates RIP-2, the packet authentication can be configured.

RIP-2 supports two authentication modes, plain text authentication and MD5 authentication. MD5 authentication uses two packet formats: One follows RFC1723 (RIP Version 2 Carrying Additional Information) and the other follows the RFC2082 (RIP-2 MD5 Authentication).

The plain text authentication does not ensure security. The authentication key not encrypted is sent together with the packet, so the plain text authentication cannot be applied to the case with higher security requirements.

Perform the following configuration in interface view.

Table 3-17 Set RIP packet authentication

Operation	Command
Configure RIP-2 plain text authentication key	**rip authentication-mode simple** *password*
Configure RIP-2 use usual MD5 authentication packet format	**rip authentication-mode md5 huawei** *key-string*
Configure RIP-2 use nonstandard MD5 authentication packet format	**rip authentication-mode md5 rfc2082** *key-id key-string*
Cancel authentication of RIP-2 packet	**undo rip authentication-mode**

When configuring MD5 authentication, you need to specify the type of MD5 authentication. Two options are available: huawei, which supports the

RFC2453-compliant packet format; and rfc2082, which supports the RFC2082-compliant packet format.

3.2.16 Specifying the Operating State of the Interface

In interface view, you can specify the operating state of RIP on the interface. For example, whether RIP is enabled on the interface, namely, whether RIP update packets are sent and received on the interface. You can also singly specify an interface to send (or receive) RIP update packet.

Perform the following configuration in interface view.

Table 3-18 Specify the Operating State of the Interface

Operation	Command
Enable RIP on an interface	**rip work**
Disable RIP on an interface	**undo rip work**
Enable an interface to receive RIP update packet	**rip input**
Disable an interface to receive RIP update packet	**undo rip input**
Enable an interface to send RIP update packet	**rip output**
Disable an interface to send RIP update packet	**undo rip output**

Like the **undo rip work** command in interface view, the **undo network** command in RIP view can disable an interface from receiving or transmitting RIP routes. They are different in the sense that the **undo rip work** command does not prevent other interfaces from forwarding the route of the interface while the **undo network** can prevent RIP from advertising the route of the interface and as a result no route is available for forwarding the packets intended for this interface.

Executing the **rip work** command is equivalent to executing the **rip input** and **rip output** commands.

By default, an interface both receives and transmits RIP update packets.

3.2.17 Configuring Multi-instance of RIP

The router supports the function RIP multiple instances and can support MPLS VPN.

Perform the following configuration in RIP view.

Table 3-19 Configure multi-instance

Operation	Command
Enter MBGP address family view of RIP	**ipv4-family** [**unicast**] **vpn-instance** *vpn-instance-name*
Remove the configuration of MBGP address family view of RIP	**undo ipv4-family** [**unicast**] **vpn-instance** *vpn-instance-name*

All configurations in MBGP address family view will be removed after the **undo ipv4-family** command is executed.

MBGP address family view applies to BGP/MPLS VPN. For related description, refer to "MPLS VPN Configuration" chapter in module "MPLS" of this manual.

3.2.18 Configuring TRIP

Perform the following configuration in interface (except for Ethernet, ATM, loopback, tunnel, and bridge-template interfaces) view.

Table 3-20 Configure TRIP

Operation	Command
Enable TRIP	**rip triggered**
Disable TRIP	**undo rip triggered**

By default, TRIP is disabled.

TRIP is compatible with RIP-1 and RIP-2 extensions.

3.3 Displaying and Debugging RIP

After the above configuration, execute **display** command in all views to display the running of the RIP configuration, and to verify the effect of the configuration. Execute **debugging** command in user view to debug the RIP module.

Table 3-21 Display and debug RIP

Operation	Command
Display the current RIP running state and configuration information	**display rip**
Display information about RIP interfaces.	**display rip interface** [**vpn-instance** *vpn-instance-name*]
Display the configuration of RIP MPGP address family	**display rip vpn-instance** *vpn-instance-name*

Operation	Command
Display the RIP routing table	**display rip routing** [**vpn-instance** *vpn-instance-name*]
Enable packet debugging of RIP.	**debugging rip packets** [**interface** *type number*]
Disable the packet debugging of RIP	**undo debugging rip packets**
Enable the packet receiving debugging of RIP	**debugging rip receive**
Disable the packet receiving debugging of RIP	**undo debugging rip receive**
Enable packet sending debugging of RIP	**debugging rip send**
Disable packet sending debugging of RIP	**undo debugging rip send**

3.4 RIP Configuration Example

3.4.1 Configuring the Operating State of the Specified Interface

I. Network requirements

An intranet is connected to the Internet through Router A. The hosts on the intranet are directly connected to Router B or Router C.

Enable RIP on these three routers and configure them as follows:

- Router A can receives routing information from external networks but cannot advertise the routing information of the intranet to the external networks.
- Routers A, B, and C can exchange RIP information between them to have the hosts on the intranet to access the Internet.

II. Network diagram

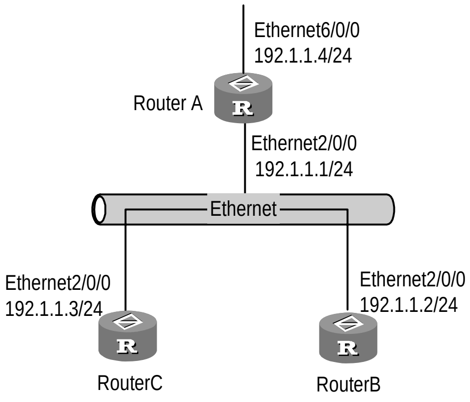


Figure 3-2 Configure the operating state of an interface

III. Configuration procedure

1) Configure RouterA:

# Configure the interfaces Ethernet 2/0/0 and Ethernet 6/0/0.

```
[Router A] interface ethernet 2/0/0
[Router A-Ethernet2/0/0] ip address 192.1.1.1 255.255.255.0
[RouterA-Ethernet2/0/0] quit
[RouterA] interface ethernet 6/0/0
[RouterA-Ethernet6/0/0] ip address 192.1.2.1 255.255.255.0
```

# Configure RIP, and configure Ethernet 2/0/0 and Ethernet 6/0/0 to run RIP.

```
[Router A] rip
[Router A-rip] network 192.1.1.0
[Router A-rip] network 192.1.2.0
```

# Configure the interface Ethernet 6/0/0 of Router A to receive RIP packets only.

```
[RouterA] interface ethernet 6/0/0
[Router A-Ethernet6/0/0] undo rip output
[Router A-Ethernet6/0/0] rip input
```

2) Configure RouterB:

# Configure the interface Ethernet 2/0/0.

```
[Router B] interface Ethernet 2/0/0
[Router B-Ethernet2/0/0] ip address 192.1.1.2 255.255.255.0
```

# Configure RIP, and configure Ethernet 2/0/0 to run RIP.

```
[Router B] rip
[Router B-rip] network 192.1.1.0
[RouterB-rip] import direct
```

3) Configure RouterC:

# Configure the interface Ethernet 2/0/0.

```
[Router C] interface Ethernet 2/0/0
[Router C-Ethernet2/0/0] ip address 192.1.1.3 255.255.255.0
```

# Configure RIP, and configure Ethernet 2/0/0 to run RIP.

```
[Router C] rip
[Router C-rip] network 192.1.1.0
[RouterC-rip] import direct
```

3.4.2 Adjusting the Convergence Time of RIP Network

I. Network requirements

Apply RIP on RouterA, RouterB and RouterC and set the network convergence time within 30 seconds.

II. Network diagram

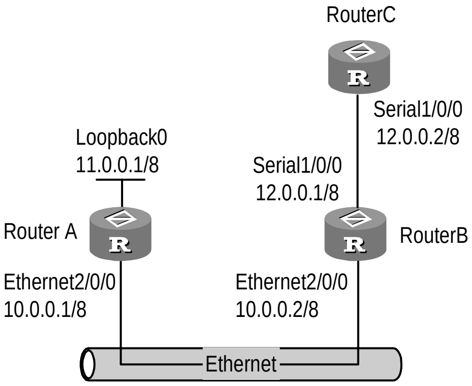


Figure 3-3 Configure RIP timer

III. Configuration procedure

📖 **Note:**

For the IP address configuration of the interface, refer to Figure 3-3.

---

1) Configure RouterA:

# Enable RIP and apply it on the interface Ethernet2/0/0 of RouterA as well as on LoopBack0.

```
[RouterA] rip
[RouterA-rip] network 10.0.0.0
[RouterA-rip] network 11.0.0.0
[RouterA-rip] timers update 10 timeout 30
```

2) Configure RouterB:

# Enable RIP and apply it on the interface Ethernet2/0/0 and Serial1/0/0 of RouterB.

```
[RouterB] rip
[RouterB-rip] network 10.0.0.0
[RouterB-rip] network 12.0.0.0
[RouterB-rip] timers update 10 timeout 30
```

3) Configure RouterC:

# Enable RIP and apply it on the interface Serial1/0/0 of RouterC.

```
[RouterC] rip
[RouterC-rip] network 12.0.0.0
[RouterC-rip] timers update 10 timeout 30
```

After the above configuration, executing **display ip routing-table** command on RouterB and RouterC, you can view the information of route 11.0.0.0/8. Shut down the interface Ethernet2/0/0 of RouterA, you can view that the route state of 11.0.0.0/8 to RouterB and RouterC changes into unreachable state within 30 seconds.

Before the timer is adjusted, it takes 180 seconds for RouterB and RouterC to know that the route is unreachable after the interface Ethernet2/0/0 of RouterA is shut down. Therefore, the convergence time of RIP network is cut down due to the adjustment on the timer.

3.4.3 Configuring Route Exchange of Indirectly Connected RIP Neighbors

I. Network requirements

As shown in the following figure, RouterB does not support the RIP protocol. the e1/0/0 interface of RouterA is RIP-enabled, directly connected routes are redistributed and configured to point to the static route of 2.0.0.0/8. The e1/0/1 interface of RouterC is RIP-enabled, directly connected routes are redistributed and configured to point to the static route of 1.0.0.0/8. RouterA and RouterC are configured to be RIP peers. The checking of the source address of the received RIP packet is disabled. The aim is to obtain the RIP route of 200.0.0.1/24 to RouterC on RouterA, and the RIP route of 100.0.0.1/8 to RouterA on RouterC.

II. Network diagram

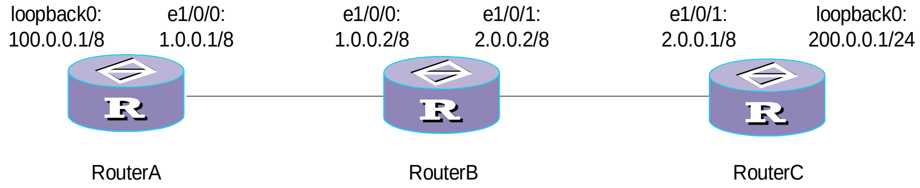


Figure 3-4 Configure route exchange of indirectly connected RIP neighbors

III. Configuration procedure

1) Configure RouterA:

# Configure the IP address of the interface.

```
[RouterA ] interface Ethernet1/0/0
[RouterA-Ethernet1/0/0] ip address 1.0.0.1 255.0.0.0
[RouterA-Ethernet1/0/0] rip version 2
[RouterA-Ethernet1/0/0] interface LoopBack0
[RouterA-LoopBack0] ip address 100.0.0.1 255.0.0.0
[RouterA-LoopBack0] quit
```

# Enable the RIP protocol.

```
[RouterA ] rip
```

```
[RouterA-rip ] undo summary
[RouterA-rip ] network 1.0.0.0
```

# Configure the RIP peer and configure not to check the source address of the RIP packet.

```
[RouterA-rip ] peer 2.0.0.1
[RouterA-rip ] undo validate-source-address
```

# Configure RIP to redistribute directly connected routes.

```
[RouterA-rip ] import-route direct
[RouterA-rip] quit
```

# Configure the static route to the 2.0.0.0 segment.

```
[RouterA ] ip route-static 2.0.0.0 255.0.0.0 1.0.0.2 preference 60
```

2) Configure RouterB:

# Configure the IP address of the interface.

```
[RouterB ] interface Ethernet1/0/0
[RouterB-Ethernet1/0/0 ] ip address 1.0.0.2 255.0.0.0
[RouterB-Ethernet1/0/0 ] interface Ethernet1/0/1
[RouterB-Ethernet1/0/1 ] ip address 2.0.0.2 255.0.0.0
```

3) Configure RouterC:

# Configure the IP address of the interface.

```
[RouterC] interface Ethernet1/0/1
[RouterC-Ethernet1/0/1] ip address 2.0.0.1 255.0.0.0
[RouterC-Ethernet1/0/1] rip version 2
[RouterC-Ethernet1/0/1] interface LoopBack0
[RouterC-LoopBack0] ip address 200.0.0.1 255.255.255.0
```

# Enable the RIP protocol.

```
[RouterC] rip
[RouterC-rip] undo summary
[RouterC-rip] network 2.0.0.0
```

# Configure the RIP peer and configure not to check the received RIP packets.

```
[RouterC-rip] peer 1.0.0.1
[RouterC-rip] undo validate-source-address
```

# Configure the ingress directly connected route.

```
[RouterC-rip] import-route direct
[RouterC-rip] quit
```

# Configure the static route to the 1.0.0.0 segment.

```
[RouterC] ip route-static 1.0.0.0 255.0.0.0 2.0.0.2 preference 60
```

RouterA and C must be configured with static routes to the peer and the static route must be reachable; otherwise, RIP packets are unable to be send to the peer.

In addition, when RouterC functions as a PE, you must configure RIP multi-instance, and you must configure not to check the received RIP packets in RIP MBGP address family view:

# Configure vpn-instance.

```
[RouterC] ip vpn-instance in
[RouterC-vpn-in] route-distinguisher 100:1
[RouterC-vpn-in] vpn-target 100:1 export-extcommunity
[RouterC-vpn-in] vpn-target 100:1 import-extcommunity
[RouterC-vpn-in] quit
```

# Configure RIP multi-instance.

```
[RouterC] rip
[RouterC-rip] ipv4-family vpn-instance in
[RouterC-rip-af-vpn-instance] undo validate-source-address
```

3.4.4 Configuring TRIP

I. Network requirements

Router A and Router B are connected using a dial-up connection. On the connected dial interfaces, TRIP is enabled.

II. Network diagram

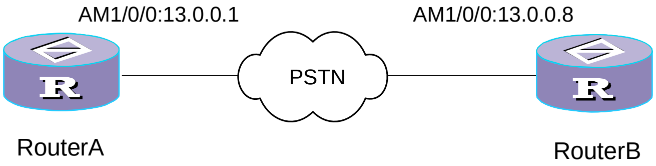


Figure 3-5 Network diagram for TRIP

III. Configuration procedure

1) Configure Router A

```
<Router> system-view
[Router] dialer-rule 1 ip permit
```

# Configure the AM interface and enable TRIP on the interface.

```
[Router] interface Analogmodem1/0/0
[Router-Analogmodem1/0/0] async mode protocol
[Router-Analogmodem1/0/0] link-protocol ppp
[Router-Analogmodem1/0/0] ip address 13.0.0.1 255.0.0.0
[Router-Analogmodem1/0/0] rip triggered
```

# Configure C-DCC.

```
[Router-Analogmodem1/0/0] dialer enable-circular
```

```
[Router-Analogmodem1/0/0] dialer-group 1
[Router-Analogmodem1/0/0] dialer number 6688012
[Router-Analogmodem1/0/0] quit
```

# Enable RIP on network segment 13.0.0.0/8.

```
[Router] rip
[Router-rip] network 13.0.0.0
[Router-rip] quit
```

# Configure the TTY interface corresponding to the AM interface.

```
[Router] user-interface tty 33 44
[Router-ui-tty 33 44] modem both
```

2) Configure Router B

```
<Router> system-view
```

# Configure the AM interface and enable RIP on it.

```
[Router] interface Analogmodem3/0/0
[Router-Analogmodem1/0/0] async mode protocol
[Router-Analogmodem1/0/0] link-protocol ppp
[Router-Analogmodem1/0/0] ip address 13.0.0.2 255.0.0.0
```

# Configure C-DCC.

```
[Router-Analogmodem1/0/0] rip triggered
[Router-Analogmodem1/0/0] dialer enable-circular
[Router-Analogmodem1/0/0] dialer-group 1
[Router-Analogmodem1/0/0] dialer number 6688003
[Router-Analogmodem1/0/0] quit
```

# Enable RIP on network segment 13.0.0.0.

```
[Router] rip
[Router-rip] network 13.0.0.0
[Router-rip] quit
```

# Configure the TTY interface corresponding to the AM interface.

```
[Router] user-interface tty 49
[Router-ui-tty 49] modem both
```

3.5 Troubleshooting RIP

Symptom 1: The update packet cannot be received when the physical connection is normal.

Troubleshooting:

It may be caused by the following reasons:

RIP is not enabled on the corresponding interface (for example, the **undo rip work** command is executed) or this interface is not enabled through the **network** command.

The opposite router is configured as the multicast mode (for example, the **rip version 2 multicast** command is executed) but the local router is not configured as the multicast mode.

Symptom 2: Route oscillation occurs to the network running RIP.

Troubleshooting: Use **display rip** command on each router that runs RIP to view the configuration of RIP timers. If the values of Period update timer and Timeout timer on different routers are different, you should reset them conformably and make sure that the timing length of Timeout timer is longer than that of Period update timer.

Chapter 4 OSPF Configuration

4.1 OSPF Overview

4.1.1 Introduction to OSPF

OSPF (Open Shortest Path First) is a link state-based internal gateway protocol developed by IETF organization. At present, OSPF version 2 (RFC2328) is used, which allows of the following features:

- Applicable scope: It can support networks in various sizes and can support several hundred routers at maximum.
- Fast convergence: It can transmit the update packets instantly after the network topology changes so that the change is synchronized in the AS.
- Loop-free: Since the OSPF calculates routes with the shortest path tree algorithm according to the collected link states, it is guaranteed that no loop routes will be generated from the algorithm itself.
- Area partition: It allows the network of AS to be divided into different areas for the convenience of management so that the routing information transmitted between the areas is abstracted further, hence to reduce the network bandwidth consumption.
- Equal-cost multi-route: Support multiple equal-cost routes to a destination.
- Routing hierarchy: OSPF has a four-level routing hierarchy. It prioritizes the routes to be intra-area, inter-area, external type-1, and external type-2 routes.
- Authentication: It supports the interface-based packet authentication so as to guarantee the security of the route calculation.
- Multicast transmission: Support multicast address to receive and send packets.

4.1.2 Process of OSPF Route Calculation

The routing calculation process of the OSPF protocol is as follows:

- Each OSPF-capable router maintains a Link State Database (LSDB), which describes the topology of the whole AS. According to the network topology around itself, each router generates a Link State Advertisement (LSA). The routers on the network transmit the LSAs among them by transmitting the protocol packets to each other. Thus, each router receives the LSAs of other routers and all these LSAs compose its LSDB.
- LSA describes the network topology around a router, so the LSDB describes the network topology of the whole network. Routers can easily transform the LSDB to a weighted directed map, which actually reflects the topology architecture of the whole network. Obviously, all the routers get a map exactly the same.

- A router uses the SPF algorithm to calculate the shortest path tree with itself as the root. The tree shows the routes to the nodes in the autonomous system. The external routing information is leaf node. A router, which advertises the routes, also tags them and records the additional information of the autonomous system. Obviously, the routing tables obtained by different routers are different.

Furthermore, to enable individual routers to broadcast information (such as available interface information and reachable neighbor information) of their local statuses to the whole AS, any two routers in the environment should establish adjacency between them. In this case, the route changes on any router will result in multiple transmissions, which are unnecessary and waste the precious bandwidth resources. To solve this problem, designated Router" (DR) is defined in the OSPF. Thus, all the routers only send information to the DR for broadcasting the network link states in the network. Thereby, the number of adjacent router relations on the multi-access network is reduced.

OSPF supports interface-based packet authentication to guarantee the security of route calculation. Also, it transmits and receives packets by IP multicast.

4.1.3 Basic Concepts Related to OSPF

I. Router ID

Every OSPF router must have a Router ID. You may assign one to an OSPF router manually. This Router ID is preferably the address of a loopback interface, because a loopback interface is always up until it is manually shut down. If no Router ID is specified, the system automatically selects one for the router as follows:

- If IP addresses of loopback interfaces are available, select the last configured one.
- If not, select the first configured physical interface that is up.

II. DR and BDR

- DR (Designated Router)

In the broadcast network or NBMA network, in order for each router to broadcast its local state information to the whole AS (Autonomous System), multiple neighboring relationships should be created between routers. This, however, makes it possible for route variation of any router to result in repeated transmission, which wastes the valuable bandwidth resource. To solve the problem, OSPF defines the "Designated Router" (DR). All the routers only need to transmit information to the DR for broadcasting the network link states. Neighboring relationship is not established between two routers other than DRs (called as DR Others), nor do the DR Others exchange any routing information.

It is not manually specified which router will be the DR of the local network segment, but commonly selected by all the routers in the network segment.

- BDR (Backup Designated Router)

If a DR becomes invalid due to some fault, it must be reelected and synchronized. It takes time and meanwhile the route calculation is incorrect. In order to speed up this process, OSPF puts forward the concept of BDR. In fact, BDR is a backup for DR. DR and BDR are elected in the mean time. The adjacencies are also established between the BDR and all the routers on the segment, and routing information is also exchanged between them. Once a DR becomes invalid, the BDR will immediately turn into a DR, and a new BDR will be reelected.

III. Area

When a large number of OSPF routers are present on a network, LSDBs may become so large that a great amount of storage room is occupied and CPU resources are exhausted performing SPF computation. In addition, as the topology of a large network is prone to changes, enormous amount of OSPF packets may be created, decreasing bandwidth utilization.

To solve this problem, OSPF splits an AS into multiple areas, which are identified by area IDs. In logical sense, the areas put routers into different groups. The area 0, also known as backbone area, is of the most significance.

The backbone area achieves routing information exchange between the non-backbone areas. The backbone area and other non-backbone areas must be physically consecutive. Otherwise, you have to configure virtual links to make them consecutive.

The router connecting the backbone area and another area is called area border router (ABR).

There also exists the autonomous system boundary router (ASBR) in OSPF, which connects OSPF routing domain and the router running other routing protocols can be taken as the router redistributing OSPF external routing information.

IV. Route aggregation

An AS is divided into areas that are interconnected via OSPF ABRs. The routing information between areas can be reduced through route aggregation. Thus, the size of routing table can be reduced and the calculation speed of the router can be improved.

After calculating an intra-area route of an area, the ABR will look up the routing table and encapsulate each OSPF route into an LSA and send it outside the area.

For example, in Figure 4-1, there are three intra-area routes in Area 19, 19.1.1.0/24, 19.1.2.0/24 and 19.1.3.0/24. If route aggregation is configured and the three routes are aggregated into one route 19.1.0.0/16, only one LSA, which describes the route after aggregation, is generated on RTA.

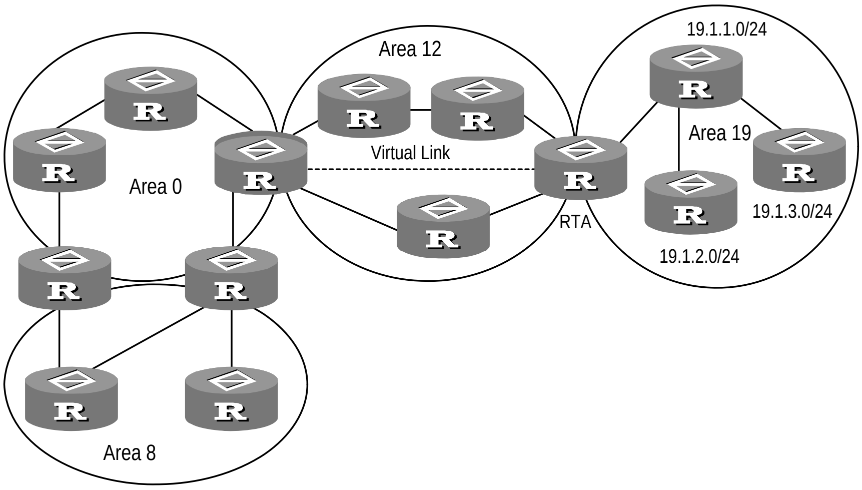


Figure 4-1 Area and route aggregation

4.1.4 OSPF Packets

OSPF uses five types of packets:

- Hello Packet:

A kind of most commonly used packet, which is periodically sent to the peer of a local router. It contains the values of some timers, DR, BDR and the known peer.

- DD packet (Database Description Packet):

When two routers synchronize their databases, they use the DD packets to describe their own LSDBs, including the summary of each LSA. The summary refers to the HEAD of an LSA, which can be used to uniquely identify the LSA. This reduces the traffic size transmitted between the routers, since the HEAD of an LSA only occupies a small portion of the overall LSA traffic. With the HEAD, the peer router can judge whether it already has had the LSA.

- Link State Request (LSR) Packet:

After exchanging the DD packets, the two routers know which LSAs of the peer routers are lacked in the local LSDBs. In this case, they will send LSR packets requesting for the needed LSAs to the peers. The packets contain the summary of the needed LSAs.

- Link State Update (LSU) Packet:

The packet is used to transmit the needed LSAs to the peer router. It contains a collection of multiple LSAs (complete contents).

- Link State Acknowledgment (LSAck) Packet

The packet is used to acknowledge the received LSU packets. It contains the HEAD(s) of LSA(s) to be acknowledged (a packet can acknowledge multiple LSAs).

4.1.5 LSA Types Available in OSPF

I. Five types of basic LSAs

OSPF calculates and maintains routing information primarily by sending LSAs.

Five types of LSAs are defined in RFC2328:

- Router-LSAs: Type-1 LSAs, generated by individual routers to describe their link state and cost and only advertised in the area for the routers themselves
- Network-LSAs: Type-2 LSAs, generated by the DRs of broadcast network or NBMA network to describe the links state for the network segment and only advertised in the area for the DRs themselves.
- Summary-LSAs: Type-3 and Type-4 LSAs, generated by ABRs and advertised in the areas associated. Each Summary-LSA describes a route to the AS in question or a destination in other areas (called inter-area route). Type-3 Summary-LSAs are for routes to network, that is their destinations are segment, while Type-4 Summary-LSAs are for the routes to ASBRs.
- AS-external-LSAs: Type-5 LSAs, generated by ASBR to describe the routes to other ASs and advertised to the whole AS (excluding STUB areas). The default AS route can also be described by AS-external-LSAs.

II. LSA type-7

In RFC1587 (OSPF NSSA Option), NSSA (Not-So-Stubby Area) LSAs, also known as LSAs Type-7 are added.

The major differences between Type-7 LSAs and Type-5 LSAs are illustrated in these two points:

- Type-7 LSAs are generated and advertised in NSSA, where Type-5 LSAs are not generated and advertised.
- Type-7 LSAs are only advertised in one NSSA. They are converted to Type-5 LSAs when they reach the ABRs, for being advertised to other areas or backbone area.

III. Opaque LSAs

In RFC2370 (The OSPF Opaque LSA), Opaque LSAs, which extends OSPF, are defined.

Opaque LSAs also include three types, each with particular spread range:

- Type-9: The spread range is link-local, i.e. only the segment for a certain interface, not beyond the local segment or local subnet.
- Type-10: The spread range is area-local, i.e. only the local area.
- Type-11: The spread range is identical with that for Type-5 LSAs, i.e. the whole AS excluding STUB areas and NSSAs.

An opaque LSA includes a standard 20-byte LSA header and application information-specific domain. See the following figure:

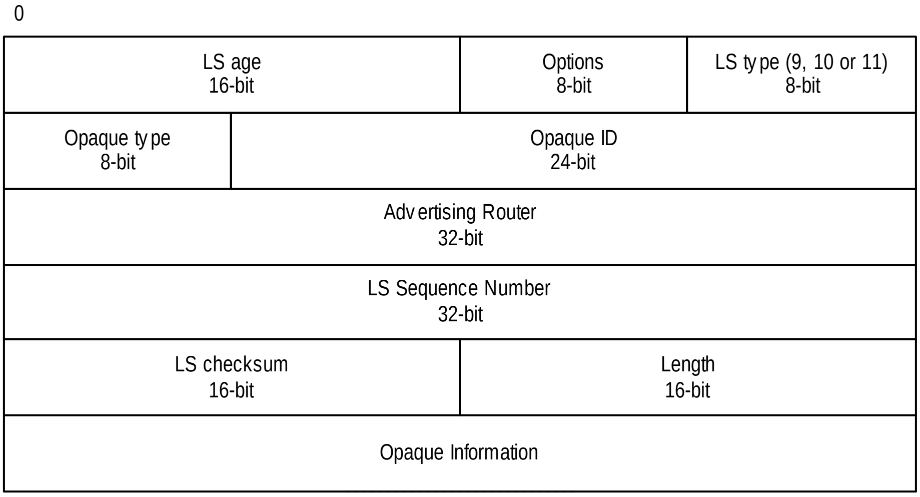


Figure 4-2 Opaque LSA architecture

The Opaque Type field indicates LSA application type, while the Opaque ID field differentiates the LSAs of the same application type.

The Opaque Information field stores the LSA-borne information, whose format may be defined accordingly.

4.1.6 OSPF Features Available in V 2.41

Currently, the V 2.41 supports these OSPF features:

- OSPF STUB area
- OSPF NSSA area
- OSPF multi-process, that is, a router runs multiple OSPF processes
- OSPF multi-VPN-instance, which runs between a CE and a PE as intra-VPN routing protocol
- MPLS traffic engineering (TE), using Type-10 Opaque LSAs with opaque type being 1 (For the application of OSPF in MPLS VPN, refer to the “MPLS” part of this manual.)
- Prioritized selection and backup of the conflicting routes of the same type across areas (not necessarily non-backbone areas) (Conflicting routes refer to routes calculated using the same LSA)

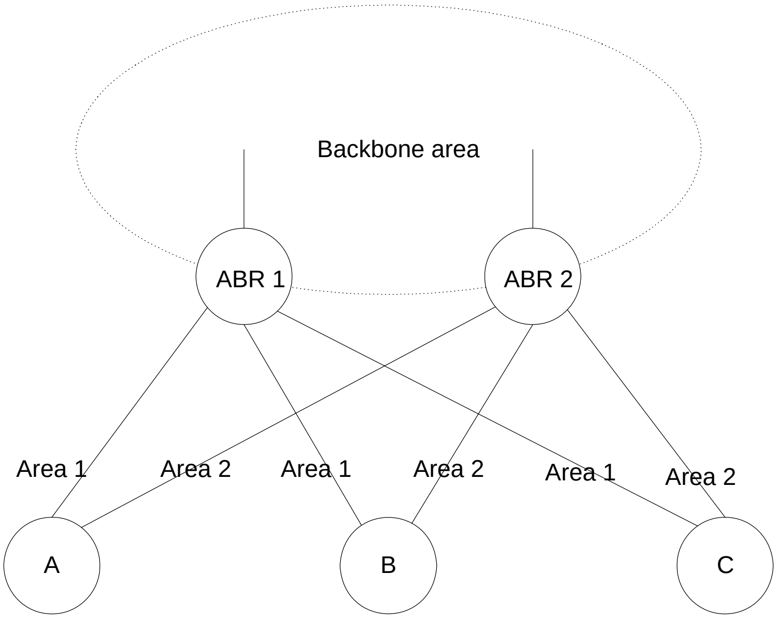


Figure 4-3 Network diagram for route backup across non-backbone areas

As shown in the above figure, devices A, B, and C are working as edge devices. They are each connected to the same two non-backbone areas (stub or NSSA) to back up their upstream routes. As the change and delete of a route in one area could trigger the route calculation in the other area, dynamic route update, selection, and backup is achieved.

When cross-area prioritized selection and backup of conflicting routes is used, the route calculations in the involved non-backbones are correlated. If multiple conflicting routes of the same type from multiple areas are present, any change of these routes could result in route recalculation in multiple areas and increases calculation load as a result. For this reason, using multiple non-backbone areas for route backup is not recommended.

4.2 OSPF Configuration

Among all the configuration tasks, only after OSPF is enabled, interface number and area number are specified, can other functions be configured. But the configuration of the functions related to the interface is not restricted by whether the OSPF is enabled or not. It should be noted that after OSPF is disabled, the OSPF-related interface parameters also become invalid.

1) Basic OSPF configuration

- Configure Router ID
- Enable OSPF process
- Enter OSPF area view
- Specify the network segment

If the OSPF backbone area is not consecutive, then it is required to

- Configure OSPF virtual link

If the network types for OSPF are different, then it is required to

- Configure network type
- Configure the adjacent point

2) OSPF route management

- Configure OSPF to redistribute routes
- Configure OSPF route filtering
- Configure route aggregation by OSPF

3) OSPF parameters configuration

- Set OSPF route preference
- Configure OSPF timers
- Set the interface priority for DR election
- Configure the cost for sending packets
- Set a PSF calculation interval for OSPF
- Configure an interval required for sending LSU packets
- Configure whether the MTU field will be filled in
- Configure maximum number of OSPF equal-cost routes

4) Security considerations

To improve the security of route information exchange or restrict propagation of OSPF packets, perform the following two tasks.

- Configure OSPF authentication
- Disable/enable the interface to send OSPF packets

5) OSPF advanced features configuration

- Configure STUB area of OSPF
- Configure NSSA parameters of OSPF
- Enable Opaque capacity of OSPF
- Configure OSPF to work with NMS
- Reset an OSPF process

Note:

For OSPF multi-instance application and OSPF configuration in MPLS VPN, refer to the VPN part. For OSPF application and configuration in MPLS TE, refer to the MPLS part.

4.2.1 Configuring Router ID

Router ID is a 32-bit unsigned integer that uniquely identifies a router within an AS. Router ID can be configured manually. If router ID is not configured, the system will automatically select one from IP addresses of the current interfaces as the router ID. When you do that manually, you must guarantee that the IDs of any two routers in the AS are unique. A common practice is to set the router ID to be the IP address of an interface on the router.

Perform the following configuration in system view.

Table 4-1 Configure a router ID

Operation	Command
Configure a router ID	**router id** *router-id*
Remove a router ID	**undo router id**

To ensure stability of OSPF, the user should determine the division of router IDs and manually configure them when implementing network planning.

🕮 **Note:**

The router IDs modified after OSPF is enabled will not take effect until the OSPF is reset.

4.2.2 Enabling OSPF Process

OSPF supports multiple-process. When multiple processes are enabled on a router, it is necessary to specify different numbers for them. OSPF process number is a local concept, with no effect on its packet exchange with other routers. Therefore, even though the process numbers of different routers are different, packet exchange is available.

Perform the following configuration in system view.

Table 4-2 Enable/disable OSPF

Operation	Command
Enable OSPF and enter OSPF view	**ospf** [*process-id* [[**router-id** *router-id*] **vpn-instance** *vpn-instance-name*]]
Disable OSPF routing protocol process	**undo ospf** [*process-id*]

By default, OSPF is not enabled.

Notice theses items in enabling OSPF:

- The default process ID 1 will be selected if no one is specified when configuring the **ospf** command; process ID 1 is disabled by default if no one is specified when configuring the **undo ospf** command.
- The process ID must be consistent in the same area; otherwise, insulation between processes will be resulted.
- If multiple OSPF processes run on a router, you are recommended to specify different router IDs for different processes with the **router-id** command.
- Binding an OSPF with a VPN with the **vpn-instance** command is available in MPLS VPN application. See the VPN part.

4.2.3 Entering the OSPF Area View

OSPF divides an AS into smaller areas and assigns routers to different groups logically.

Perform the following configuration in OSPF view.

Table 4-3 Enter the OSPF area view

Operation	Command
Enter the OSPF area view	**area** *area-id*
Delete a designated OSPF area	**undo area** *area-id*

Area ID can be input in decimal integers or in IP address format, but only output as IP address.

Take the area as whole in configuring parameters for the OSPF routers in the same area, otherwise information exchange may fail between adjacent routers, or routing information may be blocked or routing loops may be generated.

4.2.4 Specifying a Network Segment to Run OSPF

After enabling OSPF in system view, you must specify on which network segment OSPF should be applied.

Perform the following configuration in OSPF area view.

Table 4-4 Specify a network segment to run OSPF

Operation	Command
Specify a network segment to run OSPF	**network** *ip-address wildcard-mask*
Disable OSPF on the network segment.	**undo network** *ip-address wildcard-mask*

You may assign a router (an ABR) but not a network segment to multiple areas.

4.2.5 Configuring OSPF Virtual Links

OSPF stipulates that all non-backbone areas should maintain connectivity with the backbone area. That is, at least one interface on the ABR should fall into the area 0.0.0.0. If an area does not have a direct physical link to the backbone area 0.0.0.0, a virtual link must be created.

Virtual links are logic channels set up through the area of a non-backbone internal route between two ABRs. Both ends of a logic channel should be ABRs and the connection can take effect only when both ends are configured. A virtual link is identified by the ID of the remote router. Transit area provides the ends of the virtual link with a non-backbone area internal route.

The virtual link is activated after the route passing through the transit area is calculated, which is equivalent to a **p2p** connection between two ends. Therefore, similar to the physical interfaces, you can also configure various interface parameters on this link, such as hello timer.

The "logic channel" means that the multiple routers running OSPF between two ABRs only take the role of packet forwarding (the destination addresses of the protocol packets are not these routers, so these packets are transparent for them and the routers forward them as common IP packets). The routing information is directly transmitted between the two ABRs. The routing information herein refers to the type-3 LSAs generated by the ABRs, for which the synchronization mode of the routers in the area will not be changed.

Perform the following configuration in OSPF area view.

Table 4-5 Configure a OSPF virtual link

Operation	Command
Create and configure a virtual link	**vlink-peer** *router-id* [**hello** *seconds*] [**retransmit** *seconds*] [**trans-delay** *seconds*] [**dead** *seconds*] [**simple** *password* **|** **md5** *keyid key*]
Remove the created virtual link	**undo vlink-peer** *router-id*

By default, hello timer is set to 10 seconds, retransmit to 5 seconds, trans-delay to 1 second, and dead interval to 40 seconds.

4.2.6 Configuring the Network Type of an OSPF Interface

The route calculation of OSPF is based upon the topology of the adjacent network of the local router. Each router describes the topology of its adjacent network and transmits it to all the other routers.

OSPF divides networks into four types by link layer protocol:

- Broadcast: If Ethernet or FDDI is adopted, OSFP defaults the network type to broadcast.
- Non-Broadcast Multi-access (**NBMA**): If Frame Relay, ATM, HDLC or X.25 is adopted as a link layer protocol, OSPF defaults the network type to NBMA.
- Point-to-Multipoint (**p2mp**): No link layer protocol is regarded to be **p2mp** by default. A **p2mp** network must be compulsorily changed from other network types. The common practice is to change a non fully-matched NBMA into a **p2mp** network.
- Point-to-point (**p2p**): When the link layer protocol is PPP or LAPB, the default network type of OSPF is **p2p**.

NBMA network refers to a non-broadcast and multi-accessible network. ATM is a typical example for it. The period for sending a polling hello packet before a router forms neighboring relationship with its peer router can be specified by configuring the polling interval.

On a broadcast network, which has no multi-access capability, an interface can be configured into **NBMA**.

Configure the interface type to **p2mp** if not all the routers are directly accessible on an NBMA network.

Change the interface type to **p2p** if the router has only one peer on the NBMA network.

Differences between **NBMA** and **p2mp**:

- In OSPF, NBMA refers to a network that is fully matched, non-broadcast and multi-accessible. While a **p2mp** network is unnecessarily fully matched.
- On a NBMA network, it is necessary to elect DR and BDR; while a **p2mp** network has no DR and BDR.
- NBMA is the default network type. For example, if ATM is adopted as the link layer protocol, OSPF defaults the network type on the interface to NBMA, regardless of whether the network is fully connected. In contrast, **p2mp** is not a default network type. No link layer protocol is regarded as **p2mp** by default. A **p2mp** network must be compulsorily changed from other networks types. The common practice is to change a non fully-matched NBMA into a **p2mp** network.
- NBMA forwards packets by unicast and neighbors shall be configured manually. While **p2mp** forwards packets by multicast.

Perform the following configuration in interface view.

Table 4-6 Configure the network type of an OSPF interface

Operation	Command
Configure the network type of an OSPF interface	**ospf network-type** { **broadcast** | **nbma** | **p2mp** | **p2p** }

By default, OSPF identifies network type by looking at link layer type. After you specify a network type for the interface, the original network type is removed automatically.

4.2.7 Configuring the Adjacent Point

For an NBMA network, OSPF router cannot discover adjacent routers through broadcasting Hello packets; you must manually assign an IP address to the adjacent router and specify whether the adjacent router is eligible for election.

Perform the following configuration in OSPF view.

Table 4-7 Configure the adjacent point

Operation	Command
Configure a peer for the NBMA interface	**peer** *ip-address* [**dr-priority** *dr-priority-number*]
Remove the configured peer for the NBMA interface	**undo peer** *ip-address*

By default, the preference for the neighbor of NBMA interface is 1.

The preference levels set with the **ospf dr-priority** command and the **peer** command are used in different purpose:

- The preference levels set with the **ospf dr-priority** command are for real DR election.
- The preference levels set with the **peer** command indicate if the neighbors are authorized to elect. The preference level 0 means the neighbor is not authorized and no hello messages are sent to the neighbor. This is an effective way to reduce hello packet number in electing DR and BDR. But if the local router is DR or BDR, it will still send hello messages to its neighbor with preference level 0, to set up adjacency relation.

4.2.8 Configuring OSPF to Redistribute Routes

I. Redistributing routes of other protocols

The dynamic routing protocols on the router can share the routing information. As far as OSPF is concerned, the routes discovered by other routing protocols are always processed as the external routes of AS. In the **import-route** commands, you can specify the type of route cost, cost and tag to overwrite the default route receiving parameters (refer to "Configure Parameters for OSPF to Redistribute External Routes").

The OSPF uses the following four types of routes (sequencing in priority):

- Intra-area route
- Inter-area route

- External route type 1
- External route type 2

Intra-area and inter-area routes describe the internal AS topology whereas the external routes describe how to select the route to the destinations beyond the AS.

The external routes type-1 refers to the redistributed IGP routes (such as static route and RIP). Since these routes are more reliable, the calculated cost of the external routes is the same as the cost of routes within the AS. Also, such route cost and the route cost of the OSPF itself are comparable. That is, cost to reach the external route type 1 = cost to reach the corresponding ASBR from the local router + cost to reach the destination address of the route from the ASBR.

The external routes type-2 refers to the redistributed EGP routes. Since these routes have lower credibility, OSPF assumes that the cost spent from the ASBR to reach the destinations beyond the AS is greatly higher than that spent from within the AS to the ASBR. So in route cost calculation, the former is mainly considered, that is, the cost spent to reach the external route type 2 = cost spent to the destination address of the route from the ASBR. If the two values are equal, then the cost of the router to the corresponding ASBR will be considered.

Perform the following configuration in OSPF view.

Table 4-8 Configure OSPF to redistribute routes of other protocols

Operation	Command
Configure OSPF to redistribute routes of other protocols	**import-route** *protocol* [**allow-ibgp]** [**cost** *value*] [**type** { **1** | **2** }] [**tag** *value*] [**route-policy** *route-policy-name*]
Cancel redistributing routing information of other protocols	**undo import-route** *protocol*

By default, OSPF does not redistribute the routing information of other protocols. For redistributed routes, cost is 1, type is 2, and tag is 1 by default.

When the *protocol* argument is set to BGP, the keyword **allow-ibgp** is optional. Whereas the **import-route bgp** command redistributes only EBGP routes, the **import-route bgp allow-ibgp** command redistributes IBGP routes in addition and as such, must be used with cautions.

The *protocol* specifies a source routing protocol that can be redistributed. By far, it can be Direct, Static, RIP, IS-IS or BGP.

II. Configuring parameters for OSPF to redistribute external routes

In the case that OSPF redistributes routing information found by other routing protocols to the local AS, it is also necessary to configure some extra parameters, such as default cost and default tag for route redistribution. A route label can be used to identify relevant protocol information, such as the number used to distinguish different ASs when OSPF receives BGP.

Perform the following configuration in OSPF view.

Table 4-9 Configure parameters for OSPF to redistribute external routes

Operation	Command
Configure the minimum interval for OSPF to redistribute the external routes	**default interval** *seconds*
Restore the default value of the minimum interval for OSPF to redistribute the external routes	**undo default interval**
Configure upper limit for OSPF to redistribute routes each time	**default limit** *routes*
Restore the default upper limit for OSPF to redistribute routes each time	**undo default limit**
Configure the default cost for OSPF to receive external routes	**default cost** *value*
Restore the default cost for OSPF to receive external routes	**undo default cost**
Configure the default tag when OSPF receives external routes	**default tag** *tag*
Restore the default tag when OSPF receives external routes	**undo default tag**
Configure the default type of external routes that OSPF will redistribute	**default type** { **1** | **2** }
Restore the default type of the external routes redistributed by OSPF	**undo default type**

By default, cost is 1, type is 2, and tag is 1 for redistributed routes; route redistribution interval is 1 second; the upper limit to the external routes redistributed is 1000 per second.

4.2.9 Configuring OSPF to Create the Default Route

By default, no default route is configured for general OSPF areas (backbone area and non-backbone areas), and you cannot redistribute default route into OSPF routing domain by using the **import-route** command.

You can use the **default-route-advertise** command to generate and advertise a default route in OSPF area. You need to care for these points in this process:

- Using the **default-route-advertise** command at ASBR or ABR in general OSPF area, you can generate a default route which is advertised by the Type-5 LSA into OSPF area.

- Using the **default-route-advertise** command at ASBR or ABR in NSSA, you can generate a default route which is advertised by the Type-7 LSA into NSSA.
- This command is absolutely ineffective to Stub area and totally stub area.
- For an ASBR, only when the routing table contains a default route, can OSPF generate the corresponding Type-5 LSA or Type-7 LSA.
- For an ABR, the Type-5 LSA or Type-7 LSA will be generated no matter whether there is a default route in the routing table.
- The Type-5 LSA or Type-7 LSA which advertises the default route has the same spread range as the general Type-5 LSA or Type-7 LSA.

Perform the following configuration in OSPF view.

Table 4-10 Create a default route in an OSPF routing domain

Operation	Command
Create a default route	**default-route-advertise** [**always**] [cost *value*] [**type** *value*] [**route-policy** *route-policy-name*]
Remove the default route	**undo default-route-advertise** [**always**] [**cost**] [**type**] [**route-policy**]

By default, no default route is configured in OSPF areas.

If the **always** keyword is selected in using the command, the Type-5 LSA or Type-7 LSA will be generated no matter whether there is a default route in the routing table. Note that this keyword is only available for ASBR and care should be taken in using it.

As OSPF does not count the LSAs it generates in SPF calculation, no default route is available among OSPF routes. To ensure the correctness of routing information, you should configure default route redistribution only those routers connected to external networks.

Note:

An OSPF router after the **default-route-advertise** command is executed will become an ASBR, as is similar to executing the **import-route** command on an OSPF router. For the ABR or ASBR in NSSA, the **default-route-advertise** command is equivalent to the **nssa default-route-advertise** command in terms of effect.

4.2.10 Configuring OSPF Route Filtering

Perform the following configuration in OSPF view.

I. Configuring OSPF to filter received routes

After OSPF receives LSAs, it may decide based on certain filtering conditions whether to add the computed routes to the routing table. The routes filtered out do not appear in the local routing table.

Table 4-11 Configure OSPF to filter the redistributed routes

Operation	Command
Configure OSPF to filter received global routing information	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **gateway** *prefix-list-name* } **import**
Disable OSPF to filter received global routing information	**undo filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **gateway** *ip-prefix-name* } **import**

Note:

The **filter-policy import** command only filters the OSPF routes of this process received from neighbors. Even though it blocks routing information from being added to the routing table, it does not prevent the corresponding LSAs from being advertised. This command only takes effect on ASBRs.

II. Configuring OSPF to filter redistributed routes

The **filter-policy export** command is configured on an ASBR to filter the redistributed external routes of OSPF, that is, to filter the LSAs of redistributed routes to be advertised. The routes filtered out are not to be advertised as Type-5 LSAs. This command is available on ASBRs only.

Table 4-12 Configure OSPF to filter redistributed routes

Operation	Command
Enable OSPF to filter the LSAs of redistributed routes for advertisement	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*routing-process*]
Disable OSPF to filter the LSAs of redistributed routes for advertisement	**undo filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*routing-process*]

By default, OSPF does not filter redistributed or advertised routing information.

📖 **Note:**

- The **filter-policy import** command only filters the OSPF routes of this process received from the neighbors, and routes that cannot pass the filter are not to be added to the routing table. This command only takes effect on ASBRs.
- The **filter-policy export** command takes effect only on the routes redistributed using the **import-route** command. If you do not configure the **import-route** command to redistribute external routes (including OSPF routes of different processes), then the configured **filter-policy export** command does not take effect. This is because OSPF advertises routing information by sending LSAs rather than routing tables.
- If no routing protocol is specified, the **filter-policy export** command applies to all redistributed routes specified using the **import-route** command.

4.2.11 Configuring Route Aggregation by OSPF

I. Configuring the Route Aggregation of OSPF Area

Route aggregation means that ABR can aggregate information of the routes of the same prefix and advertise only one route to other areas. An area can be configured with multiple aggregate segments, thereby OSPF can summarize them. When the ABR transmits routing information to other areas, it will generate Sum_net_Lsa (type-3 LSA) per network. If some continuous segments exist in this area, you can use the **abr-summary** command to summarize these segments into one segment. In this way, ABR only sends an LSA after aggregation. No LSA that falls into the specified aggregation network segment of this command will be separately transmitted. The LSDB scale in other areas is accordingly reduced.

Once the aggregate segment of a certain network is added to the area, all the internal routes of the IP addresses in the range of the aggregate segment will no longer be separately broadcast to other areas. If the keyword **not-advertise** is used to qualify the network segment, the summary route information to the network segment will not be broadcast. This network segment is defined by IP address/mask.

Note: Only when configured on ABR can route aggregation take effect.

Perform the following configuration in OSPF area view.

Table 4-13 Configure the route aggregation in OSPF area

Operation	Command
Configure the route aggregation in OSPF area	**abr-summary** *ip-address mask* [**advertise** | **not-advertise**]
Cancel route aggregation in OSPF area	**undo abr-summary** *ip-address mask*

By default, the inter-area routes will not be aggregated.

II. Configuring aggregation of redistributed routes by OSPF

OSPF supports route aggregation of redistributed routes.

Perform the following configuration in OSPF view.

Table 4-14 Configure aggregation of redistributed routes by OSPF

Operation	Command
Configure aggregation of redistributed routes by OSPF	**asbr-summary** *ip-address mask* [**not-advertise** | **tag** *value*]
Remove aggregation of redistributed routes by OSPF	**undo asbr-summary** *ip-address mask*

By default, aggregation of redistributed routes is disabled; if it is enabled, aggregate distributed routes are advertised with the tag of 1.

After the aggregation of redistributed routes is configured, if the local router is an autonomous system border router (ASBR), this command aggregates the redistributed Type-5 LSAs in the aggregation address range. When NSSA is configured, this command will also aggregate the redistributed Type-7 LSA in the aggregation address range.

If the local router works as an area border router (ABR) and a transit router in the NSSA, this command aggregates Type-5 LSAs transformed from Type-7 LSAs. If the router is not the router in the NSSA, the aggregation is disabled.

4.2.12 Setting OSPF Route Preference

Since maybe multiple dynamic routing protocols are run on one router concurrently, the problem of route sharing and selection between various routing protocols occurs. The system sets a priority for each routing protocol, which will be used in tie-breaking in the case that different protocols discover the same route.

Perform the following configuration in OSPF view.

Table 4-15 Set OSPF route preference

Operation	Command
Configure a preference for OSPF to compare with the other routing protocols	**preference** [**ase**] *preference*
Restore the default protocol preference	**undo preference** [**ase**]

By default, the OSPF preference is 10, and the redistributed external routing protocol is 150.

4.2.13 Configuring OSPF Timers

I. Setting the interval of Hello packet transmission

Hello packets are a kind of most frequently used packets, which are periodically sent to the adjacent router for discovering and maintaining the adjacency, and for electing DR and BDR. The user can set the value of "*seconds*", the interval for sending a hello packet.

According to provisions in RFC2328, it is necessary to keep consistency of the hello timer between network neighbors. Note that the value of hello timer is inversely proportional to route convergence speed and network load.

Perform the following configuration in interface view.

Table 4-16 Set the interval of hello packet transmission

Operation	Command
Set the hello interval of the interface	**ospf timer hello** *seconds*
Restore the default hello of the interface	**undo ospf timer hello**
Set the poll interval on the NBMA interface	**ospf timer poll** *seconds*
Restore the default poll interval	**undo ospf timer poll**

By default, **p2p** and **broadcast** interfaces send Hello packets every 10 seconds; while **p2mp** and **NBMA** interfaces send Hello packets every 30 seconds.

By default, poll timer is 40 seconds.

You are recommended to set the poll timer longer than the hello timer.

II. Setting dead time for the neighboring routers

If a router receives no hello packet from its neighbor in a certain time, the neighbor router is regarded invalid. This time interval is called dead time between neighboring routers.

Perform the following configuration in interface view.

Table 4-17 Set dead time for the neighboring routers

Operation	Command
Configure a dead timer for the neighboring routers	**ospf timer dead** *seconds*
Restore the default dead interval of the neighboring routers	**undo ospf timer dead**

By default, the dead interval for the neighboring routers of **p2p** or broadcast interfaces is 40 seconds and that for the neighboring routers of **p2mp** or **NBMA** interface is 120 seconds.

Note that both hello and dead timer will restore to the default values after the user modify the network type.

III. Setting an interval for LSA retransmission between neighboring routers

After a router sends an LSA to its neighbor, it waits for the acknowledgement packet from its neighbor. If it receives no acknowledgement packet from its neighbor, it will retransmit the LSA. The user can set the value of retransmit.

Perform the following configuration in interface view.

Table 4-18 Set the interval for LSA retransmission between neighboring routers

Operation	Command
Configure the interval of LSA retransmission for the neighboring routers	**ospf timer retransmit** *interval*
Restore the default LSA retransmission interval for the neighboring routers	**undo ospf timer retransmit**

By default, the interval for neighboring routers to retransmit LSAs is 5 seconds.

The value of *interval* must be greater than the time for a packet to be transmitted a round between two routers.

Note that you should not set the LSA retransmission interval too small. Otherwise, unnecessary retransmission will be caused.

4.2.14 Setting the Interface Priority for DR Election

Designated router (DR) and backup designated router (BDR) should be elected in broadcast network or NBMA network.

The priority of the router interface determines the qualification of the interface in DR election, and the router with priority 0 cannot be elected as a DR or BDR.

DR is elected by all the routers on the segment. Routers with the priorities greater than 0 in the network are eligible "candidates". Among all the routers self-proclaimed to be the DR, the one with the highest priority will be elected. If two routers have the same priority, the one with the highest router ID will be elected as the DR. Votes are the hello packets. Each router writes the elected DR in the packet and sends it to all the other routers on the segment. If two routers attached to the same segment concurrently declare themselves to be the DR, choose the one with higher priority. If their priorities are equal, the one with greater router ID will be preferred. A router, whose priority is 0, cannot be elected as a DR or BDR.

If a DR becomes invalid due to some fault, it must be reelected from routers on the network and synchronized with other routers. It takes time and meanwhile the route calculation is incorrect. In order to speed up this process, the concept of BDR is instilled in OSPF. In fact, BDR is a backup for DR. DR and BDR are elected in the mean time. The adjacencies are also established between the BDR and all the routers on the segment, and routing information is also exchanged between them. When the DR fails, the BDR will become the DR instantly. Since no re-election is needed and the adjacencies have already been established, the process is very short. But in this case, a new BDR should be elected. Although it will also take a quite long period of time, it will not exert any influence upon the route calculation.

But please note:

- When the precedence of an interface is 0, the interface cannot be a DR/BDR anyway, which may result in a network without DR or BDR.
- The DR on the network is not necessarily the router with the highest priority. Likewise, the BDR is not necessarily the router with the second highest priority. If a new router is added after DR and BDR election, it is impossible for the router to become the DR even if it has the highest priority.
- A DR is on a certain network segment, in the sense of router interface. Maybe a router is a DR on one interface, but can be a BDR or DR Other on the other interface.
- Only when an interface is of broadcast or NBMA type, is it necessary to elect DR. A **p2mp** or a **p2p** interface needs not to elect DR. On a broadcast network or NBMA network, if no one declares that it is DR in the hello packets received, the election process starts; if multiple routes declare that they are the DR/BDR, the election process also starts; if a router declares that it is the DR/BDR, new-added routers will accept the existing DR/BDR without considering about its precedence; when the DR fails, the BDR will become the DR, a new BDR will be elected.

Perform the following configuration in interface view.

Table 4-19 Set the interface priority for DR election

Operation	Command
Configure the interface with a priority for DR election	**ospf dr-priority** *priority_num*
Restore the default interface priority	**undo ospf dr-priority**

By default, the priority of the Interface is 1 in the DR election. The value can be taken from 0 to 255.

4.2.15 Configuring the Cost for Sending Packets on an Interface

You may configure the cost for sending packets on interfaces to interfere route calculation.

Perform the following configuration in interface view.

Table 4-20 Configure the cost for sending packets on an interface

Operation	Command
Configure the cost for sending packets on an interface	**ospf cost** *value*
Restore the default cost for packet transmission on the interface	**undo ospf cost**

By default, OSPF calculates the cost for sending packets according to the interface rate.

4.2.16 Setting a Shortest Path First (SPF) Calculation Interval for OSPF

Whenever the LSDB of OSPF changes, the shortest path should be recalculated. Calculating the shortest path upon change will consume enormous resources as well as affect the operation efficiency of the router. Adjusting the SPF calculation interval, however, can restrain the resource consumption due to frequent network changes.

Perform the following configuration in OSPF view.

Table 4-21 Set the SPF calculation interval

Operation	Command
Set the SPF calculation interval	**spf-schedule-interval** *seconds*
Restore the SPF calculation interval	**undo spf-schedule-interval** *seconds*

By default, the interval of SPF recalculation is 5 seconds.

4.2.17 Configuring an Interval Required for Sending LSU Packets

Transmitting-delay should be added to the aging time of the LSA in an LSU packet. Setting the parameter like this mainly considers the time duration that the interface requires for transmitting the packet.

The user can configure the interval of sending LSU packets. Obviously, more attention should be paid on this item over low speed network.

Perform the following configuration in interface view.

Table 4-22 Configure the interval for sending LSU packets

Operation	Command
Configure the interval for sending LSU packets	**ospf trans-delay** *seconds*
Restore the default interval of sending LSU packets	**undo ospf trans-delay**

By default, the LSU packets are transmitted per second.

4.2.18 Configuring if Filling in the MTU Field When Transmitting DD Packets

OSPF-running routers use the DD (Database Description) packets to describe their own LSDBs when synchronizing the databases.

You can manually specify an interface to fill in the MTU field in a DD packet when it transmits the packet. The MTU should be set to the real MTU on the interface.

Perform the following configuration in the Ethernet interface view.

Table 4-23 Configure if filling in the MTU field when transmitting DD packets

Operation	Command
Enable an interface to fill in the MTU field when transmitting DD packets	**ospf mtu-enable**
Disable the interface to fill in MTU when transmitting DD packets	**undo ospf mtu-enable**

By default, the interface does not fill in the MTU field when transmitting DD packets. In other words, the MTU field in the DD packets is 0.

4.2.19 Configuring Maximum Number of Equal-Cost Routes

Perform the following configuration in OSPF view.

Table 4-24 Configure maximum number of OSPF equal-cost routes

Operation	Command
Configure maximum number of OSPF equal-cost routes	**multi-path-number** *number*
Restore the default maximum number of OSPF equal-cost routes	**undo multi-path-number**

The default maximum number of OSPF equal-cost routes is 8.

4.2.20 Configuring OSPF Authentication

I. Configuring the OSPF area to support packet authentication

OSPF requires that all routers in the same area must use the same authentication mode, whether it is none, simple, or MD5; the passwords used by links could be different however.

Use the **authentication-mode simple** command to configure plain text authentication password in the area. Use the **authentication-mode md5** command to configure MD5 encrypted authentication password in the area.

Perform the following configuration in OSPF area view.

Table 4-25 Configure the OSPF area to support packet authentication

Operation	Command
Configure the area to support MD5 authentication	**authentication-mode** { **simple** | **md5** }
Disable the area to support MD5 authentication attributes	**undo authentication-mode**

By default, the area does not support packet authentication.

II. Configuring OSPF packet authentication

OSPF supports plain text authentication or MD5 authentication between neighboring routers.

Perform the following configuration in the Ethernet interface view.

Table 4-26 Configure OSPF Packet Authentication

Operation	Command
Specify a password for OSPF simple text authentication	**ospf authentication-mode simple** *password*
Cancel plain text authentication on the interface	**undo ospf authentication-mode simple**
Specify the key-id and key for OSPF MD5 authentication	**ospf authentication-mode md5** *key_id key*
Cancel MD5 authentication on the interface	**undo ospf authentication-mode md5**

By default, the interface is not configured with either plain text authentication or MD5 authentication.

4.2.21 Disabling the Interface to Send OSPF Packets

To prevent OSPF routing information from being acquired by the routers on a certain network, use the **silent-interface** command to disable the interface to transmit OSPF packets.

Different processes can disable the same interface to forward OSPF packet; while the **silent-interface** command is only valid for the OSPF interface where the specified process has been enabled, with no effect to the interface with other processes.

Perform the following configuration in OSPF view.

Table 4-27 Enable the interface to send IS-IS packets

Operation	Command
Disable the interface from sending OSPF packets	**silent-interface** *interface-type* interface-*number*
Enable the interface to send OSPF packets	**undo silent-interface interface-type interface-number**

By default, all the interfaces are allowed to transmit and receive OSPF packets.

After an OSPF interface is set to be in silent status, the interface can still advertise its direct route. However, the OSPF hello packets of the interface will be blocked, and no neighboring relationship can be established on the interface. Thereby, the capability for OSPF to adapt to the networking can be enhanced, which will hence reduce the consumption of system resources.

4.2.22 Configuring OSPF STUB Area

The Stub area, a type of OSPF area, does not receive or advertise Type-5 LSAs. The Stub area is often at the AS border and can effectively minimize the LSDB size of the routers in the Stub area and lower resource occupation for SPF calculation.

To ensure correct forwarding of the packets from the Stub area to the external network, the ABR in the Stub area advertises a default route through the Tyep-3 LSAs and only within this area.

📖 **Note:**

The ABR advertises inter-area default routes through Type-3 LSA.

Please pay attention to the following items when configuring a STUB area:

- The backbone area cannot be configured to be the STUB area.
- The virtual link cannot pass through the STUB area.
- If you want to configure an area to be the STUB area, then all the routers in this area should be configured with this attribute.
- ASBR cannot exist in a STUB area. In other words, routes outside an AS cannot be transmitted in the local area.

Perform the following configuration in OSPF area view.

Table 4-28 Configure OSPF STUB area

Operation	Command
Configure an area to be the STUB area	**stub** [**no-summary**]
Remove the configured STUB area	**undo stub**
Configure the cost of the default route transmitted by OSPF to the STUB area	**default-cost** *value*
Remove the cost of the default route to the STUB area	**undo default-cost**

By default, the STUB area is not configured, and the cost of the default route to the STUB area is 1.

Note that the **no-summary** parameter is only available for the ABR. When it is used for the ABR in the Stub area, the ABR only advertises in the area a Summary-LSA of the default route, not others. Since this kind of Stub area has no AS-external-LSAs or Summary-LSAs, it is also called totally stub area.

The **default-cost** parameter is for the ABR in the Stub area and defines the cost value for the default route advertised by the ABR to the Stub area.

4.2.23 Configuring NSSA Parameters of OSPF

RFC1587 (OSPF NSSA Option) defines the Not-So-Stubby-Area (NSSA), which keeps the strong points of Stub area while providing flexible networking. This area can redistribute AS external routes in a limited way.

NSSA is, in fact, the expansion of the Stub area, so it resembles the Stub area in many ways. These points should be cared for in configuring an NSSA:

- The backbone area cannot be configured as NSSA.
- NSSA cannot serve as transit area, that is, a viral link cannot be set up across an NSSA.
- All routers in an NSSA must be configured with the corresponding attribute.

Unlikely the Stub area, an NSSA area may contain ASBRs.

Type-7 LSAs, which are similar to Type-5 LSAs, are used for the AS external route information in the NSSA. For more details about these two types, see “4.1.5 LSA Types Available in OSPF”.

The advertisement of AS external route information in NSSA is illustrated in Figure 4-4 NSSA, where three areas are included in the OSPF process 100: area 0 is backbone area; area 1 is non-backbone area; area 2 is NSSA.

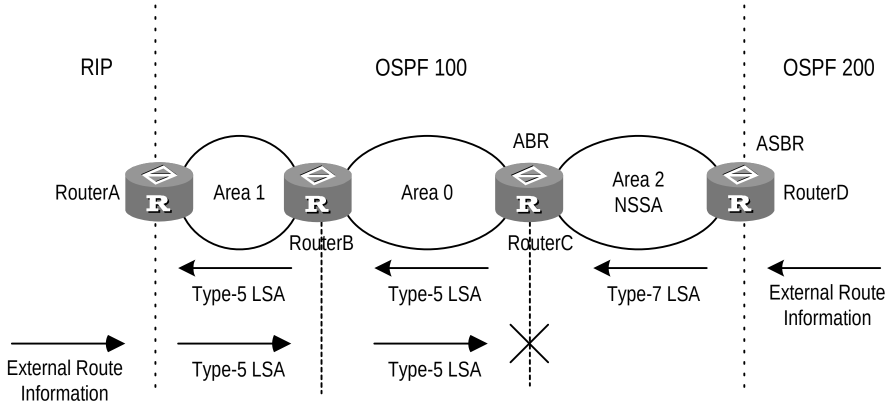


Figure 4-4 NSSA

The ASBR in the area 2 redistributes AS external route information (the route information of OSPF process 200) to generateType-7 LSAs and advertises them in the area 2. When the Type-7 LSAs reach the NSSA ABR, they are converted into Type-5 LSAs which are advertised among the entire AS. The ASBR in the area 1 redistributes AS external route information (the RIP route information) to generate Type-5 LSAs, which are advertised among the OSPF AS. The RIP route information cannot arrive at the area 2, the NSSA.

Perform the following configuration in OSPF area view.

Table 4-29 Configure NSSA area parameters of OSPF

Operation	Command
Configure an area to be an NSSA area	**nssa** [**default-route-advertise**] [**no-import-route**] [**no-summary**]
Remove a configured NSSA area	**undo nssa**
Configure the cost for transmitting the default route to NSSA area	**default-cost** *cost*
Restore the default cost for transmitting the default route to NSSA area	**undo default-cost**

By default, the NSSA is not configured, and the cost of the default route to the NSSA is 1.

If the ASBR is also the ABR in NSSA, you are often not recommended to redistribute AS external route information twice respectively as Type-5 LSAs and Type-7 LSAs. Then you can select the **no-import-route** parameter to forbid AS external route information being advertised to the NSSA as Type-7 LSAs.

Since the NSSA gets limited AS external route information, so the ABR in it need to advertise a default route via the Type-7 LSAs to ensure correct forwarding of packets to the networks outside the AS. The default route information from the NSSA ABR will not be converted into Type-5 LSAs, while that from the NSSA ASBR will be converted.

The **default-route-advertise** parameter, which is only available for NSSA ASBR or ABR, is used to generate Type-7 LSAs for the default route.

- When using the parameter at NSSA ABR, you can generate Type-7 LSAs for the default route no matter whether there exists the default route 0.0.0.0 in the routing table.
- When using the parameter at NSSA ASBR, you can generate Type-7 LSAs for the default route only if there exists the default route 0.0.0.0 in the routing table.

The **no-summary** parameter is only available for the ABR in NSSA, as is the same as in stub area. When the parameter is selected, the NSSA ABR advertises a default route via the Summary-LSAs (Type-3) in the area, but no other Summary-LSAs to other areas.

Note:

The **default-route-advertise** parameter generates AS external default route which is advertised in the NSSA via the Type-7 LSAs.
The **no-summary** parameter generates inter-area default route which is advertised via the Type-3 LSAs.

The **default-cost** parameter, which is only available for the NSSA ABR, defines the cost value for the default route advertised by the ABR to the NSSA.

4.2.24 Enabling Opaque Capacity of OSPF

Enable the opaque capacity of OSPF before implementing OSPF TE.

Perform the following configuration in OSPF view.

Table 4-30 Enable Opaque capacity of OSPF

Operation	Command
Enable Opaque capacity of OSPF	**opaque-capability enable**
Disable Opaque capacity of OSPF	**undo opaque-capability**

⚠ **Caution:**

If OSPF TE has been enabled in an area, then the **undo opaque-capability** command will fail in this area.

4.2.25 Configuring OSPF in Concert with Network Management System

I. Configuring OSPF MIB binding

When multiple OSPF processes are enabled, you can configure OSPF MIB to opt for the process under processing. In other words, you can configure which process OSPF MIB is to be bound with.

Perform the following configuration in system view.

Table 4-31 Configure OSPF MIB binding

Operation	Command
Configure OSPF MIB binding	**ospf mib-binding** *process-id*
Remove the default OSPF MIB binding	**undo ospf mib-binding**

By default, MIB is bound with the first enabled OSPF process.

II. Configuring OSPF TRAP

OSPF can be configured to forward diversified SNMP TRAP packets and a certain OSPF process can be specified via process number to send SNMP TRAP packets.

Perform the following configuration in system view.

Table 4-32 Configure OSPF TRAP

Operation	Command
Enable OSPF TRAP	**snmp-agent trap enable ospf** [*process-id*] [**ifstatechange** | **virifstatechange** | **nbrstatechange** | **virnbrstatechange** | **ifcfgerror** | **virifcfgerror** | **ifauthfail** | **virifauthfail** | **ifrxbadpkt** | **virifrxbadpkt** | **txretransmit** | **viriftxretransmit** | **originatelsa** | **maxagelsa** | **lsdboverflow** | **lsdbapproachoverflow**]
Disable OSPF TRAP	**undo snmp-agent trap enable ospf** [*process-id*] [**ifstatechange** | **virifstatechange** | **nbrstatechange** | **virnbrstatechange** | **ifcfgerror** | **virifcfgerror** | **ifauthfail** | **virifauthfail** | **ifrxbadpkt** | **virifrxbadpkt** | **txretransmit** | **viriftxretransmit** | **originatelsa** | **maxagelsa** | **lsdboverflow** | **lsdbapproachoverflow**]

By default, OSPF TRAP is disabled, that is, OSPF process does not forward TRAP packets. If the process number is not specified during configuration, OSPF TRAP configuration will be valid for all OSPF processes.

For detailed configuration about SNMP TRAP, refer to the module about “System Management” of this manual.

4.2.26 Resetting an OSPF process

If the **undo ospf** command is executed on a router and then the **ospf** command is used to reset an OSPF process, the previous OSPF configuration will be lost. With the **reset ospf all** command, you can reset the OSPF process without losing the previous OSPF configuration.

Perform the following configuration in user view.

Table 4-33 Reset an OSPF process

Operation	Command
Reset an OSPF process	**reset ospf** [**statistics**] { **all** | *process-id* }

Resetting the OSPF process can immediately clear the invalid LSAs, make the modified Router ID immediately effective or re-elect the DR and BDR.

If the process number is not specified, all OSPF processes will be reset.

4.3 Displaying and Debugging OSPF

After the above configuration, execute **display** command in all views to display the running of the OSPF configuration, and to verify the effect of the configuration. Execute **debugging** command in user view to debug the OSPF module.

Table 4-34 Display and debug OSPF

Operation	Command
Display the summary of OSPF redistributed routes	**display ospf** [*process-id*] **asbr-summary** [*ip-address mask*]
Display the brief information of the OSPF routing process	**display ospf** [*process-id*] **brief**
Display OSPF statistics	**display ospf** [*process-id*] **cumulative**
Display LSDB information of OSPF	**display ospf** [*process-id*] **lsdb** [**brief**] [**asbr** | **ase** | **network** | **nssa** | **router** | **summary**] [*ip-address*] [**originate-router** *ip-address*] [**self-originate**]
Display OSPF neighbor information	**display ospf** [*process-id*] **peer** [**brief**]
Display OSPF next hop information	**display ospf** [*process-id*] **nexthop**
Display OSPF routing table	**display ospf** [*process-id*] **routing**
Display OSPF virtual links	**display ospf** [*process-id*] **vlink**
Display OSPF request list	**display ospf** [*process-id*] **request-queue**
Display OSPF retransmission list	**display ospf** [*process-id*] **retrans-queue**
Display the OSPF routing information to ABR and ASBR	**display ospf** [*process-id*] **abr-asbr**
Display OSPF interface information	**display ospf** [*process-id*] **interface**
Display OSPF errors	**display ospf** [*process-id*] **error**
Display the debugging of OSPF process	**display debugging ospf**
Enable the system to output state changes of the peer for the current OSPF process (in OSPF view)	**log-peer-change**
Disable the system to output state changes of the peer for the current OSPF process (in OSPF view)	**undo log-peer-change**
Enable the debugging of OSPF packet	**debugging ospf packet** [**ack** | **dd** | **hello** | **interface** *type num* | **request** l **update**]
Disable the debugging of OSPF packet	**undo debugging ospf packet** [**ack** | **dd** | **hello** | **interface** *type num* | **request** l **update**]
Enable the debugging of OSPF event	**debugging ospf event**
Disable the debugging of OSPF event	**undo debugging ospf event**
Enable the debugging of OSPF LSA packet	**debugging ospf lsa**

Operation	Command
Disable the debugging of OSPF LSA packet	**undo debugging ospf lsa**
Enable OSPF SPF debugging	**debugging ospf spf**
Disable OSPF SPF debugging	**undo debugging ospf spf**

4.4 OSPF Configuration Example

⚠ **Caution:**

In configuration examples, only the commands related to the OSPF configuration are listed.

4.4.1 OSPF Configuration Example

I. Network requirements

RouterA and RouterB are connected by serial interfaces, and RouterB and RouterC are connected by Ethernet interfaces. RouterA belongs to area0, RouterC belongs to area1, and RouterB belongs to both area0 and area1.

II. Network diagram

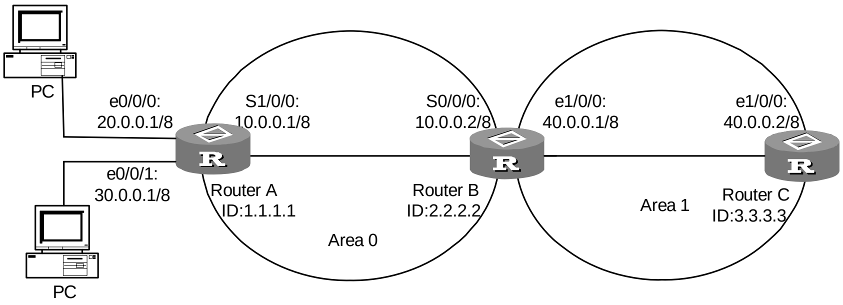


Figure 4-5 Configure OSPF

III. Configuration procedure

# Configure Router A:

```
[RouterA] router id 1.1.1.1
[RouterA] interface serial1/0/0
```

```
[RouterA-serial1/0/0] ip address 10.0.0.1 255.0.0.0
[RouterA-serial1/0/0] interface ethernet0/0/0
[RouterA-ethernet 0/0/0] ip address 20.0.0.1 255.0.0.0
[RouterA- ethernet 0/0/0] interface ethernet0/0/1
[RouterA- ethernet 0/0/1] ip address 30.0.0.1 255.0.0.0
[RouterA- ethernet 0/0/1] quit
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 10.0.0.1 0.255.255.255
[RouterA-ospf-1 -area-0.0.0.0] network 20.0.0.1 0.255.255.255
[RouterA-ospf-1 -area-0.0.0.0] network 30.0.0.1 0.255.255.255
```

# Configure Router B:

```
[RouterB] router id 2.2.2.2
[RouterB] internet serial0/0/0
[RouterB-serial0/0/0] ip address 10.0.0.2 255.0.0.0
[RouterB-serial0/0/0] Interface ethernet 1/0/0
[RouterB-ethernet 1/0/0] ip address 40.0.0.1 255.0.0.0
[RouterB-ethernet 1/0/0] quit
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 10.0.0.2  0.255.255.255
[RouterB-ospf-1-area-0.0.0.0] area 1
[RouterB-ospf-1-area-0.0.0.1] network 40.0.0.1  0.255.255.255
```

# Configure Router C:

```
[RouterC] router id 3.3.3.3
[RouterC] interface ethernet 1/0/0
[RouterC-ethernet 1/0/0] ip address 40.0.0.2 255.0.0.0
[RouterC-ethernet 1/0/0] quit
[RouterC] ospf
[RouterC-ospf-1] area 1
[RouterC-ospf-1-area-0.0.0.1] network 40.0.0.2  0.255.255.255
```

Performing the **display ip routing-table** command on Router A and C, you can see that the two obtains the route to each other by OSPF, that is, both of them have routes to 20.0.0.0/8, 30.0.0.0/8, and 40.0.0.0/8.

4.4.2 Configuring OSPF Multi-process

I. Network requirements

Enable the OSPF process 100 on the interface Ethernet1/0/0 of Router A in Area 0.

Enable the OSPF process 100 on the interface Ethernet1/0/0 of Router B in Area 0and enable the OSPF process 200 on the interface Ethernet2/0/0 of Router B in Area 0.

Enable the OSPF process 200 on the interface Ethernet2/0/0 of Router C in Area 0.

Router A and Router B can be neighbors, and Router B and Router C can be neighbors.

II. Network diagram

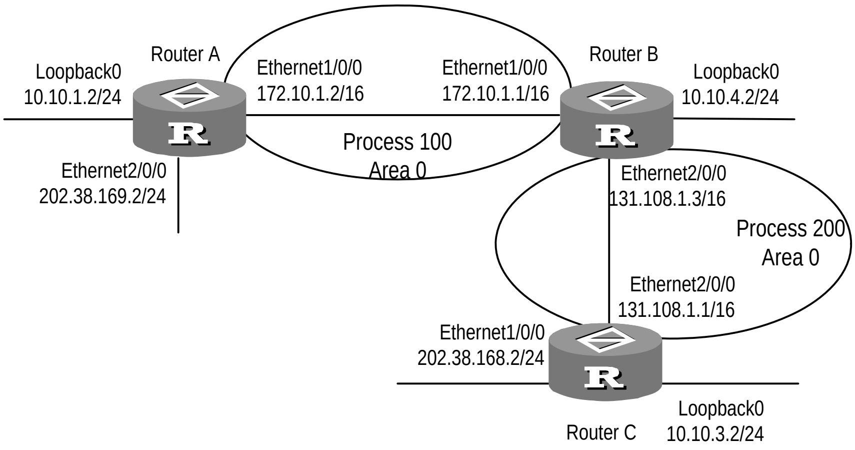


Figure 4-6 Configure OSPF multi-process

III. Configuration procedure

# Configure Router A:

```
[Router A] interface ethernet 1/0/0
[Router A-Ethernet1/0/0] ip address 172.10.1.2 255.255.0.0
[Router A-Ethernet1/0/0] quit
[Router A] router id 10.10.1.2
[Router A] ospf 100
[Router A-ospf-100] area 0
[Router A-ospf-100-area-0.0.0.0] network 172.10.0.0 0.0.255.255
```

# Configure Router B:

```
[Router B] interface ethernet 1/0/0
[Router B-Ethernet1/0/0] ip address 172.10.1.1 255.255.0.0
[Router B-Ethernet1/0/0] quit
[Router B] interface ethernet 2/0/0
[Router B-Ethernet2/0/0] ip address 131.108.1.3 255.255.0.0
[Router B-Ethernet2/0/0] quit
[Router B] ospf 100 router-id 10.10.20.1
[Router B-ospf-100] area 0
[Router B-ospf-100-area-0.0.0.0] network 172.10.0.0 0.0.255.255
[Router B-ospf-100] quit
[Router B] ospf 200 router-id 10.10.20.2
[Router B-ospf-200] area 0
```

```
[Router B-ospf-200-area-0.0.0.0] network 131.108.0.0 0.0.255.255
```

# Configure Router C:

```
[Router C] interface ethernet 2/0/0
[Router C-Ethernet2/0/0] ip address 131.108.1.1 255.255.0.0
[Router C-Ethernet2/0/0] quit
[Router C] router id 10.10.3.2
[Router C] ospf 200
[Router C-ospf-200] area 0
[Router C-ospf-200-area-0.0.0.0] network 131.108.0.0 0.0.255.255
```

Execute the **display ospf peer** command on Router B to view the neighbor creation. You will find that Router B and Router A form neighboring relationship in the OSPF process 100; while Router A and Router C cannot learn the routes from the peer via OSPF.

4.4.3 Configuring DR Election Based on OSPF Priority

I. Network requirements

In the following figure, the priority of Router A is 100, which is the highest in the network, so it is elected as the DR; Router C has the second highest priority, so it is elected as the BDR; The priority of Router B is 0, it means that it cannot be elected as the DR, and Router D does not have a priority, so the priority is 1 by default.

II. Network diagram

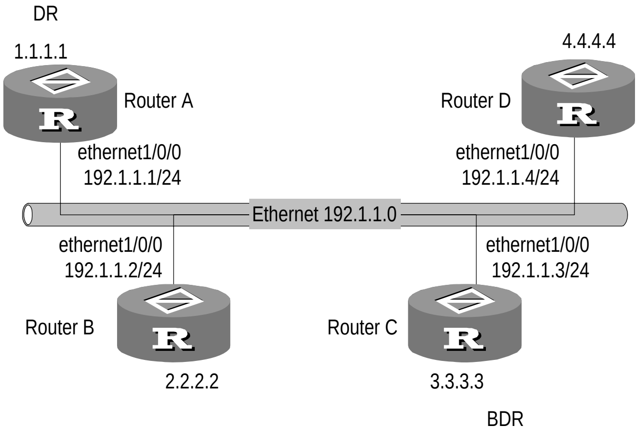


Figure 4-7 Configure DR election based on OSPF priority

III. Configuration procedure

# Configure Router A:

```
[Router A] interface ethernet 1/0/0
[Router A-Ethernet1/0/0] ip address 192.1.1.1 255.255.255.0
```

```
[Router A-Ethernet1/0/0] ospf dr-priority 100
[Router A-Ethernet1/0/0] quit
[Router A] router id 1.1.1.1
[Router A] ospf
[Router A-ospf] area 0
[Router A-ospf-area-0.0.0.0] network 192.1.1.0 0.0.0.255
```

# Configure Router B:

```
[Router B] interface ethernet 1/0/0
[Router B-Ethernet1/0/0] ip address 192.1.1.2 255.255.255.0
[Router B-Ethernet1/0/0] ospf dr-priority 0
[Router B-Ethernet1/0/0] quit
[Router B] router id 2.2.2.2
[Router B] ospf
[Router B-ospf] area 0
[Router B-ospf-area-0.0.0.0] network 192.1.1.0 0.0.0.255
```

# Configure Router C:

```
[Router C] interface ethernet 1/0/0
[Router C-Ethernet1/0/0] ip address 192.1.1.3 255.255.255.0
[Router C-Ethernet1/0/0] ospf dr-priority 2
[Router C-Ethernet1/0/0] quit
[Router C] router id 3.3.3.3
[Router C] ospf
[Router B-ospf] area 0
[Router B-ospf-area-0.0.0.0] network 192.1.1.0 0.0.0.255
```

# Configure Router D

```
[Router D] interface ethernet 1/0/0
[Router D-Ethernet1/0/0] ip address 192.1.1.4 255.255.255.0
[Router D-Ethernet1/0/0] quit
[Router D] router id 4.4.4.4
[Router D] ospf
[Router B-ospf] area 0
[Router B-ospf-area-0.0.0.0] network 192.1.1.0 0.0.0.255
```

In Router A, run **display ospf peer** to view the OSPF peers. Please note that Router A has three peers.

All neighbors are in full state. This indicates that Router A forms neighboring relationships with all its neighbors (Router A and Router C must form neighboring relationships with all routers on the network so as to act on the DR and BDR on the network. Router A is the DR and Router C the BDR on the network. All other neighbors are DR other (this indicates that they are neither DR nor BDR).

Change the priority of Router B into 200:

[Router B-Ethernet1/0/0] ospf dr-priority 200

On router A, run **display ospf peer** to view its OSPF peers. Please note the priority of Router B has been modified as 200, but it is still not the DR.

Only when the current DR is offline, will the DR be changed. Switch off Router A, and run **display ospf peer** command in Router D to view its peers. Note that the original BDR (Router C) becomes the DR, and Router B now becomes the BDR.

Switch off all the routers and restart them. Such operations will bring about a new DR/BDR selection. Router B will be elected as the DR (with a priority of 200), and Router A becomes the BDR (with a priority of 100).

4.4.4 Configuring Virtual Link of the OSPF

I. Network requirements

In the following figure, Area 2 is not directly connected with Area 0. Area 1 serves as a transit area to connect Area 2 and Area 0. A virtual link is configured between Router B and Router C.

II. Network diagram

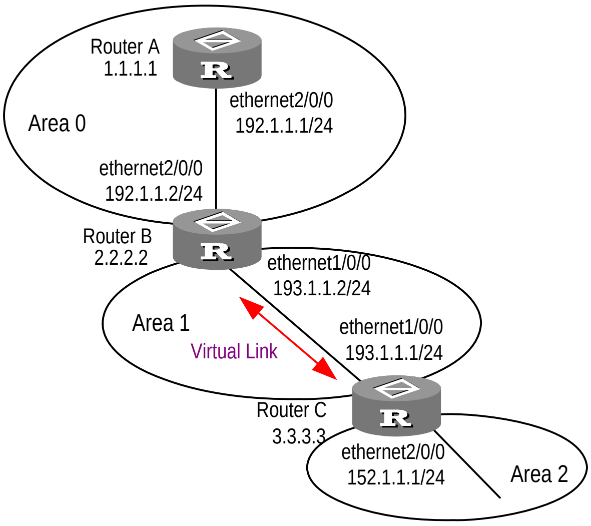


Figure 4-8 Configure OSPF virtual link

III. Configuration procedure

# Configure Router A:

```
[Router A] interface ethernet 2/0/0
[Router A-Ethernet2/0/0] ip address 192.1.1.1 255.255.255.0
[Router A-Ethernet2/0/0] quit
[Router A] router id 1.1.1.1
[Router A] ospf
[Router A-ospf] area 0
```

```
[Router A-ospf-area-0.0.0.0] network 192.1.1.0 0.0.0.255
```

# Configure Router B:

```
[Router B] interface ethernet 2/0/0
[Router B-Ethernet2/0/0] ip address 192.1.1.2 255.255.255.0
[Router B-Ethernet2/0/0] interface ethernet 1/0/0
[Router B-Ethernet1/0/0] ip address 193.1.1.2 255.255.255.0
[Router B-Ethernet1/0/0] quit
[Router B] router id 2.2.2.2
[Router B] ospf
[Router B-ospf] area 0
[Router B-ospf-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[Router B-ospf-area-0.0.0.0] quit
[Router B-ospf] area 1
[Router B-ospf-area-0.0.0.1] network 193.1.1.0 0.0.0.255
[Router B-ospf-area-0.0.0.1] vlink-peer 3.3.3.3
```

# Configure Router C:

```
[Router C] interface ethernet 2/0/0
[Router C-Ethernet2/0/0] ip address 152.1.1.1 255.255.255.0
[Router C-Ethernet2/0/0] interface ethernet 1/0/0
[Router C-Ethernet1/0/0] ip address 193.1.1.1 255.255.255.0
[Router C-Ethernet1/0/0] quit
[Router C] router id 3.3.3.3
[Router C] ospf
[Router C-ospf] area 1
[Router C-ospf-area-0.0.0.1] network 193.1.1.0 0.0.0.255
[Router C-ospf-area-0.0.0.1] vlink-peer 2.2.2.2
[Router C-ospf-area-0.0.0.1] quit
[Router C-ospf] area 2
[Router C –ospf-area-0.0.0.2] network 152.1.1.0 0.0.0.255
```

4.4.5 Configuring OSPF Peer Authentication

I. Network requirements

In the following figure, Router A adopts pure text authentication when it exchanges route update information with Router C; while it adopts MD5 encryption authentication when it exchanges route update with Router C.

The Ethernet interfaces of Router A and Router B are in the OSPF Area 0. The Serial interfaces of Router A and Router C are in Area 1 and MD5 authentication is configured on them.

II. Network diagram

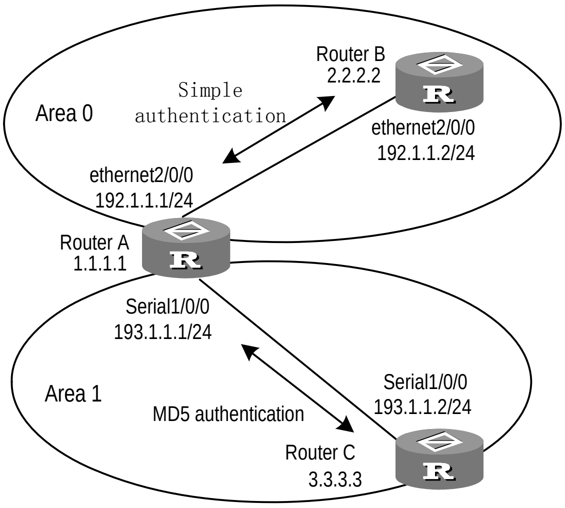


Figure 4-9 Configure OSPF neighboring authentication

III. Configuration procedure

# Configure Router A:

Configure the Area 1, where the network segment 193.1.1.0 of the interface serial1/0/0 resides, to support MD5 encryption authentication, with the identifier of authentication character being 1 and the authentication character being password.

Configure the Area 0, where the network segment 192.1.1.0 of the interface ethernet2/0/0 resides, to support plain text authentication, with the authentication character being password.

```
[Router A] interface ethernet 2/0/0
[Router A-Ethernet2/0/0] ip address 192.1.1.1 255.255.255.0
[Router A-Ethernet2/0/0] ospf authentication-mode simple password
[Router A] interface serial 1/0/0
[Router A-serial1/0/0] ip address 193.1.1.1 255.255.255.0
[Router A-serial1/0/0] ospf authentication-mode md5 1 password
[Router A] router id 1.1.1.1
[Router A] ospf
[Router A-ospf] area 0
[Router A-ospf-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[Router A-ospf-area-0.0.0.0] authentication-mode simple
[Router A-ospf-area-0.0.0.0] quit
[Router A-ospf] area 1
[Router A-ospf-area-0.0.0.1] network 193.1.1.0 0.0.0.255
[Router A-ospf-area-0.0.0.1] authentication-mode md5
```

# Configure Router B:

```
[Router B] interface ethernet 2/0/0
[Router B-Ethernet2/0/0] ip address 192.1.1.2 255.255.255.0
[Router B-Ethernet2/0/0] authentication-mode simple password
[Router B] router id 2.2.2.2
[Router B] ospf
[Router B-ospf] area 0
[Router B-ospf-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[Router B-ospf-area-0.0.0.0] authentication-mode simple
```

# Configure Router C:

```
[Router C] interface serial 1/0/0
[Router C-serial1/0/0] ip address 193.1.1.2 255.255.255.0
[Router C-serial1/0/0] ospf authentication-mode md5 1 password
[Router C] router id 3.3.3.3
[Router C] ospf
[Router C-ospf] area 1
[Router C-ospf-area-0.0.0.1] network 193.1.1.0 0.0.0.255
[Router C-ospf-area-0.0.0.1] authentication-mode md5
```

4.4.6 Configuring OSPF STUB areas

I. Network requirements

RouterA and RouterB are connected by serial interfaces, and RouterB and RouterC are connected by Ethernet interfaces. RouterA belongs to area0, RouterC belongs to area1, and RouterB belongs to both area0 and area1. Configure area1 as a STUB area.

II. Network diagram

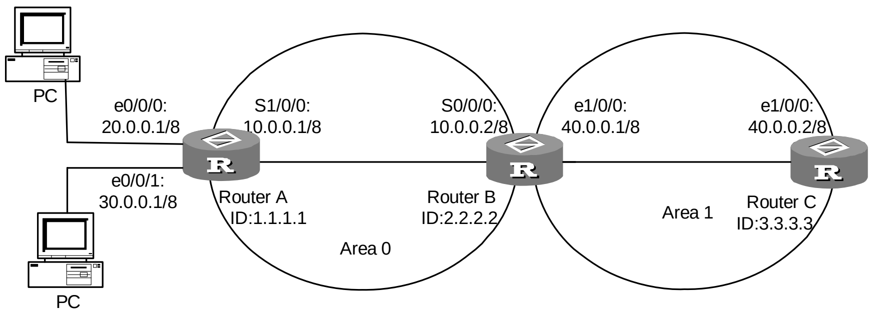


Figure 4-10 Configure OSPF STUB areas

III. Configuration procedure

# Configure RouterA:

```
[RouterA] router id 1.1.1.1
[RouterA] interface serial1/0/0
```

```
[RouterA-serial1/0/0] ip address 10.0.0.1 255.0.0.0
[RouterA-serial1/0/0] interface ethernet0/0/0
[RouterA-ethernet 0/0/0] ip address 20.0.0.1 255.0.0.0
[RouterA- ethernet 0/0/0] interface ethernet0/0/1
[RouterA- ethernet 0/0/1] ip address 30.0.0.1 255.0.0.0
[RouterA- ethernet 0/0/1] quit
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0]  network 10.0.0.1 0.255.255.255
[RouterA-ospf-1 -area-0.0.0.0] network 20.0.0.1 0.255.255.255
[RouterA-ospf-1 -area-0.0.0.0] network 30.0.0.1 0.255.255.255
```

# Configure RouterB:

```
[RouterB] router id 2.2.2.2
[RouterB] internet serial0/0/0
[RouterB-serial0/0/0] ip address 10.0.0.2 255.0.0.0
[RouterB-serial0/0/0] Interface ethernet 1/0/0
[RouterB-ethernet 1/0/0] ip address 40.0.0.1 255.0.0.0
[RouterB-ethernet 1/0/0] quit
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 10.0.0.2  0.255.255.255
[RouterB-ospf-1-area-0.0.0.0] area 1
[RouterB-ospf-1-area-0.0.0.1] network 40.0.0.1  0.255.255.255
[RouterB-ospf-1-area-0.0.0.1] stub
```

# Configure RouterC:

```
[RouterC] router id 3.3.3.3
[RouterC] interface ethernet 1/0/0
[RouterC-ethernet 1/0/0] ip address 40.0.0.2 255.0.0.0
[RouterC-ethernet 1/0/0] quit
[RouterC] ospf
[RouterC-ospf-1] area 1
[RouterC-ospf-1-area-0.0.0.1] network 40.0.0.2  0.255.255.255
[RouterC-ospf-1-area-0.0.0.1] stub
```

Now, on RouterC, in addition to inter-area routes discovered by OSPF, there should be a default route of 0.0.0.0/0.

If you configure the **stub nosummary** command instead of the **stub** command on ABR Router B, area1 will become completely a STUB area, and RouterC no longer has any inter-area routes but a default route.

4.5 Troubleshooting OSPF

Symptom 1: The OSPF is configured according to the above procedures, but the router OSPF cannot operate normally.

Troubleshooting:

Please check according to the following procedures.

1) Local fault removal: First, check whether the protocol between two directly connected routers is in normal operation. The normal sign is the peer status machine between the two routers reaches the FULL state. (Note that in the Broadcast and NBMA network, the peer state machine between two DR Other routers cannot reach the FULL state but the 2-way state. But Full State can be reached between the DR, BDR and all the other routers)

- Run the **display ospf peer** command to view the information about OSPF peer.
- Run **display ospf interface** command to view the OSPF information in the interface.
- Check whether the physical connections and the lower level protocols operate normally. You can run **ping** command to test. If the local router cannot reach the remote router, it indicates that the physical connections and the lower level protocols cannot operate normally.
- If the physical connections and the lower level protocols are normal, then please check the OSPF parameters configured in the interface, but you must guarantee the consistency of the parameters of its adjacent router. The area IDs should be the same, and the network segments and the masks should also be consistent (the **p2p** and virtually linked network segments and masks can be different).
- Check and ensure that the value of the dead-interval on the same interface should be at least four times the value of the hello-interval and be consistent with the configuration on the peer.
- If the network type is NBMA, you must manually specify Peer. The **peer ip-address** command is used.
- If the network type is Broadcast or NBMA, the priority of at least one interface should be larger than 0.
- If an Area is set as the STUB area, then the area must be set **stub** in all the routers connected to this area.
- The interface types of two adjacent routers should be consistent.
- If more than two areas are configured, then at least one area should be configured as the backbone area (i.e. the area ID is 0).
- Ensure the backbone area is connected with all the other areas.
- The virtual links cannot pass through the STUB area.

2) Global fault removal: If the above procedures are correct, but the OSPF still cannot find the remote routes, please check the following configurations:

- If a router is configured with more than two areas, then at least one area should be configured as the backbone area.

As is shown in the following figure, only an area is configured in RTA and RTD, but two areas are configured in RTB (area0, area1) and RTC (area1, area2) respectively. In which, RTB has an area with the ID of 0, so it meets the requirement; while both areas of RTC are not 0, and accordingly it is necessary to create a virtual connection between RTC and RTB. Ensure that Area 2 and Area 0 (the backbone area) be interconnected.

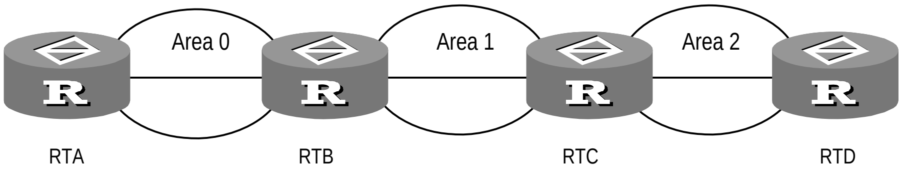


Figure 4-11 OSPF area

- A virtual connection cannot go across a STUB area. The backbone area (Area 0) cannot be configured into a STUB area either. In other words, if a virtual connection is configured between RTB and RTC, neither Area 1 nor Area 0 can be configured into a STUB area. In the above figure, only Area 2 can be configured into a STUB area.
- The router in the STUB area cannot receive external routes.
- The backbone area should guarantee the connection between various nodes.

Chapter 5 Integrated IS-IS Configuration

5.1 Integrated IS-IS Overview

Intermediate System-to-Intermediate System intra-domain routing information exchange protocol (IS-IS) is the dynamic routing protocol initially issued by the International Organization for Standardization (ISO) for its CLNP (Connectionless Network Protocol). To provide route support to IP, IETF extends and modifies IS-IS in RFC1195, nominating it as Integrated IS-IS or Dual IS-IS, which applies to TCP/IP and OSI environment simultaneously.

IS-IS protocol, based on the link state algorithm, uses the Shortest Path First (SPF) algorithm and highly resembles the Open Shortest Path First (OSPF) protocol. IS-IS, used for internal AS, belongs to IGP (Interior Gateway Protocol).

5.1.1 Related Concepts

I. Some terms of IS-IS

- Intermediate System (IS). IS equals to a router of TCP/IP. It is the basic unit in IS-IS protocol used for propagating routing information and generating routes. In the following text, "IS" shares the same meaning with the "router".
- End System (ES). It equals to the host system of TCP/IP. ES does not involve in IS-IS processing. ISO has the dedicated ES-IS protocol to define the communication between an ES and an IS.
- Routing Domain (RD). A group of ISs exchange routing information via the same routing protocol in a routing domain.
- Area. Area is the division unit in the routing domain.
- Link State DataBase (LSDB). All the link states in the network form the LSDB. In an IS, at least one LSDB is available. The IS uses the SPF algorithm and the LSDB to generate its own routes.
- Link State Protocol Data Unit (LSP). In the IS-IS, each IS will generate an LSP which contains all the link state information of the IS. Each IS collects all the LSPs in the local area to generate its own LSDB.
- Network Protocol Data Unit (NPDU). It is the network layer packets of ISO and equals to the IP packet of TCP/IP.
- DIS (Designated IS), an election router on a broadcast network.
- NSAP (Network Service Access Point), namely a network layer address in the ISO system. It identifies an abstract network service access point and describes the network address for ISO model routing.

II. Link types suitable for IS-IS

IS-IS can operate over point-to-point links, such as PPP and HDLC, or broadcast links, such as Ethernet and Token-ring. For NBMA (Non-Broadcast Multi-Access) network, such as ATM, it is necessary to configure sub-interfaces and configure the types of sub-interfaces as P2P or broadcast network. IS-IS cannot operate over point-to-multipoint links.

5.1.2 Two-level Structure of IS-IS Routing Protocol

I. Two-level structure

In order to support large-scale routing networks, IS-IS adopts a two-level structure in an RD. A large RD is divided into one or more areas. Intra-area routing is managed by Level-1 routers while inter-area routing is managed by Level-2 routers.

II. Level-1 and Level-2

- Level-1 router

The Level-1 router manages the intra-area routing. Level-1 routers in the same area form neighborhood to maintain the LSDB in its own Level-1 area. The LSDB contains the routing information of its area. When a Level-1 router receives a packet whose destination address is in an extra area, it will forward the packet to the nearest Level-2 router.

- Level-2 router

The Level-2 router manages the inter-area routing. A Level-2 router can form neighborhood with other Level-2 routers to maintain the LSDB of Level-2 area. The LSDB contains routing information between areas. All Level-2 routers constitute the backbone network of the routing domain, and are responsible for communication between different areas. The Level-2 routers in the routing domain must be successive to ensure the continuity of the backbone network. Only Level-2 routers can exchange data packets or routing information with routers outside the routing domain.

- Level-1-2 router

A router, which belongs to both a level-1 area and a level-2 area, is called as a level-1-2 router. Each area has at least one level-1-2 router to connect the area to the backbone network. A level-1-2 router maintains two LSDBs: one level-1 LSDB for intra-area routing and one level-2 LSDB for inter-area routing.

The following figure illustrates an IS-IS enabled network, containing both Routing Domain 1 and Routing Domain 2. Routing Domain 1 includes two areas, Area 1 and Area 2. Routing Domain 2 only includes one area, Area 3. In Routing Domain 1, the three ISs connected with bold lines forms the backbone of the Routing Domain. These 3 ISs are all level-2 routers. The other 4 ISs, which are not directly connected with bold lines, are level-1 routers.

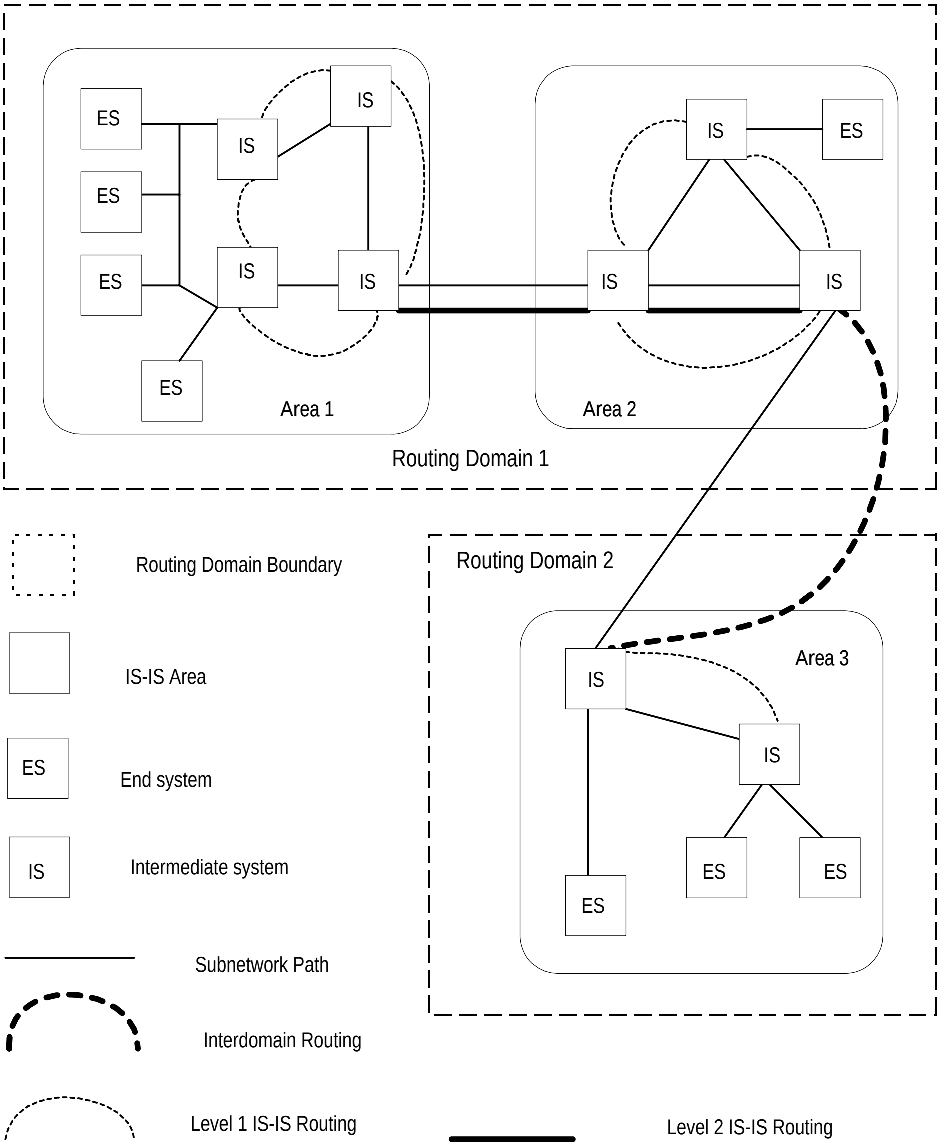


Figure 5-1 IS-IS topology

III. Routing leak

Generally speaking, an IS-IS area can also be called as a Level-1 area. Internal routes are managed by Level-1 routers. All Level-2 routers form a Level-2 area. Thus, an IS-IS routing domain may contain multiple Level-1 areas but only one Level-2 area.

A Level-1 area can only connect with a Level-2 area. Different Level-1 areas cannot connect with each other.

Routing information inside a Level-1 area is advertised to the Level-2 area via Level-1-2 routers. Therefore, Level-2 routers know routing information in the whole IS-IS routing domain. However, Level-2 routers do not advertise the routing information of other Level-1 areas and the Level-2 area they know to Level-1 area by default. Thus, Level-1 routers do not know outside routing information, which may make them unable to choose the best route to a destination address outside their local area.

In order to address the above problem, IS-IS provides routing leak function, which enables a Level-2 router to advertise the routing information of other Level-1 areas and the Level-2 area it knows to a specified Level-1 area.

5.1.3 Address Structure of IS-IS Routing Protocol

I. Address structure

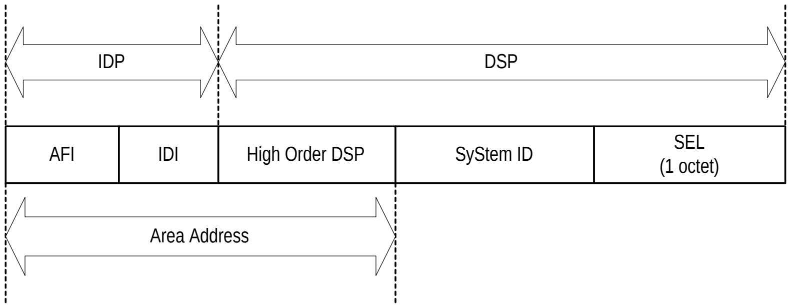


Figure 5-2 Address structure of IS-IS protocol

ISO adopts the address structure as shown in the above figure, namely NSAP, which consists of Initial Domain Part (IDP) and Domain Specific Part (DSP). Stipulated in ISO, IDP specifies the authority, who assigns other parts of an address, as well as the format that an address adopts. DSP is assigned by the specified entity in IDP. The length of IDP and DSP is variable, but their total length is of 20 bytes at most.

- Area address

IDP consists of Authority and Format Indicator (AFI) and Initial Domain Identifier (IDI). AFI decides the format of IDI. DSP is formed by multiple bytes. IDP, along with HO-DSP of DSP, can identify both a routing domain and areas in a routing domain; therefore, (IDP, HO-DSP) as a whole is also called as Area Address.

Generally speaking, a router only needs to be configured with one area address. Moreover, all the nodes in the same area have the same area address. In order to support seamless combination, division and transformation of areas, a router can be configured with 3 area addresses at most.

- System ID

A system ID is used to uniquely identify an ES or a router in an area. Its length is optional, being 48 bits (6 bytes). Normally, a Router_ID is adopted to correspond with a system ID.

Suppose a router takes the IP address 168.10.1.1 of the interface Loopback0 as its Router_ID, then its System ID used in IS-IS can be transformed with the following method:

Extend every part of the IP address 168.10.1.1 to 3 bits. Add 0 to the front of the part that includes less than 3 bits.

Divide the extended address 168.010.001.001 into 3 parts, with each part consisting of 4 digits.

The reconstructed 1680.1000.1001 is just the System ID.

Actually, there are many ways to designate a System ID, as long as it can uniquely identify an ES or a router.

- SEL

The role of an SEL (NSAP Selector, or N-SEL as called sometimes) is similar to the “protocol ID” of IP. Different transport protocols correspond to different SELs. The SEL over IP is uniformed into "00”.

As this kind of address structure definitely defines an area, level-1 routers can easily identify packets sent to an outside area, which packets are to be forwarded to level-2 routers.

Level-1 routers use System ID to implement intra-area routing. Once a level-1 router finds that the destination address of a packet is out of its own area, it will forward the packet to a nearest level-2 router.

Level-2 routers perform inter-area routing according to their area addresses (IDP + HO-DSP).

II. NET

Network Entity Title (NET) indicates the network layer information of IS itself, excluding transport layer information (SEL = 0). It can be regarded as a special NSAP.

Generally, a router is only configured with one NET. When it is necessary to reconstruct an area, for example, to combine many areas together or to divide an area into separate areas, multiple NETs should be configured on a router so that route correctness could be guaranteed even upon reconfiguration. As 3 area addresses can be configured at most, totally there can be only 3 configured NETs.

For example, there is a NET 47.0001.aaaa.bbbb.cccc.00, in which,

Area = 47.0001, System ID = aaaa.bbbb.cccc, SEL = 00.

For example, there is a NET 01.1111.2222.4444.00, in which,

Area = 01, System ID = 1111.2222.4444, SEL = 00.

5.1.4 IS-IS Routing Protocol Packets

IS-IS packets are directly encapsulated in data link frames. Basically, they fall into 3 categories: Hello packet, LSP and SNP.

I. Hello packet

Hello packets, also called as IIHs (IS-to-IS Hello PDUs), are used to create and construct neighboring relationship. Among them, the Level-1 LAN IIH apply to level-1 routers on broadcast LAN, Level-2 LAN IIHs apply to level-2 routers on broadcast LAN and Point-to-Point IIHs apply to non-broadcast networks.

II. LSP

LSPs (link state PDUs) are used for exchanging link state information. There are two kinds of LSPs: Level-1 LSP and Level-2 LSP. Level-2 LSP is forwarded via level-2 routers; while Level-1 LSP is forwarded via Level-1 routers. Level-1-2 routers can forward the both.

III. SNP

SNPs (sequence number PDUs) are used to confirm the newly received LSP between neighbors. Their role is similar to but more effective than that of acknowledge packets. SNP include CSNP (Complete SNP) and PSNP (Partial SNP), which are further divided into level-1 CSNP, level-2 CSNP, level-1 PSNP and level-2 PSNP.

PSNP only lists lately received one or more LSP sequence numbers. It can acknowledge multiple LSPs at one time. Once LSDB is found asynchronous, PSNP is also adopted to request a neighbor to send a new LSP.

CSNP contains all LSP summary information in LSDB, so that LSDB synchronization could be maintained between neighboring routers. On a broadcast network, CSNP is periodically transmitted by DIS (the default transmission period is 10 seconds). On a point-to-point line, CSNP is only transmitted when a neighboring relationship is initially created.

5.2 Integrated IS-IS Configuration

Among the following configurations, the "Enable IS-IS" is required, while other configurations are optional.

IS-IS configuration includes:

- Enable IS-IS
- Configure NET
- Enable IS-IS on the Specified Interface
- Configure Metrics Notation of IS-IS Packets
- Configure IS-IS link State Routing Metrics
- Configure the Timers of IS-IS
- Configure the Priority of a Router
- Configure Interface Circuit Level
- Configure Interface Authentication Password
- Configure the Mesh Group of the Interface

- Configure Router Type
- Set to Generate the Default Route
- Configure IS-IS Authentication Password
- Configure Route Aggregation
- Configure Overload Flag Bit
- Configure to Ignore the LSP Checksum Errors
- Configure to Log the Peer Changes
- Configure LSP Refresh Interval
- Configure Lifetime of LSP
- Set the SPF Calculation Interval
- Set SPF Fragmented Calculation
- Set SPF to Release CPU Actively
- Enable/Disable the Interface to Send Packets
- Configure IS-IS to Redistribute Routes from Other Protocols
- Configure IS-IS Route Filtering
- Configure the Preference of IS-IS Protocol
- Configure IS-IS Routing Leak
- Reset IS-IS Data Structure
- Reset the Specified IS-IS Peer

5.2.1 Enabling IS-IS

To enable IS-IS protocol, you must create an IS-IS routing process and activate it on the interface, which may associate with other routers.

Perform the following configuration in system view.

Table 5-1 Enable IS-IS

Operation	Command
Enable IS-IS routing process and enter the IS-IS view	**isis** [*tag*]
Delete IS-IS routing process	**undo isis** [*tag*]

The parameter *tag* is an identifier in an IS-IS process. In the current version, only one IS-IS process is enabled.

By default, the IS-IS routing process is disabled.

5.2.2 Configuring NET

Network Entity Titles (hereinafter referred to as NETs) defines the current IS-IS area address and the system ID of the router.

Perform the following configuration in IS-IS view.

Table 5-2 Configure NET

Operation	Command
Set NET	**network-entity** *net*
Delete NET	**undo network-entity** *net*

The format of parameter *net* is X...XXXXXXXXXXXX.XX, among which the first "X…X" is the area address, the twelve Xs in the middle is the System ID of the router. The last XX should be 00.

5.2.3 Enabling IS-IS on the Specified Interface

After enabling IS-IS, you need to specify on which interfaces the IS-IS will be enabled.

Perform the following configuration in interface view.

Table 5-3 Enable IS-IS on the specified interface

Operation	Command
Enable IS-IS on the specified interface	**isis enable** [*tag*]
Disable IS-IS on the specified interface	**undo isis enable** [*tag*]

By default, IS-IS is disabled on interfaces.

Note:

So far, a router can enable IS-IS process on 255 interfaces at most, including logic interfaces such as subinterfaces.

5.2.4 Configuring Hello Packet Stuffing of IS-IS

Perform the following configuration in interface view.

Table 5-4 Enable/disable Hello packet stuffing of IS-IS

Operation	Command
Disable IS-IS to stuff Hello packets to the size of interface MTU if their data sizes are smaller.	**isis small-hello**
Restore the default to allow IS-IS to stuff Hello packets to the size of interface MTU if their data sizes are smaller.	**undo isis small-hello**

You are recommended to configure the **isis small-hello** command on the interfaces with an MTU greater than 1500 bytes, such as tunnel and GE interfaces.

5.2.5 Configuring Metrics Notation of IS-IS Packets

IS-IS routing protocol has two notations for link metrics:

- Narrow mode, in which the metrics ranges from 1 to 63.
- Wide mode, in which the metrics ranges from 1 to 2^{24}-1, i.e., 1 to 16777215.

The router can either support one of them or support the both.

Perform the following configuration in IS-IS view.

Table 5-5 Configure metrics notation of IS-IS packets

Operation	Command
Configure metrics notation of IS-IS packets	**cost-style** { **narrow** | **wide** | **compatible** [**relax-spf-limit**] | **narrow-compatible** [**relax-spf-limit**] | **wide-compatible** }
Restore the default setting	**undo cost-style**

By default, IS-IS only receives/sends packets whose metric is notated in Narrow mode.

5.2.6 Configuring IS-IS link State Routing Metrics

Users can configure the interface cost, i.e. the default routing metrics. When the cost type is narrow, its range is 1 to 63; when the cost type is wide, its range is 1 to 16777215.

Perform the following configuration in interface view.

Table 5-6 Configure IS-IS link state routing metrics

Operation	Command
Set the routing metrics of the interface	**isis cost** *vlaue* [**level-1** | **level-2**]
Restore the default routing metrics of the interface	**undo isis cost** [**level-1** | **level-2**]

If the command does not specify a metrics to be level-1 or level-2, it is a level-1 metrics by default.

By default, the routing metrics of IS-IS on an interface is 10.

5.2.7 Configuring the Timers of IS-IS

Perform the following configuration in interface view.

I. Configuring the Hello packet broadcast interval

IS-IS sends hello packets on an interface periodically. Routers maintain their neighboring relationship through the sending/receiving of Hello packets. The transmission interval of hello packets can be changed through configuration.

Table 5-7 Configure the hello packet broadcast interval

Operation	Command
Set the transmission interval of hello packets on an interface, with the time unit being second	**isis timer hello** *seconds* [**level-1** | **level-2**]
Restore the default transmission interval of hello packets on an interface	**undo isis timer hello** [**level-1** | **level-2**]

Usually, on the broadcast links, there exist level-1 and level-2 hello packets. For different packets, different broadcast intervals should be set. However, there are two exceptions. One is when there is no level separation in the link, parameters of level-1 and level-2 need not be specified in the command (adopt the default values). The system will set the broadcast intervals of all packets as that of the level-1 hello packet. The other is if hello packets are not separated according to level-1 and level-2 on the **p2p** links, the attribute of the packets need not be set either.

By default, Hello packets are transmitted on interface every 10 seconds.

II. Configuring the CSNP packet broadcast interval

The CSNP packet is transmitted by the DIS (Designated IS) over the broadcast network to synchronize the link state database (LSDB). The CSNP packet is regularly broadcast over the broadcast network at an interval, which can be set by users.

Table 5-8 Configure the CSNP packet broadcast interval

Operation	Command
Set the CSNP packet broadcast interval, measured in seconds	**isis timer csnp** *seconds* [**level-1** | **level-2**]
Restore the default CSNP packet broadcast interval on the interface	**undo isis timer csnp** [**level-1** | **level-2**]

If the level is not specified, it defaults to setting CSNP packet broadcast interval for Level-1.

By default, the CSNP packet is transmitted via interface every 10 second.

III. Configuring the LSP packet transmission interval

LSP carries the link state records for propagation throughout the area.

Table 5-9 Configure the LSP packet transmission interval

Operation	Command
Set LSP packet transmission interval on the interface, measured in milliseconds.	**isis timer lsp** *time*
Restore the default LSP packet transmission interval on the interface	**undo isis timer lsp**

By default, the LSP packet is transmitted via the interface every 33 millisecond.

IV. Configuring LSP packet retransmission interval

Over a **p2p** link, if the local end does not receive the response within a period of time after it sends an LSP packet, it considers that the originally transmitted LSP packet has been lost or dropped. In order to guarantee the transmission reliability, the local router will retransmit the original LSP packet.

Table 5-10 Set LSP packet retransmission interval

Operation	Command
Set the retransmission interval of the LSP packet over **p2p** links	**isis timer retransmit** *seconds*
Restore the default retransmission interval of the LSP packet over **p2p** links	**undo isis timer retransmit**

By default, the LSP packet is transmitted every 5 seconds over the **p2p** link.

V. Specifying the ratio of holdingtime to Hello interval

The IS-IS protocol maintains the adjacency among routers by transmitting/receiving the Hello packets. If the local router does not receive Hello packets in a time interval transmitted by the peer continuously, it considers the adjacent router as invalid. The waiting time is the Holddown time of IS-IS.

In IS-IS, the Holddown time is adjusted by setting the number of Hello messages, that is, the adjacent router will be regarded as invalid if the number of continuously received Hello messages does not reach the configured number.

Table 5-11 Specify the ratio of holding time to Hello interval

Operation	Command
Specify the ratio of holding time to Hello interval	**isis timer holding-multiplier** *value* [**level-1** | **level-2**]
Restore the default setting	**undo isis timer holding-multiplier** [**level-1** | **level-2**]

By default, the number of Hello messages is 3.

If neither **Level-1** nor **Level-2** is configured in the command, the configuration takes effect on Hello messages of both Level-1 and Level-2.

5.2.8 Configuring the Priority of a Router

In the broadcast network, the IS-IS needs to elect a DIS from all the routers.

When you need to select a DIS from the IS-IS peers on the broadcast network, you should select level-1 DIS and level-2 DIS respectively. The higher the priority is, the more possible it is selected. If there are two or more routers with the highest priority in the broadcast network, the one with the greatest MAC address will be selected. If all the adjacent routers' priorities are 0, the one with the greatest MAC address will be selected.

The DISs of Level-1 and Level-2 are elected separately. You can set different priorities for DIS election at different levels.

Perform the following configuration in interface view.

Table 5-12 Set the priority for DIS election

Operation	Command
Set the priorities for DIS election on the interface	**isis dis-priority** *value* [**level-1** | **level-2**]
Restore the default priorities for DIS election on the interface	**undo isis dis-priority** [**level-1** | **level-2**]

By default, the priority on an interface is 64. If the level is not specified, the priority of level-1 is set by default.

5.2.9 Configuring Interface Circuit Level

Perform the following configuration in Ethernet interface view.

Table 5-13 Set interface circuit level

Operation	Command
Set interface circuit level	**isis circuit-level** [**level-1** | **level-1-2** | **level-2**]
Restore the default interface circuit level	**undo isis circuit-level**

You can set the circuit level to limit what adjacency can be established for the interface. For example, Level-1 interface can only have Level-1 adjacency. Level-2 interface can only have Level-2 adjacency. For the Level-1-2 router, you can configure some interfaces to Level-2 to prevent transmitting Level-1 Hello packets to Level-2 backbone so as to save the bandwidth. However Level-1 and Level-2 use the same kind of Hello packet over the **p2p** link, and therefore such setting is unnecessary in this case.

By default, the circuit-level on the interface route is **level-1-2**.

5.2.10 Configuring Interface Authentication Password

The authentication password set on the interface is mainly used in the Hello packet so as to confirm the validity and correctness of its peers. The authentication passwords at the same level of all the interfaces of a network should be identical.

Perform the following configuration in Ethernet interface view.

Table 5-14 Set interface authentication password

Operation	Command
Configure authentication password	**isis authentication-mode** { **simple** | **md5** } *password* [{ **level-1** | **level-2** } [**ip** | **osi**]]
Delete authentication password	**undo isis authentication-mode** { **simple** | **md5** } *password* [{ **level-1** | **level-2** } [**ip** | **osi**]]

By default, the interface is not configured with any authentication password or performs authentication. If the level is not specified, it defaults to setting the authentication password of Level-1.

5.2.11 Configuring the Mesh Group of the Interface

On NBMA network, the interface of a router will flood the received LSP to other interfaces. However, this processing method applied to a network with higher connectivity and several **p2p** links will cause repeated LSP flooding and waste bandwidth.

To avoid such problem, you can configure several interfaces into a mesh group. The interface will not flood the LSP received from inside the group to other interfaces of the same group and flood it outside the group only.

Perform the following configuration in interface view.

Table 5-15 Configure the mesh group of the interface

Operation	Command
Add the interface into a mesh group	**isis mesh-group** [*mesh-group-number* | **mesh-blocked**]
Remove the interface from a mesh group	**undo isis mesh-group**

By default, the LSP is flooded normally from the interface. When configured with the **mesh-blocked** parameter, it will not flood the LSP to other interfaces.

Thus the IS-IS configuration on the interface are done. The following sections discuss how to configure other parameters of IS-IS.

5.2.12 Configuring Router Type

Users can set the levels of the current router. Based upon the position of the router, the levels can be divided into Level-1 (intra-domain router), Level-2 (inter-domain router) and Level-1-2 (i.e. intra-domain router as well as inter-domain router).

Perform the following configuration in IS-IS view.

Table 5-16 Set router type

Operation	Command
Set router type	**is-level** { **level-1** | **level-1-2** | **level-2** }
Restore the default router type	**undo is-level**

By default, the router type is **level-1-2**.

5.2.13 Setting to Generate the Default Route

In the IS-IS route domain, the Level-1 router only has the LSDB of the local area, so it can only generate the routes in the local areas. But the Level-2 router has the backbone LSDB in the IS-IS route domains and generates the backbone network routes only. If a Level-1 router in those areas wants to forward the packets to other areas, it needs to first forward the packets to the closest Level-1-2 router in the local area along its default route.

Perform the following configuration in IS-IS view.

Table 5-17 Set to generate the default route

Operation	Command
Set to generate the default route	**default-route-advertise** [**route-policy** *route-policy-name*]
Set not to generate the default route	**undo default-route-advertise** [**route-policy** *route-policy-name*]

The default route generated by this command will only be redistributed to the router at the same level.

5.2.14 Configuring IS-IS Authentication Password

Users can configure the IS-IS area or the IS-IS routing domain with authentication password.

If area authentication is needed, the area authentication password will be encapsulated into the level-1 LSP, CSNP and PSNP packets, in the specified mode. If other routers in the same area also have started the area authentication, the authentication modes and passwords of them must be identical to the old ones, so that they can work normally. Similarly, for routing domain authentication, the password will also be encapsulated into the level-2 LSP, CSNP and PSNP packets in the specified mode. If the routers in the backbone layer (level-2) also need routing domain authentication, the authentication mode and password must be identical to the old ones.

Perform the following configuration in IS-IS view.

Table 5-18 Configure IS-IS authentication password

Operation	Command
Set area authentication password	**area-authentication-mode** { **simple** | **md5** } *password* [**ip** | **osi**]
Delete area authentication password	**undo area-authentication-mode** { **simple** | **md5** } [**ip** | **osi**]
Set routing domain authentication password	**domain-authentication-mode** { **simple** | **md5** } *password* [**ip** | **osi**]
Delete routing domain authentication password	**undo domain-authentication-mode** { **simple** | **md5** } [**ip** | **osi**]
Configure ISIS to use the Huawei-compatible MD5 algorithm	**md5-compatible**
Restore the default MD5 algorithm (standard algorithm)	**undo md5-compatible**

By default, the system does not require password or perform authentication.

Note:

After configuring the **area-authentication-mode** command, you must execute the **reset isis peer** command to reset the neighboring relation; Otherwise, the **area-authentication-mode** command does not take effect.

5.2.15 Configuring Route Aggregation

Route aggregation aggregates multiple routes in the same segment but different subnets into a single route. The segment does not necessarily mean a natural segment, but it can also be a subnet segment or supernet segment. All the subnet routes to be aggregated must have the same next hop.

Route aggregation can effectively minimize route information and routing tables.

Perform the following configuration in IS-IS view.

Table 5-19 Configure route aggregation

Operation	Command
Set route aggregation	**summary** *ip-address ip-mask* [**level-1** | **level-1-2** | **level-2**]
Delete the route aggregation	**undo summary** *ip-address ip-mask* [**level-1** | **level-1-2** | **level-2**]

By default, the system disables route aggregation.

5.2.16 Configuring Overload Flag Bit

Sometimes, the router in the IS-IS domain may encounter some problems in operation thus error may occur in the whole routing area. In order to avoid this problem, we can set the overload flag bit for this router.

When the overload threshold is set, other routers should not send this router the packets which should be forwarded by this router.

Perform the following configuration in IS-IS view.

Table 5-20 Configure overload flag bit

Operation	Command
Set overload flag bit	**set-overload**
Remove the overload flag bit	**undo set-overload**

By default, no over load bit is set.

5.2.17 Configuring to Ignore the LSP Checksum Errors

When the local IS-IS receives an LSP packet, it will perform checksum check to it. By default, if the checksum in the packet is inconsistent with the calculated check sum, the LSP will be dropped. But if we set to ignore the checking error through the command **ignore-lsp-checksum-error**, this packet will be processed as a normal one even if the LSP checksum errors are found.

Perform the following configuration in IS-IS view.

Table 5-21 Configure to ignore the LSP checksum errors

Operation	Command
Configure to ignore the LSP checksum errors	**ignore-lsp-checksum-error**
Configure not to ignore the LSP checksum errors	**undo ignore-lsp-checksum-error**

By default, the LSP checksum errors will not be ignored.

5.2.18 Configuring to Log the Peer Changes

After peer changes log is enabled, the IS-IS peer changes will be output on the configuration terminal until the log is disabled.

Perform the following configuration in IS-IS view.

Table 5-22 Configure to Log the Peer Changes

Operation	Command
Enable peer changes log	**log-peer-change**
Disable peer changes log	**undo log-peer-change**

By default, the peer changes log is disabled.

5.2.19 Configuring LSP Refresh Interval

In order to ensure that the LSPs in the whole area can maintain the synchronization, all the current LSPs will be transmitted periodically.

You can customize the LSP refresh interval, with longer period for more stable networks and shorter period for less stable network.

Perform the following configuration in IS-IS view.

Table 5-23 Configure LSP refresh interval

Operation	Command
Configure LSP refresh interval	**timer lsp-refresh** *seconds*
Restore the default LSP refresh interval	**undo timer lsp-refresh**

By default, LSP is refreshed every 900 seconds (15 minutes).

5.2.20 Configuring Lifetime of LSP

When a router generates the LSP of the system, it will fill in the maximum lifetime of this LSP. When other routers receive this LSP, its life time will be reduced continuously as the time goes. If updated LSP has not been received before the old one times out, this LSP will be deleted from the LSDB.

LSP lifetime must be longer than the LSP refresh interval.

Perform the following configuration in IS-IS view.

Table 5-24 Configure lifetime of LSP

Operation	Command
Configure lifetime of LSP	**timer lsp-max-age** *seconds*
Restore the default LSP lifetime	**undo timer lsp-max-age**

By default, LSP can live for 1200 seconds (20 minutes).

5.2.21 Setting the SPF Calculation Interval

When the LSDB of IS-IS changes, the router needs to recalculate the shortest path. If the shortest path is recalculated upon each change, it will occupy a large amount of router resource and affect router efficiency. After SPF calculation interval is set, when LSDB changes, the system will wait if SPF calculation interval timer is not timeout, and SPF algorithm will not be performed until timeout.

Perform the following configuration in IS-IS view.

Table 5-25 Set the SPF calculation interval

Operation	Command
Set the SPF calculation interval	**timer spf** *second* [**level-1** | **level-2**]
Restore the default SPF calculation interval	**undo timer spf** [**level-1** | **level-2**]

If the level is not specified, it defaults to setting SPF calculation interval for Level-1.

By default, the interval of SPF recalculation is 5 seconds.

5.2.22 Setting SPF Fragmented Calculation

Where are many routing entries in a routing table (exceeding 150,000), the SPF calculation of IS-IS will occupy system resource for long time. In order to avoid this, you can divide the SPF calculation into slices.

Perform the following configuration in IS-IS view.

Table 5-26 Set SPF fragmented calculation

Operation	Command
Set SPF fragmented calculation	**spf-slice-size** *seconds*
Restore the default setting	**undo spf-slice-size**

By default, SPF calculation is not fragmented but operates to end at one time. This is also the case when the parameter *seconds* valued 0.

After fragmented calculation is set, the routes that are not processed within one operation will continue to be calculated after 1 second's waiting.

Generally, the default setting is not recommended to be changed. When there are more than 150,000 to 200,000 routes, *seconds* is recommended to be 1, that is, each SPF calculation lasts 1 second.

5.2.23 Setting SPF to Release CPU Actively

To prevent SPF calculation from occupying the system resources for a long time, which has impact on the response speed of the console, SPF can be set to automatically release the system CPU resources after processing a certain number of routes and the unprocessed routes will be calculated in one second.

Perform the following configuration in IS-IS view.

Table 5-27 Configure SPF to release CPU actively

Operation	Command
Set the interval for SPF to release CPU actively	**spf-delay-interval** *number*
Restore the default setting	**undo spf-delay-interval**

By default, CPU is released once when every 5000 routes are processed by the SPF of IS-IS.

5.2.24 Enabling/Disabling the Interface to Send Packets

To prevent the IS-IS routing information from obtaining by some router in a certain network, the **silent-interface** command can be used to prohibit sending IS-IS packets via the interface connecting with the router.

Perform the following configuration in IS-IS view.

Table 5-28 Enable/Disable the interface to send IS-IS packets

Operation	Command
Disable the interface to send IS-IS packets	**silent-interface** *silent-interface-type silent-interface-number*
Enable the interface to send IS-IS packets	**undo silent-interface** *silent-interface-type silent-interface-number*

By default, the interface is allowed to receive and send IS-IS packets.

The **silent-interface** command is only used to restrain the IS-IS packets not to be sent on the interface, but the interface routes still can be sent from other interfaces.

5.2.25 Configuring IS-IS to Redistribute Routes from Other Protocols

For IS-IS, the routes discovered by other routing protocols are processed as the routes outside the routing domain. When redistributing the routes from other protocols, you can specify the default cost for them.

When IS-IS redistributes routes, you can also specify to redistribute the routes to Level-1, Level-2 or Level-1-2.

Perform the following configuration in IS-IS view.

Table 5-29 Configure IS-IS to redistribute routes from other protocols

Operation	Command
Configure IS-IS to redistribute routes from other protocols	**import-route** *protocol* **[allow-ibgp]** [**cost** *value*] [**type** { **external** | **internal** }] [**level-1**] [**level-1-2**] [**level-2**] [**route-policy** *route-policy-name*]
Disable IS-IS to redistribute routes from other protocols	**undo import-route** *protocol* [**cost** *value*] [**type** { **external | internal** }] [**level-1**] [**level-1-2**] [**level-2**] [**route-policy** *route-policy-name*]

If the level for redistributing the route is not specified in the command, it defaults to redistribute the routes into Level-1 routing table.

protocol specifies the routing protocol sources that can be redistributed, which can be direct, static, rip, bgp, and ospf, etc.

When the *protocol* argument is set to BGP, the keyword **allow-ibgp** is optional. Whereas the **import-route bgp** command redistributes only EBGP routes, the **import-route bgp allow-ibgp** command redistributes IBGP routes in addition and as such, must be used with cautions.

By default, IS-IS does not redistribute routing information from any other protocols.

5.2.26 Configuring IS-IS Route Filtering

IS-IS protocol can filter received and redistributed routing information according to the access control list specified by *acl-number*.

Perform the following configuration in IS-IS view.

I. Configuring IS-IS to filter received routing information

Table 5-30 Configure IS-IS to filter received routing information

Operation	Command
Configure IS-IS to filter received routing information	**filter-policy** *acl-number* **import**
Disable IS-IS to filter received routing information	**undo filter-policy** *acl-number* **import**

II. Configuring IS-IS to filter redistributed routes

Table 5-31 Configure IS-IS to filter redistributed routes

Operation	Command
Configure IS-IS to filter redistributed routes	**filter-policy** *acl-number* **export** [*protocol*]
Disable IS-IS to filter redistributed routes	**undo filter-policy** *acl-number* **export** [*protocol*]

By default, IS-IS does not filter received and redistributed routing information.

The *protocol* argument specifies a routing protocol, which could be direct, static, RIP, BGP, OSPF, or OSPF-ASE.

🕮 **Note:**

- The **filter-policy import** command only filters the IS-IS routes received from neighbors, and routes that cannot pass the filter are not to be added to the routing table. This command only takes effect on Level-1-2 routers.
- The **filter-policy export** command takes effect only on the routes redistributed using the **import-route** command. If you do not configure the **import-route** command to redistribute external routes, then the configured **filter-policy export** command does not take effect.
- If no routing protocol is specified, the **filter-policy export** command applies to alll redistributed routes specified using the **import-route** command.

For more information, refer to section 7.2 "Configuring IP Routing Policy".

5.2.27 Configuring the Preference of IS-IS Protocol

In a router on which several routing protocols are concurrently operating, there is an issue of sharing and selecting the routing information among all the routing protocols. The system sets a preference for each routing protocol. When various routing protocols find the route to the same destination, the protocol with the higher preference will take effect.

Perform the following configuration in IS-IS view.

Table 5-32 Configure the preference of IS-IS protocol

Operation	Command
Configure the preference of IS-IS protocol	**preference** *value*
Restore the default preference of IS-IS protocol	**undo preference**

By default, the preference of IS-IS route is 15.

5.2.28 Configuring IS-IS Routing Leak

By virtual of IS-IS routing leak function, a Level-2 router can advertise the routing information of Level-1 areas and the Level-2 area it knows to a Level-1 router.

Perform the following configuration in IS-IS view.

Table 5-33 Configure IS-IS routing leak

Operation	Command
Enable IS-IS routing leak	**import-route isis level-2 into level-1** [**acl** *acl-number*]
Disable IS-IS routing leak	**undo import-route isis level-2 into level-1** [**acl** *acl-number*]

By default, a Level-2 router does not advertise its routing information to a Level-1 area.

5.2.29 Resetting IS-IS Data Structure

Perform the following command in user view when it is necessary to immediately refresh some LSPs.

Table 5-34 Reset All the IS-IS data structure

Operation	Command
Reset IS-IS data structure	**reset isis all**

5.2.30 Resetting the Specified IS-IS Peer

Perform the following command in user view when it is necessary to recreate a connection with a specified peer.

Table 5-35 Reset the specified IS-IS peer

Operation	Command
Reset the specified IS-IS peer	**reset isis peer** *system-id*

5.3 Displaying and Debugging Integrated IS-IS

After the above configuration, execute **display** command in all views to display the running of IS-IS configuration, and to verify the effect of the configuration. Execute **debugging** command in user view to debug the IS-IS.

Through the following operation, you can check the LSDB of IS-IS and check the sending/receiving of various IS-IS packets and SPF calculation, so as to ascertain IS-IS route maintenance.

Table 5-36 Display and debug integrated IS-IS

Operation	Command
Display the brief information of IS-IS	**display isis brief**

Operation	Command
Display LSDB of IS-IS	**display isis lsdb** [**l1**] [**l2**] [**level-1**] [**level-2**] [**local**] [**verbose**] [*LSPID*]
Display SPF calculation logs of IS-IS	**display isis spf-log**
Display IS-IS routing information	**display isis routing**
Display IS-IS peer information	**display isis peer** [**verbose**]
Display information about mesh group	**display isis mesh-group**
Enable IS-IS debugging	**debugging isis** { **adjacency** | **all** | **authentication-error** | **checksum-error** | **circuit-information** | **configuration-error** | **datalink-receiving-packet** | **datalink-sending-packet** | **general-error** | **interface-information** | **memory-allocating** | **receiving-packet-content** | **self-originate-update** | **sending-packet-content** | **snp-packet** | **spf-event** | **spf-summary** | **spf-timer** | **task-error** | **timer** | **update-packet** }
Disable IS-IS debugging	**Undo debugging isis** { **adjacency** | **all** | **authentication-error** | **checksum-error** | **circuit-information** | **configuration-error** | **datalink-receiving-packet** | **datalink-sending-packet** | **general-error** | **interface-information** | **memory-allocating** | **receiving-packet-content** | **self-originate-update** | **sending-packet-content** | **snp-packet** | **spf-event** | **spf-summary** | **spf-timer** | **task-error** | **timer** | **update-packet** }

5.4 Integrated IS-IS Configuration Example

I. Network requirements

As is shown in the following figure, Routers A, B, C and D belong to the same autonomous system. The IS-IS routing protocol is run in these four routers so as to implement route interconnection. In the network design, Routers A, B, C and D belong to the same area.

II. Network diagram

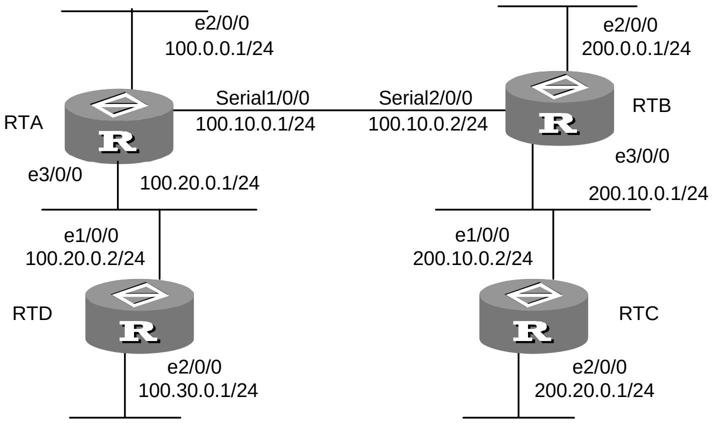


Figure 5-3 Configure IS-IS

III. Configuration procedure

# Configure RTA:

```
[RTA] isis
[RTA-isis] network-entity 86.0001.0000.0000.0005.00
[RTA] interface ethernet 2/0/0
[RTA-Ethernet2/0/0] ip address 100.0.0.1 255.255.255.0
[RTA-Ethernet2/0/0] isis enable
[RTA-Ethernet2/0/0] interface serial 1/0/0
[RTA-serial1/0/0] ip address 100.10.0.1 255.255.255.0
[RTA-serial1/0/0] isis enable
[RTA-serial1/0/0] interface ethernet 3/0/0
[RTA-ethernet 3/0/0] ip address 100.20.0.1 255.255.255.0
[RTA-ethernet 3/0/0] isis enable
```

# Configure RTB:

```
[RTB] isis
[RTB-isis] network-entity 86.0001.0000.0000.0006.00
[RTB] interface ethernet 2/0/0
[RTB-Ethernet2/0/0] ip address 200.0.0.1 255.255.255.0
[RTB-Ethernet2/0/0] isis enable
[RTB-Ethernet2/0/0] interface ethernet 3/0/0
[RTB-ethernet 3/0/0] ip address 200.10.0.1 255.255.255.0
[RTB-ethernet 3/0/0] isis enable
[RTB-ethernet 3/0/0] interface serial 2/0/0
[RTB-serial 2/0/0] ip address 100.10.0.2 255.255.255.0
[RTB-serial 2/0/0] isis enable
```

# Configure RTC:

```
[RTC] isis
[RTC-isis] network-entity 86.0001.0000.0000.0007.00
[RTC] interface ethernet 1/0/0
[RTC-Ethernet1/0/0] ip address 200.10.0.2 255.255.255.0
[RTC-Ethernet1/0/0] isis enable
[RTC-Ethernet1/0/0] interface ethernet 2/0/0
[RTC-Ethernet2/0/0] ip address 200.20.0.1 255.255.255.0
[RTC-Ethernet2/0/0] isis enable
```

# Configure RTD:

```
[RTD] isis
[RTD-isis] network-entity 86.0001.0000.0000.0008.00
[RTD] interface ethernet 1/0/0
[RTD-Ethernet1/0/0] ip address 100.20.0.2 255.255.255.0
[RTD-Ethernet1/0/0] isis enable
[RTD-Ethernet1/0/0] interface ethernet 2/0/0
[RTD-Ethernet2/0/0] ip address 100.30.0.1 255.255.255.0
[RTD-Ethernet2/0/0] isis enable
```

After the configuration, use the **display isis peer** command on each router to view the establishment of the peer relation.

Chapter 6 BGP Configuration

🕮 **Note:**

For VPN instances and VPNv4 configuration examples and parameter explanation in BGP, refer to the "Multicast" and "MPLS" modules of this manual.

6.1 BGP Overview

Border Gateway Protocol (BGP) is a dynamic inter-AS route discovery protocol.

Three early versions of BGP are BGP-1 (RFC1105), BGP-2 (RFC1163) and BGP-3 (RFC1267). The current version in use is BGP-4 (RFC1771). BGP-4 applies to distributed structure and supports CIDR. BGP also helps to implement user-configured policies. BGP-4 is rapidly becoming the defacto Internet exterior routing protocol standard and is commonly used between ISPs.

The characteristics of BGP are as follows:

- BGP is an external routing protocol. Different from internal routing protocols such as OSPF and RIP, it focuses on the control of route propagation and the selection of optimal routes rather than the discovery and calculation of routes.
- Eliminating routing loops completely by adding AS path information to BGP routes.
- Using TCP as its transport layer protocol so as to enhance its reliability.
- BGP-4 supports CIDR, which is a major improvement over BGP-3. With a brand-new perspective of IP address, networks are no longer distinguished as Class-A networks, Class-B networks, or Class-C networks in CIDR. For example, by means of CIDR notation, an illegal Class-C network address 192.213.0.0 (255.255.0.0) turns into 192.213.0.0/16, a legal super network address, wherein the “/16” indicates that the subnet mask is composed of 16 bits starting from the left most bit of the address. The introduction of CIDR simplifies route aggregation. Actually, route aggregation is the process of aggregating several different routes, which turns advertisement processes of several routes into the advertisement of single route so as to reduce the size of the routing tables.
- When routes are updated, BGP only advertises updated routes, which greatly reduces bandwidth occupation. It applies to advertising a great amount of routing information on the Internet.
- In consideration of management and security, users desire to perform control over outgoing and incoming routing information of each AS. BGP-4 provides abundant

routing policies, allowing implementing flexible filtering and route selection and being extended easily to support new developments of the networks.

BGP runs on a special router as an upper-layer protocol. On the initial startup of the BGP system, the BGP router exchanges routing information with its peers by advertising the full BGP routing table, and after that only update messages are exchanged. While in operation, the system sends and receives keep-alive messages to check the correctness of the connections between peers.

A router advertising BGP messages is called a BGP speaker. It receives and generates new routing information continuously and advertises the information to the other BGP speakers. When a BGP speaker receives a new route advertisement from another AS, it will advertise the route, if the route is better than the current route that has been learned or is a new route, to all the other BGP speakers in the AS. A BGP speaker calls other BGP speakers peers that exchange information with it, and multiple related peers form a peer group.

BGP runs on a router in one of the following two modes:

- IBGP (Interior BGP)
- EBGP (External BGP)

The BGP is called IBGP when it runs within an AS and is called EBGP when it runs between ASs.

The operation of BGP is driven by messages of the following four types:

- Open message
- Update message
- Notification message
- Keep-alive message

The open message is the first message sent after a connection is created; it is used to create the connection relationship between BGP peers. The notification message is used to notify errors. The keep-alive message is used to check the validity of a connection. The update message is the most important information in a BGP system, which is used to exchange routing information between peers. It is composed of up to three parts: unreachable route, path attributes and network layer reach/reachable information (NLRI).

6.2 BGP Configuration

The BGP configuration includes:

- Enable BGP
- Configure the network routes for BGP to advertise
- Configure a BGP peer/peer group
- Configure BGP timer
- Configure the local preference
- Configure MED for AS

- Compare MED Routing Costs from the Peers in Different ASs
- Configure BGP community
- Configure BGP route aggregation
- Configure the BGP preference
- Configure BGP route reflector
- Configure BGP AS confederation attribute
- Configure BGP route dampening
- Configure the interaction between BGP and IGP
- Configure BGP route filtering
- Define ACL, AS path list and route-policy
- Reset BGP connection
- Configure BGP load balancing

6.2.1 Enabling BGP

To enable BGP, you must specify the local AS number. After BGP is enabled, the local router listens to BGP connection requests from adjacent routers. To make the local router send BGP connection requests to adjacent routers, refer to the **peer** command. When BGP is disabled, all established BGP connections are disconnected.

Perform the following configuration in system view.

Table 6-1 Enable/disable BGP

Operation	Command
Enable BGP and enter the BGP view	**bgp** *as-number*
Disable BGP	**undo bgp** [*as-number*]

By default, BGP is disabled.

6.2.2 Configuring the Network Routes for BGP to Advertise

Perform the following configuration in BGP view.

Table 6-2 Configure the network routes for BGP to advertise

Operation	Command
Configure the network routes for BGP to advertise	**network** *ip-address address-mask* [**route-policy** *route-policy-name*]
Cancel the network routes for BGP to advertise	**undo network** *ip-address address-mask* [**route-policy** *route-policy-name*]

By default, no network route is advertised by the local BGP system.

6.2.3 Configuring a BGP Peer/Peer Group

The BGP speakers who exchange BGP packets form peer relationship. A BGP peer cannot exist independently from its peer group. In other words, a peer must belong to a specific peer group. To configure a BGP peer, you must first configure a peer group and then add the peer into the peer group.

In case of any change in the configuration of the group, the configuration of each group member changes accordingly. However, you may configure certain attributes for a certain member by designating its IP address, making the member not affected by the group configuration in terms of these attributes.

Perform the following configuration in BGP view.

I. Configuring a peer group

Before configuring a BGP peer, you must first configure the peer group that the peer belongs to.

Table 6-3 Configure a peer group

Operation	Command
Create a peer group	**group** *group-name* [**internal**] **| external**
Delete the specified peer group	**Undo group** *group-name*

When configuring a peer group, you need to specify the type of the peer group. All members of an internal peer group are IBGP peers; while members of an external peer group are EBGP peers or confederation EBGP peers.

By default, a peer group is internal.

II. Specifying the AS number of a peer group

You can specify an AS number for an external peer group. An internal peer group do not need to be configured with an AS number. After a peer group is configured with an AS number, all peers added into the peer group inherit the AS number of the peer group.

Table 6-4 Specify an AS number for a peer group

Operation	Command
Specify an AS number for a peer group	**peer** *group-name* **as-number** *as-number*
Delete the specified AS number of the peer group	**undo peer** *group-name* **as-number** *as-number*

You cannot specify an AS number for a peer group with members. When the AS number of a peer group is deleted, all peers in the peer group also are deleted.

III. Adding a peer into a peer group

A BGP peer cannot exist independently from its peer group. Therefore, to configure a peer, you must specify the peer group it belongs to. You can also specify its AS number at the same time.

Table 6-5 Add a peer into a peer group

Operation	Command
Create a peer in a peer group	**peer** *peer-address* **group** *group-name* [**as-number** *as-number*]
Delete a peer from a peer group	**undo peer** *peer-address* **group**

In the case of an internal peer group, you cannot specify the AS number, and the added peer is an IBGP peer.

In the case of an external peer group, if it is not specified with an AS number, you must specify an AS number for the peer to be added into it; if it has been configured with an AS number, the peer will inherit its AS number and no AS number is necessary to be specified for the peer.

IV. Configuring a description for a peer/peer group

In order to help understand the characteristics of a peer/peer group, you can configure a description for the peer/peer group.

Table 6-6 Configure a description for a peer/peer group

Operation	Command
Configure a description for a peer/peer group	**peer** { *peer-address* | *group-name* } **description** *description-line*
Delete the description of a peer/peer group	**undo peer** { *peer-address* | *group-name* } **description**

By default, no BGP peer/peer group description is set.

V. Connecting with EBGP peer groups on indirectly connected networks

Generally, EBGP peers must be connected physically, or the command below can be used to perform the configuration.

Table 6-7 Connect with EBGP peer groups on indirectly connected networks

Operation	Command
Configure to permit connections with EBGP peer groups on indirectly connected networks	**peer** *group-name* **ebgp-max-hop** [*ttl*]
Configure to permit connections with EBGP peer groups on directly connected networks only	**undo peer** *group-name* **ebgp-max-hop**

By default, it is only permitted to establish connections with peer groups on directly connected networks. *ttl* represents the maximum hop count, ranging from 1 to 255. By default, it is 64.

VI. Configuring the timer of a specified peer/peer group

The **peer timer** command is used to configure the timer of a specified BGP peer/peer group, including the keep-alive message interval and the hold timer. The preference of this command is higher than the **timer** command that is used to configure timers for all the BGP peers.

Table 6-8 Configure the timer of a peer/peer group

Operation	Command
Configure the keep-alive interval and hold timer of a specified peer/peer group	**peer** { *group-name* | *peer-address* } **timer keep-alive** *keepalive-interval* **hold** *holdtime-interval*
Restore the default keep-alive interval and hold timer of a specified peer/peer group	**undo peer** { *group-name* | *peer-address* } **timer**

By default, the keep-alive message is sent every 60 seconds and the value of the hold timer is 180 seconds.

VII. Configuring the interval at which route updates are sent by a peer group

Table 6-9 Configure the interval at which route updates are sent by a peer group

Operation	Command
Configure the interval at which route updates are sent by a peer group	**peer** *group-name* **route-update-interval** *seconds*
Restore the default route update sending interval of a peer group	**undo peer** *group-name* **route-update-interval**

By default, the intervals at which route updates are sent by an IBGP and EBGP peer group are 5 seconds and 30 seconds respectively.

VIII. Configuring to send community attributes to a peer group

Table 6-10 Configure to send community attributes to a peer group

Operation	Command
Configure to send community attributes to a peer group	**peer** *group-name* **advertise-community**
Not to send community attributes to a peer group	**undo peer** *group-name* **advertise-community**

IX. Configuring a peer group to be a route reflector client

Table 6-11 Configure a peer group to be a route reflector client

Operation	Command
Configure a peer group to be a route reflector client	**peer** *group-name* **reflect-client**
Disable a peer group from being a route reflector client	**undo peer** *group-name* **reflect-client**

Only internal peer groups can be configured to be a reflector client.

By default, all IBGP peers in the AS are fully-connected and do not mutually notify IBGP routes learned so as to avoid creating routing loops.

For detailed information on route reflector, refer to "Configure Route Reflector" section of this manual.

X. Configuring to send the default route to a peer group

Table 6-12 Configure to send the default route to a peer group

Operation	Command
Configure to send the default route to a peer group	**peer** *group-name* **default-route-advertise**
Disable sending of the default route to a peer group	**undo peer** *group-name* **default-route-advertise**

By default, the local router does not send the default route to any peer group. This command does not require that the default route exist in the BGP routing table. Rather, it unconditionally sends a default route with the next-hop being itself to the peer.

XI. Configuring to take the local address as the next-hop in advertising route

A BGP router can specify itself as the next hop while advertising a route to a peer group.

Table 6-13 Configure to take the local address as the next-hop in advertising a route

Operation	Command
Configure itself as the next hop in advertising a route	**peer** *group-name* **next-hop-local**
Disable itself from being the next hop in advertising a route	**undo peer** *group-name* **next-hop-local**

By default, the local router does not take its address as the next-hop, when it advertises route to a peer group.

Note: If BGP load balancing is configured, no matter the **peer next-hop-local** command is configured or not, the local router will take its address as the next-hop when it advertises a route to an IBGP peer group.

XII. Configuring not to carry private AS numbers inforwarding BGP updates

Generally speaking, BGP carries AS numbers (either public or private) when it forwards BGP updates. In order for some egress routers to ignore private AS numbers while sending updates, you can configure to make them carry no private AS numbers when forwarding BGP updates.

Table 6-14 Configure not to carry private AS numbers in forwarding BGP updates

Operation	Command
Configure not to carry private AS numbers in forwarding BGP updates	**peer** *group-name* **public-as-only**
Configure to carry private AS number in forwarding BGP updates	**undo peer** *group-name* **public-as-only**

By default, AS numbers are carried when BGP updates are forwarded.

XIII. Specifying the source interface for route updates

For updates to be forwarded in case the interface for them experiences a failure, you can configure to enable the internal BGP session to use any interface on which a TCP connection can be established with the peer. The Loopback interface is usually used for the purpose.

Table 6-15 Specify the source interface for route updates

Operation	Command
Specify the source interface for route updates	**peer** { *group-name* | *peer-address* } **connect-interface** *interface-type interface-number*

Operation	Command
Restore to use the optimal source interface for route updates	**undo peer** { *group-name* | *peer-address* } **connect-interface** *interface-type interface-number*

By default, BGP employs the optimal source interface for route updates.

XIV. Enabling/disabling a peer/peer group

A BGP speaker does not exchange routing information with a disabled peer or peer group.

Table 6-16 Enable/disable a peer/peer group

Operation	Command
Enable a peer/peer group	**peer** { *group-name* | *peer-address* } **enable**
Disable a peer/peer group	**undo peer** { *group-name* | *peer-address* } **enable**

By default, a peer or peer group is enabled.

XV. Enabling MD5 authentication for BGP

TCP connections are necessary for BGP peers/peer groups. To improve BGP security, you can configure BGP to perform MD5 authentication before setting up a TCP connection. A TCP connection will not be set up unless the authentication succeeds. The MD5 authentication does not authenticate BGP packets; it only sets an MD5 authentication password for the TCP connection. The authentication is carried out by TCP.

Table 6-17 Enable MD5 authentication for BGP

Operation	Command
Enable MD5 authentication for a BGP peer (group)	**peer** { *group-name* | *peer-address* } **password** { **cipher** | **simple** } *password*
Disable MD5 authentication	**undo peer** { *group-name* | *peer-address* } **password**

By default, MD5 authentication is disabled.

The MD5 authentication command can be configured in either BGP view or MBGP VPN-instance address family view. When configured in the BGP view, this command is also in effect for MBGP multicast expansion and MBGP VPN expansion because all of them share the same TCP connection.

XVI. Disabling a BGP peer/peer group to initiate or receive BGP connection

Perform the following configuration in BGP view or VPN instance view.

Table 6-18 Disable a BGP peer/peer group to initiate or receive BGP connection

Operation	Command
Disable the specified BGP peer/peer group to initiate or receive BGP connection	**peer** { *group-name* | *peer-address* } **shutdown**
Restore the default	**undo peer** {*group-name* | *peer-address* } **shutdown**

By default, the BGP peer/peer group is allowed to initiate and receive BGP connection.

6.2.4 Configuring Routing Policy for BGP Peer/Peer Group

Perform the following configuration in BGP view.

I. Configuring a routing policy

The peers in a peer group must use the same outbound route update policy as the peer group, but they can have different inbound policies. In other words, when advertising routes, a peer group follows the same policy; when receiving routes, each peer in the group can choose its own policy.

Table 6-19 Configure a routing policy for a peer/peer group

Operation	Command
Configure to apply a routing policy to routes received from a peer/peer group	**peer** { *group-name* | *peer-address* } **route-policy** *policy-name* **import**
Cancel the routing policy applied to routes received from a peer/peer group	**undo peer** { *group-name* | *peer-address* } **route-policy** *policy-name* **import**
Configure to apply a routing policy to routes advertised to a peer/peer group	**peer** *group-name* **route-policy** *policy-name* **export**
Cancel the routing policy applied to routes advertised to a peer/peer group	**undo peer** *group-name* **route-policy** *policy-name* **export**

By default, no routing policy is applied to routes advertised or received.

II. Configuring a route filtering policy based on IP ACL

Table 6-20 Configure a route filtering policy based on IP ACL

Operation	Command
Configure to apply an IP ACL-based route filtering policy to routes received from a peer/peer group	**peer** { *group-name* | *peer-address* } **filter-policy** *acl-number* **import**
Cancel the IP ACL-based route filtering policy applied to routes received from a peer/peer group	**undo peer** { *group-name* | *peer-address* } **filter-policy** *acl-number* **import**
Configure to apply an IP ACL-based route filtering policy to routes advertised to a peer group	**peer** *group-name* **filter-policy** *acl-number* **export**
Cancel the IP ACL-based route filtering policy applied to routes advertised to a peer/peer group	**undo peer** *group-name* **filter-policy** *acl-number* **export**

By default, no route filtering policy based on IP ACL is applied to routes advertised or received.

III. Configuring a route filtering policy based on AS path ACL

Table 6-21 Configure a route filtering policy based on AS path ACL

Operation	Command
Configure to apply an AS path ACL-based route filtering policy to routes received from a peer/peer group	**peer** { *group-name* | *peer-address* } **as-path-acl** *number* **import**
Cancel the AS path ACL-based route filtering policy applied to routes received from a peer/peer group	**undo peer** { *group-name* | *peer-address* } **as-path-acl** *number* **import**
Configure to apply an AS path ACL-based route filtering policy to routes advertised to a peer group	**peer** *group-name* **as-path-acl** *number* **export**
Cancel the AS path ACL-based route filtering policy applied to routes advertised to a peer/peer group	**undo peer** *group-name* **as-path-acl** *number* **export**

By default, no route filtering policy based on AS path ACL is applied to routes advertised or received.

IV. Configuring a route filtering policy based on address prefixes

Table 6-22 Configure a route filtering policy based on address prefixes

Operation	Command
Configure to apply an address prefixes-based route filtering policy to routes received from a peer/peer group	**peer** { *group-name* | *peer-address* } **ip-prefix** *prefixname* { **import** | **export** }
Cancel the address prefixes-based route filtering policy applied to routes received from a peer/peer group	**undo peer** { *group-name* | *peer-address* } **ip-prefix** *prefixname* { **import** | **export** }
Configure to apply an address prefixes-based route filtering policy to routes advertised to a peer group	**peer group-name ip-prefix prefixname export**
Cancel the address prefixes-based route filtering policy applied to routes advertised to a peer/peer group	**undo peer group-name ip-prefix prefixname export**

By default, no route filtering policy based on address prefixes is applied to routes advertised or received.

6.2.5 Removing the Route Synchronization between IGP and IBGP

Perform the following configuration in BGP view and VPN instance view.

Table 6-23 Removing the route synchronization between IGP and IBGP

Operation	Command
Removing the route synchronization between IGP and IBGP	**undo synchronization**

6.2.6 Configuring BGP Timers

After a BGP connection is established between peers, each peer periodically sends Keepalive message to the other so as to avoid the routers from assuming that the BGP connection is down. If a router does not receive any Keepalive message or any kind of packet from the peer within the specified Holdtime, it assumes that the BGP connection is down and processes the routes received from the BGP connection accordingly. Therefore, the interval for sending a Keepalive message and the BGP connection Holdtime are two important parameters in BGP mechanism.

When a BGP router tries to establish a BGP connection with its peer, a negotiation needs to be carried out on the Holdtime. The resulting Holdtime is the smaller one those for the peers. If the resulting Holdtime is 0, no keepalive message will be transmitted and no detection on whether the Holdtime is timed out will be performed.

Perform the following configuration in BGP view.

Table 6-24 Configure BGP timers

Operation	Command
Configure BGP timers	**timer keepalive** *keepalive-interval* **hold** *holdtime-interval*
Restore the default values of the timers	**undo timer**

The reasonable maximum interval for sending keepalive messages is one third of the Holdtime and must not be less than 1 second. Thus, if the Holdtime is not configured as 0, it is 3 seconds at least.

By default, the interval for sending keepalive messages is 60 seconds and the Holdtime is 180 seconds.

6.2.7 Configuring the Local Preference Attribute

Different local preferences can be configured to affect the BGP routing. When a router running BGP gets routes with the same destination address but different next hops through different internal peers, it selects the route with the highest local preference.

Perform the following configuration in BGP view.

Table 6-25 Configure the local preference attribute

Operation	Command
Configure the local preference attribute	**default local-preference** *value*
Restore the default local preference value	**undo default local-preference**

The local preference attribute is transmitted only when IBGP peers exchange update packets and is not transmitted beyond the local AS.

By default, the local preference is 100.

The configured default local preference does not take effect on the BGP routes received and sent before the change is made. To have the new setting take effect on all BGP routes, you must perform the **reset bgp all** command or reboot the system.

6.2.8 Configuring the MED Attribute for an AS

The multi-exit discriminator (MED) attribute is the external routing cost of the routes. They are exchanged among ASs. However, a MED entering an AS will no longer be sent out of the AS.

Local preference is used to select the route for going out of an AS; while the MED attribute is used to judge the optimal route for entering an AS. When a BGP router receives multiple routes with the same destination address but different next-hops from different external peers, it will opt for the one with the smallest MED value as its optimal route under the premise that the other conditions are the same.

Perform the following configuration in BGP view.

Table 6-26 Configure an MED for the system

Operation	Command
Configure a MED for the system	**default med** *med-value*
Restore the default MED of the system	**undo default med**

A router configured with the **default med** command compares only the MED values of routes from different EBGP peers in the same AS. If you hope to compare the MED values of routes from different EBGP peers in different ASs, use the **compare-different-as-med** command.

By default, the value of the MED attribute is 0.

6.2.9 Comparing the MED Values of Routes from Peers in Different ASs

It is used to select the optimal route. When the other conditions are the same, the route with the smallest MED value will be selected as the outgoing route of the AS.

Perform the following configuration in BGP view.

Table 6-27 Compare the MED values of routes from peers in different ASs

Operation	Command
Compare the MED values of routes from peers in different ASs	**compare-different-as-med**
Disable the comparison of the MED values of routes from peers in different ASs	**Undo compare-different-as-med**

By default, it is not allowed to compare the MED values of routes from peers in different ASs.

You are not recommended to use this configuration unless you are sure that the ASs are using the same IGP protocol and the same routing method.

6.2.10 Configuring the BGP Community Attributes

The community attributes are optional and transitional. Some of them are accepted all around the world, called as standard community attributes; others are used for special purposes. You can also define extended community attributes.

Community lists, including standard-community-lists and extended-community-lists, are lists identifying information of communities.

In addition, a route can have more than one community attributes. The speakers of multiple community attributes of a route can act according to one, several or all the attributes. A router can choose to change the community attributes or leave them unchanged before advertising the route to its peers.

Perform the following configuration in system view.

Table 6-28 Configure the community attributes

Operation	Command
Configure a standard-community-list	**ip community-list** *standard-community-list-number* { **permit** | **deny** } { *aa:nn* | **internet** | **no-export-subconfed** | **no-advertise** | **no-export** }
Configure an extended-community-list	**ip community-list** *extended-community-list-number* { **permit | deny** } *as-regular-expression*
Remove the configured community list	**undo ip community-list** { *standard-community-list-number* | *extended-community-list-number* }

By default, no BGP community attribute is configured.

The *standard-community-list-number* argument takes a value in the range 1 to 99; the *extended-community-list-number* argument takes a value in the range 100 to 199.

6.2.11 Configuring BGP Route Aggregation

BGP supports Classless Inter-Domain Routing (CIDR) and route aggregation. There are two modes of BGP route aggregation: **summary** and **aggregate**. The former is to aggregate the IGP subnet routes redistributed by BGP. After **summary** is configured, BGP cannot receive subnet routes redistributed from IGP. The **aggregate** mode is to aggregate the local BGP routes. A series of parameters can be configured in the **aggregate** mode. In general, the preference of the **aggregate** mode is higher than that of the **summary** mode.

Perform the following configuration in BGP view.

Table 6-29 Configure BGP route aggregation

Operation	Command
Configure the subnet routes automatic summary function	**summary**
Cancel the subnet routes automatic summary function	**undo summary**
Configure the local route aggregation function	**aggregate** *address mask* [**as-set**] [**detail-suppressed**] [**suppress-policy** *route-policy-name*] [**origin-policy** *route-policy-name*] [**attribute-policy** *route-policy-name*]
Cancel the local route aggregation function	**undo aggregate** *address mask* [**as-set**] [**detail-suppressed**] [**suppress-policy** *route-policy-name*] [**origin-policy** *route-policy-name*] **attribute-policy** *route-policy-name*]*policy-name*] [**attribute-policy** *policy-name*]

By default, BGP does not aggregate subnet routes and local routes.

6.2.12 Configuring the BGP Preference

Each routing protocol has its own preference, by which the routing policy will select the optimal one from the routes of different protocols. The greater the preference value is, the lower the preference becomes. BGP has three kinds of routes: routes learned from external peers, routes learned from internal peers, and the local routes. You can manually set BGP preferences for these three kinds of routes respectively.

Different sub-address families can be set with different BGP preferences. Both unicast address family and multicast address family are supported currently.

Perform the following configuration in BGP view or BGP multicast address family view.

Table 6-30 Configure the BGP preference

Operation	Command
Configure the BGP preference	**preference** *value1 value2 value3*
Restore the default preference values	**undo preference**

Where *value1* is for routes learned from EBGP peers, *value2* is for routes learned from IBGP peers, and *value3* is for local routes. They can be in the range 1 to 256.

By default, *value1*, *value2*, *value3* are 256, 256, and 130 respectively.

6.2.13 Configuring the BGP Route Reflector

To ensure the connectivity between IBGP peers, it is necessary to establish a fully connected network. In some networks, there are large numbers of IBGP peers, and the internal BGP networks become very large, consequently, the cost to establish a fully meshed network is very high. Thus, it is required to utilize new peer technology. The basic idea behind the route reflector conception is to specify a centralized router as the focus of the internal sessions. Multiple BGP routers can peer one central point, and then multiple route reflectors will peer again.

The route reflector is the centralized point of other routers, and other routers are called the clients. A client and the route reflector are peers. They exchange routing information with each other. The route reflector transfers (reflect) information among clients in turn.

In the following figure, Router A receives an update message from an external peer and transmits it to Router C. Router C is configured as the route reflector, with two clients, Router A and Router B.

Router C reflects the update message from the client Router A to the client Router B. Under this configuration, no peer session between Router A and Router B is virtually needed because the router reflector will transmit the BGP information to Router B.

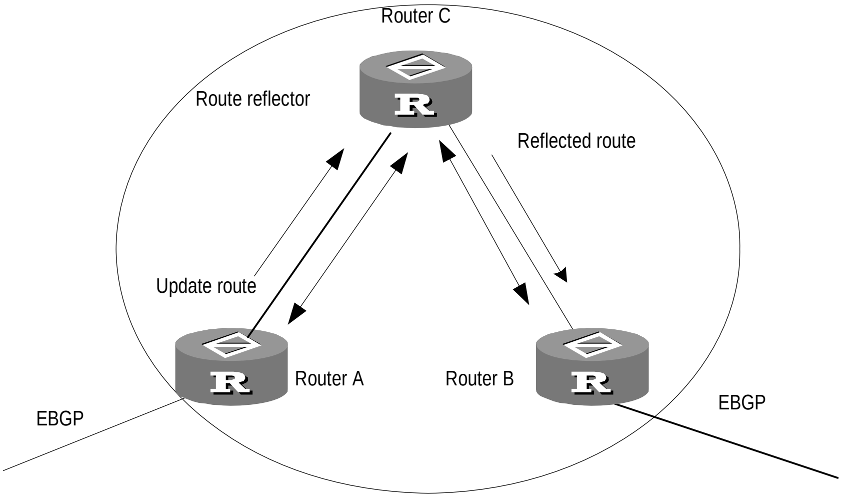


Figure 6-1 Route reflector

A reflector is a router that performs the route reflection function. Its peers fall into two categories: clients and non-clients. A route reflector and its clients constitute a cluster, while all other peers in the AS, not belonging to the cluster, are non-clients. Use the **peer reflect-client** command to specify the route reflector and add its clients.

The non-client peers and the route reflector must forms a fully connected network because they have to follow the basic IBGP peer connectivity principle. A client can not form peer relationship with any IBGP router outside its cluster. The route reflection function is implemented by the route reflector, and all its client peers and non-client peers are regular BGP peers that have no relation to the reflection function. The client peers are clients just because the route reflector regards them as clients.

I. Configuring route reflection between clients

Perform the following configuration in BGP view.

Table 6-31 Configure route reflection between clients

Operation	Command
Enable route reflection between clients	**reflect between-clients**
Disable route reflection between clients	**undo reflect between-clients**

By default, route reflection between clients is enabled.

II. Configuring the route reflector

Generally speaking, there is a route reflector in a cluster, whose ID identifies the cluster.

Perform the following configuration in BGP view.

Table 6-32 Configure the cluster ID of the route reflector

Operation	Command
Configure the cluster ID of the route reflector	**reflector cluster-id** { *cluster-id* | *address* }
Cancel the cluster ID of the route reflector	**undo reflector cluster-id**

III. Two measures to avoid loops inside an AS

With the introduction of the route reflector, routing loops might occur in the AS. An update message originated from the cluster may attempt to return to the cluster. The conventional AS path method cannot detect an internal loop in the AS because the update message has not left the AS. With a route reflector configured, you can use the following measures to avoid internal loops in the AS:

1) Configuring the Originator_ID of the route reflector

If the Originator_ID is wrongly configured, the update message will be returned to the originator, and the originator will discard it.

This parameter needs no manual configuration, and it is enabled automatically with BGP.

2) Configuring the Cluster_ID of the route reflector

6.2.14 Configuring BGP AS Confederation Attribute

Confederation provides another solution to handle the booming IBGP network connections inside an AS. It divides an AS into multiple sub-ASs, with the IBGP peers inside each sub-AS fully connected and connecting to other sub-ASs in the confederation.

The shortcomings of confederation lie in: it is required that the router be reconfigured upon switching from non-confederation to confederation solution, and that the logic topology be basically changed. Furthermore, the path selected via confederation may not be the best path if there is no manually-set BGP policy.

I. Configuring confederation ID

In the sight of the BGP speakers that are not included in the confederation, multiple sub-ASs that belong to the same confederation are a whole. The external network does not need to know the status of internal sub-ASs, and the confederation ID is the AS number identifying the confederation as a whole.

Perform the following configuration in BGP view.

Table 6-33 Configure confederation ID

Operation	Command
Configure confederation ID	**confederation id** *as-number*
Cancel confederation ID	**undo confederation id**

By default, the confederation ID is not configured.

The configured confederation ID cannot be the same as the existing AS number of a peer or a peer group.

II. Configuring the sub-ASs belonging to a confederation

Configure confederation ID first, and then configure the sub-AS belonging to the confederation. One confederation includes up to 32 sub-ASs. The *as-number* used upon configuring sub-AS belonging to the confederation is valid within the confederation.

Perform the following configuration in BGP view.

Table 6-34 Configure the sub-ASs belonging to a confederation

Operation	Command
Configure the sub-ASs belonging to a confederation	**confederation peer-as** *as-number-1* [... *as-number-n*]
Cancel the specified sub-AS in the confederation	**undo confederation peer-as** [*as-number-1*] [*...as-number-n*]

By default, no sub-AS is configured as a member of the confederation.

The configured confederation sub-AS number cannot be the same as the AS number of a certain peer who is not configured with peer group AS number.

III. Configuring AS confederation attribute compatible with nonstandard router

If it is necessary to interwork with routers whose implementation mechanisms are different from RFC1965, you should configure all these routers in the confederation.

Perform the following configuration in BGP view.

Table 6-35 Configure AS confederation attribute compatible with nonstandard router

Operation	Command
Configure AS confederation attribute compatible with nonstandard router	**confederation nonstandard**
Cancel AS confederation attribute compatible with nonstandard router	**undo confederation nonstandard**

By default, the configured confederation complies with RFC1965.

6.2.15 Configuring BGP Route Dampening

The main possible reason for unstable route is the intermittent disappearance and reemergence of the route that formerly existed in the routing table. This situation is called the flapping. When flapping occurs, update packet will be propagated on the network repeatedly, which will occupy much bandwidth and much processing time of the router. We have to find measures to avoid it. The technology controlling unstable route is called route dampening.

The dampening divides the route into the stable route and unstable route, the latter of which shall be suppressed (not to be advertised). The history performance of the route is the basis to evaluate the future stability. When the route flapping occurs, penalty will be given, and when the penalty reaches a specific threshold, the route will be suppressed. With time going, the penalty value will decrease according to power function, and when it decreases to certain specific threshold, the route suppression will be eliminated and the route will be re-advertised.

Perform the following configuration in BGP view.

Table 6-36 Configure BGP route dampening

Operation	Command
Configure BGP route dampening	**dampening** [*half-life-reachable half-life-unreachable reuse suppress ceiling*] [**route-policy** *route-policy-name*]
Clear route dampening information and eliminating the suppression of the route	**reset dampening** [*network-address* [*mask*]]
Cancel BGP route dampening	**undo dampening**

By default, BGP route dampening is not configured.

It must be noted that the parameters in the command are interdependent. If one parameter is configured, other parameters must be specified.

The **dampening** command dampens only the routes that are learned from EBGP peers but not the IBGP routes.

6.2.16 Configuring the Interaction between BGP and IGP

BGP can transmit the internal network information of local AS to other AS. To achieve the purpose, the network information about the internal system discovered by the local router via IGP routing protocol can be transmitted.

Perform the following configuration in BGP view.

Table 6-37 Redistribute IGP routing information

Operation	Command
Configure BGP to redistribute IGP routing information	**import-route** *protocol* [*process-id*] [**med** *med*] [**route-policy** *route-policy-name*]
Disable BGP from redistributing IGP routing information	**undo import-route** *protocol*
Redistribute the local default routes.	**default-route imported**
Disable BGP from redistributing the local default routes.	**undo default-route imported**

By default, BGP does not redistribute the route information of other protocol.

The specified and redistributed source route protocols can be direct, static, rip, isis, ospf, ospf-ase, and ospf-nssa.

For detailed description of routing information, refer to "Redistributing other Protocol Route" in "IP Route Policy Configuration".

6.2.17 Configuring the Repeating Times of Local AS Number

This command can be used to configure the repeating times of local AS number.

Perform the following configuration in BGP view, VPNv4 view and VPN instance view.

Table 6-38 Configure the repeating times of AS-path

Operation	Command
Configure the repeating times of local AS number	**peer** { *group-name* | *peer-address* } **allow-as-loop** [*number*]
Remove the repeating times of local AS number	**undo peer** { *group-name* | *peer-address* } **allow-as-loop**

By default, the value of the *number* argument is 3.

6.2.18 Defining ACL, AS Path List, and route-policy

ACL, AS path list, and route-policy can all be the conditions for BGP filtering.

I. Defining the ACL

Refer to "Firewall Configuration" in module "Security" of this manual.

II. Defining the AS path list

The routing information packet of the BGP includes an autonomous system path domain. The **as-path-acl** can be used to match with the autonomous system path domain of the BGP routing information so as to filter the routing information, which does not conform to the requirements. For the same list number, the user can define multiple pieces of **as-path-acl**. In other words, a list number stands for a group of AS path ACLs. Each AS path list is identified with digits.

Perform the following configuration in system view.

Table 6-39 Configure regular expression of an AS

Operation	Command
Configure regular expression of an AS	**ip as-path-acl** *aspath-acl-number* { **permit | deny** } *as-regular-expression*
Remove the configured regular expression	**undo ip as-path-acl** *aspath-acl-number*

By default, no AS regular expression is defined.

During the matching, the relationship of F "Or" is available between the members (*acl-number*) of the ACLs, i.e., when the routing information passes through one piece of this group of lists, it means that the routing information has been filtered by this group of as-path lists identified with this list number.

III. Defining a route-policy

Step 1: For route-policy definition, refer to the "Define the Routing Policy" part of the "IP Routing Policy Configuration".

Step 2: For match-rule definition, refer to the "Define If-match Clause of route-policy" part in the "IP Routing Policy Configuration".

Step 3: For definition of evaluation rules, refer to the "Define Apply Clause of route-policy" part in the "IP Routing Policy Configuration".

6.2.19 Configuring BGP Route Filtering

I. Configuring BGP to filter the received routes

Perform the following configuration in BGP view.

The routes received by the BGP can be filtered, and only those routes that meet the certain conditions will be received by the BGP.

Table 6-40 Configure to filter the redistributed routes

Operation	Command
Configure to filter the redistributed routes	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] } **import**
Cancel the filtering of the redistributed routes	**undo filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] } **import**

For more details, please refer to the "Configure Route Filtering" part in the "IP Routing Policy Configuration".

II. Configuring BGP to filter the routes to be advertised

The routes advertised by BGP can be filtered, and only those routes that meet certain conditions will be advertised by BGP.

Perform the following configuration in BGP view.

Table 6-41 Configure to filter the routes to be advertised by BGP

Operation	Command
Configure to filter the routes to be advertised by BGP	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol*]

Operation	Command
Cancel the filtering of the routes to be advertised by BGP	**undo filter-policy** *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol*]

By default, BGP does not filter received and advertised routing information.

To have BGP filter the routes redistributed from a particular routing protocol, specify the *protocol* argument, which can take the value of direct, static, RIP, IS-IS, OSPF, OSPF-ASE or OSPF-NSSA.

For more information, refer to the "Configure Route Filtering" part in "IP Routing Policy Configuration".

6.2.20 Configuring BGP Load Balancing

The load balancing implementations of BGP and IGP are different:

- IGP calculates metrics for different routes to the same destination address according to its route algorithm and perform load balancing between routes with identical metrics.
- BGP cannot determine whether to perform load balancing based on an explicit metric since it has no route algorithm. However, it can select routes to implement load balancing depending on its abundant routing rules, that is, it adds load balancing into its routing rules.

V 2.41 supports BGP load balancing. When BGP load balancing is configured, upon BGP route selection, a rule is added between the last two routing rules “Select routes learned from EBGP first” and “Select routes advertised by the routers with lowest BGP ID first”. That is, if load balancing is configured and there are multiple external routes heading for the same AS or AS confederation, BGP will select multiple routes for load balancing.

The implementation of BGP load balancing follows these rules:

- The participating routes must be those redistributed from EBGP.
- These routes must come from the same AS and have the same metric value.
- These routes must have the same AS_PATH property and origin property (IGP, EGP, or INC).

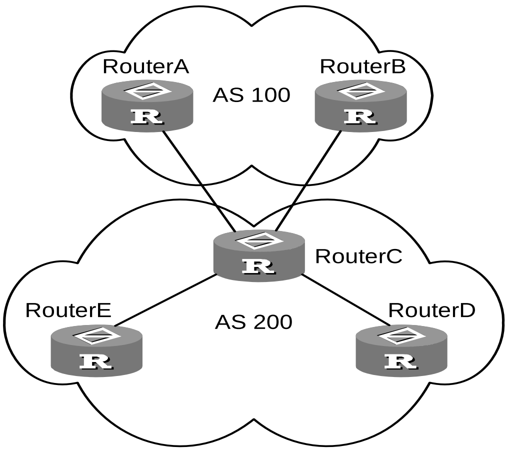


Figure 6-2 BGP load balancing

In the above figure, Router D and Router E are IBGP peers of Router C. When Router A and Router B advertise routes heading for the same destination to Router C simultaneously, if the user configures load balancing (such as balance 2) on Router C, Router C will add the received two routes into the forward table for BGP load balancing as long as the two route satisfy certain routing rules and they have the same AS_PATH attribute. Router C only transmits the route once to Router D and Router E, with the same AS_PATH, but a NEXT_HOP changed into Router C address rather than the original EBGP peer address. Other BGP transitional attributes will be transmitted according to the attributes of optimal route.

BGP load balancing also applies to the ASs in a confederation.

Perform the following configuration in BGP view.

Table 6-42 Configure BGP load balancing

Operation	Command
Configure BGP load balancing	**balance** *num*
Remove BGP load balancing	**undo balance**

By default, BGP load balancing is disabled.

At present, BGP load balancing is not available with private networks.

6.2.21 Resetting BGP Connection

After changing BGP policies or protocols, the user must reset the current BGP connection so as to validate the new configuration.

Perform the following configuration in user view.

Table 6-43 Reset BGP connection

Operation	Command
Reset BGP connection between specified peers	**reset bgp** *peer-address* [**vpn-instance** *vpn-instance-name*]
Reset all BGP connections	**reset bgp all** [**vpn-instance** *vpn-instance-name*]
Reset the BGP connections between all peers in a specified peer group	**reset bgp group** *group-name* [**vpn-instance** *vpn-instance-name*]

6.3 Displaying and Debugging BGP

After the above configuration, execute **display** command in all views to display the running of the BGP configuration, and to verify the effect of the configuration. Execute **debugging** command in user view to debug BGP.

Table 6-44 Display and debug BGP

Operation	Command
Display the routing information in the BGP routing table	**display bgp** [**multicast** | **vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }] **routing** [*ip-address mask*]
Display the statistics of the routing information in the BGP routing table	**display bgp** [**multicast** | **vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }] **routing statistic**
Display the BGP AS path information	**display ip as-path-acl** *aspath-acl-number*
Display CIDR routes	**display bgp** [**multicast** | [**vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }]] **routing cidr**
Display the routing information of the specified BGP community	**display bgp** [**multicast** | [**vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }]] **routing community** [*aa:nn* | **internet** | **no-export-subconfed** | **no-advertise** | **no-export**] [**whole-match**]
Display the routing information allowed by the specified BGP community list	**display bgp** [**multicast** | [**vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }]] **routing community-list** *community-list-number* [**whole-match**]
Display BGP dampened route	**display bgp routing dampened**

Operation	Command
Display the routing information the specified BGP peer advertised or received	**display bgp routing peer** *peer-address* { **advertised** | **received** }
Display information about the dampened routes received from the specified peer	**display bgp routing peer** *peer-address* **dampened** [**statistic** | *ip-address*]
Display the route information received from the specified peer and matching the specified regular expression.	**display bgp routing peer** *peer-address* **regular-expression** *text*
Display the routes matching with the specified access-list	**display bgp** [**multicast** | [**vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }]] **routing as-path-acl** *aspath-acl-number*
Display route flapping statistics information	**display bgp routing flap-info** [**regular-expression** *as-regular-rexpession* | **as-path-acl** *aspath-acl-number* | *address* [*mask* [**longer-prefix-list**]]]
Display routes with different source ASs	**display bgp** [**multicast**] **routing different-origin-as**
Display peer information	**display bgp** [**multicast** | [**vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }]] **peer** [[*peer-address*] **verbose**]
Display the routing information that has been configured	**display bgp** [**multicast** | [**vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }]] **network**
Display AS path information	**display bgp paths** *as-regular-expression*
Display information about a peer group	**display bgp** [**multicast** | [**vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }]] **routing group** [*group-name*]
Display the AS path matching AS regular expression	**display bgp** [**multicast** | [**vpnv4** { **all** | **route-distinguisher** *route-distinguisher* | **vpn-instance** *vpn-instance-name* }]] **routing regular-expression** *as-regular-expression*
Display configured route-policy information	**display route-policy** *route-policy-name*
Enable the system to output state changes of the peer for the current OSPF process (in BGP view)	**log-peer-change**

Operation	Command
Disable the system to output state changes of the peer for the current OSPF process (in BGP view)	**undo log-peer-change**
Enable/disable debugging of all BGP information	[**undo**] **debugging bgp all**
Enable/disable debugging of BGP events	[**undo**] **debugging bgp event**
Enable/disable debugging of normal BGP operation information	[**undo**] **debugging bgp normal**
Enable/disable debugging of BGP Keepalive packets	[**undo**] **debugging bgp keepalive** [**receive** | **send**] [**verbose**]
Enable/disable debugging of MBGP update packets	[**undo**] **debugging bgp mp-update** [**receive** | **send**] [**verbose**]
Enable/disable debugging of BGP Open packets	[**undo**] **debugging bgp open** [**receive** | **send**] [**verbose**]
Enable/disable debugging of BGP packets	[**undo**] **debugging bgp packet** [**receive** | **send**] [**verbose**]
Enable/disable debugging of BGP route update packets	[**undo**] **debugging bgp route-refresh** [**receive** | **send**] [**verbose**]
Enable/disable debugging of BGP Update packets	[**undo**] **debugging bgp update** [**receive** | **send**] [**verbose**]
Display dampened routes	**display bgp routing dampened**
Display the flapping information of all the routes	**display bgp routing flap-info**
Clear the flap information of all the routes	**reset bgp flap-info**
Display the route flap information of the AS paths conforming to the regular expression	**display bgp routing flap-info regular-expression** *as-regular-expression*
Clear the route flapping information of the AS paths conforming to the regular expression	**reset bgp flap-info regular-expression** *as-regular-expression*
Display the route flapping information passing AS filtering list	**display bgp routing flap-info as-path-acl** *aspath-acl-number*
Clear the route flapping information passing AS filtering list	**reset bgp flap-info as-path-acl** *aspath-acl-number*
Display the route flapping information of the destination address	**display bgp routing flap-info** *network-address mask*
Clear the route flapping information of the destination address	**reset bgp** *network-address* **flap-info**

Operation	Command
Display the route flapping information more detailed than that of the specified address	**display bgp routing flap-info** *network-address mask* **longer-match**

6.4 BGP Configuration Example

6.4.1 Configuring BGP AS Confederation Attribute

⚠ **Caution:**

In configuration examples, only the commands related to the BGP configuration are listed.

I. Network requirements

In the following figure, the AS 100 is divided into 3 sub-ASs, namely 1001, 1002 and 1003. Configure EBGP, confederation EBGP and IBGP.

II. Network diagram

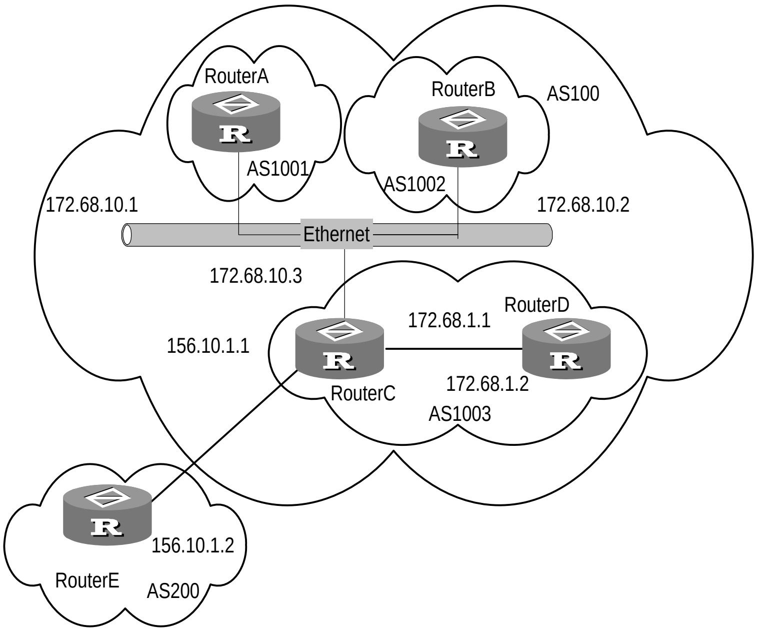


Figure 6-3 Configure AS confederation

III. Configuration procedure

1) Configure Router A:

# Configure the Ethernet interface.

```
[Router A] interface Ethernet0/0/0
[Router A-Ethernet0/0/0] ip address 172.68.10.1 255.255.255.0
```

# Configure BGP.

```
[Router A] bgp 1001
[Router A-bgp] confederation id 100
[Router A-bgp] confederation peer-as 1002 1003
[Router A-bgp] undo synchronization
[Router A-bgp] group confed1002 external
[Router A-bgp] peer confed1002 as-number 1002
[Router A-bgp] peer 172.68.10.2 group confed1002
[Router A-bgp] group confed1003 external
[Router A-bgp] peer confed1003 as-number 1003
[Router A-bgp] peer 172.68.10.3 group confed1003
```

2) Configure Router B:

# Configure the Ethernet interface.

```
[Router B] interface Ethernet0/0/0
[Router B- Ethernet0/0/0] ip address 172.68.10.2 255.255.255.0
```

# Configure BGP:

```
[Router B] bgp 1002
[Router B-bgp] confederation id 100
[Router B-bgp] undo synchronization
[Router B-bgp] confederation peer-as 1001 1003
[Router B-bgp] group confed1001 external
[Router B-bgp] peer confed1001 as-number 1001
[Router B-bgp] peer 172.68.10.1 group confed1001
[Router B-bgp] group confed1003 external
[Router B-bgp] peer confed1003 as-number 1003
[Router B-bgp] peer 172.68.10.3 group confed1003
```

3) Configure Router C:

# Configure the Ethernet interface.

```
[Router C] interface Ethernet0/0/0
[Router C-Ethernet0/0/0] ip address 172.68.10.3 255.255.255.0
```

# Configure BGP:

```
[Router C] bgp 1003
[Router C-bgp] confederation id 100
[Router C-bgp] undo synchronization
```

```
[Router C-bgp] confederation peer-as 1001 1002
[Router C-bgp] group confed1001 external
[Router C-bgp] peer confed1001 as-number 1001
[Router C-bgp] peer 172.68.10.1 group confed1001
[Router C-bgp] group confed1002 external
[Router C-bgp] peer confed1002 as-number 1002
[Router C-bgp] peer 172.68.10.2 group confed1002
[Router C-bgp] group ebgp200 external
[Router C-bgp] peer 156.10.1.2 group ebgp200 as-number 200
[Router C-bgp] group ibgp1003 internal
[Router C-bgp] peer 172.68.1.2 group ibgp1003
```

6.4.2 Configuring BGP Route Reflector

I. Network requirements

Router B receives an update packet passing EBGP and forwards it to Router C. Router C is configured as a route reflector with two clients: Router B and Router D. Router B and Router D need no IBGP connection. When Router C receives the route update packet from Router B, it will reflect the information to Router D and vice versa.

II. Network diagram

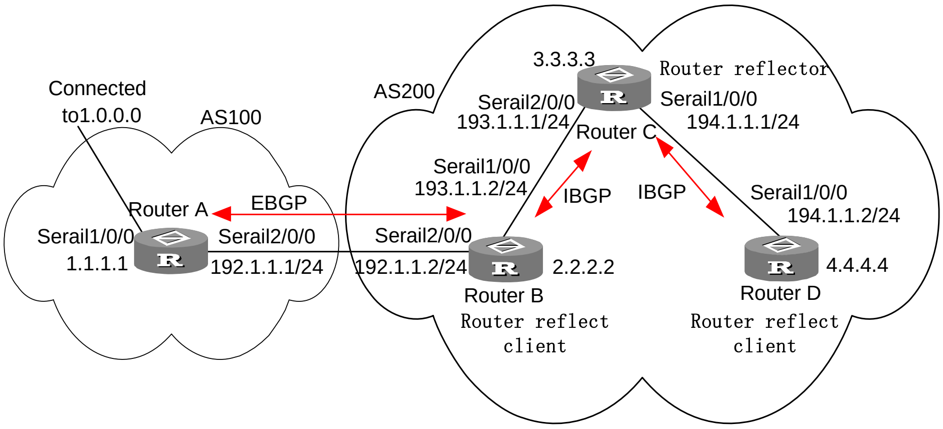


Figure 6-4 Configure BGP route reflector

III. Configuration procedure

1) Configure Router A:

```
[Router A] interface serial 2/0/0
[Router A-Serial2/0/0] ip address 192.1.1.1 255.255.255.0
[Router A-Serial2/0/0] interface serial 1/0/0
[Router A-Serial1/0/0] ip address 1.1.1.1 255.0.0.0
[Router A-Serial1/0/0] quit
[Router A] bgp 100
```

```
[Router A-bgp] group ex external
[Router A–bgp] peer 192.1.1.2 group ex as-number 200
[Router A–bgp] network 1.0.0.0 255.0.0.0
```

2) Configure Router B:

```
[Router B] interface serial 2/0/0
[Router B-Serial2/0/0] ip address 192.1.1.2 255.255.255.0
[Router B-Serial2/0/0] interface serial 1/0/0
[Router B-Serial1/0/0] ip address 193.1.1.2 255.255.255.0
[Router B-Serial1/0/0] quit
[Router B] bgp 200
[Router B-bgp] group ex external
[Router B-bgp] peer 192.1.1.1 group ex as-number 100
[Router B-bgp] peer in next-hop-local
[Router B-bgp] group in internal
[Router B-bgp] peer 193.1.1.1 group in
```

3) Configure Router C:

```
[Router C] interface serial 2/0/0
[Router C-Serial2/0/0] ip address 193.1.1.1 255.255.255.0
[Router C-Serial2/0/0] interface serial 1/0/0
[Router C-Serial1/0/0] ip address 194.1.1.1 255.255.255.0
[Router C-Serial1/0/0] quit
[Router C] bgp 200
[Router C-bgp] group rr internal
[Router C-bgp] reflect between-clients
[Router C-bgp] peer rr reflect-client
[Router C-bgp] peer 193.1.1.2 group rr
[Router C-bgp] peer 194.1.1.2 group rr
```

4) Configure Router D:

```
[Router D] interface serial 1/0/0
[Router D-Serial1/0/0] ip address 194.1.1.2 255.255.255.0
[Router D-Serial1/0/0] quit
[Router D] bgp 200
[Router D-bgp] group in internal
[RouterD-bgp] peer 194.1.1.1 group in
```

Using the **display bgp routing** command on Router B, you can see that Router B has known the existence of network 1.0.0.0.

Using the **display bgp routing** command on Router D, you can see that Router D also knows the existence of network 1.0.0.0.

6.4.3 Configuring BGP Load Balancing

I. Network requirement

EBGP connection is created between Router C and Router A and between Router C and Router B. IBGP connection is created between Router C and Router D.

Static route 9.0.0.0/8 is redistributed on Router A and Router B respectively. It is required to perform load balancing on Router A and Router B.

II. Network diagram

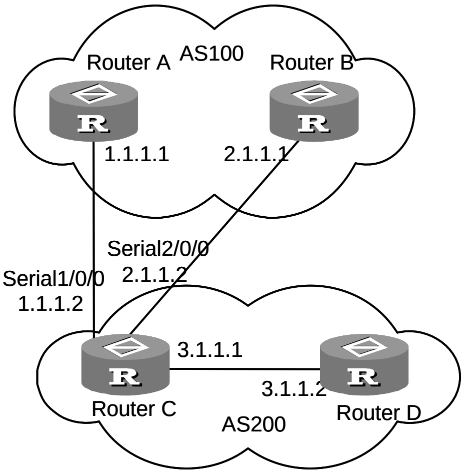


Figure 6-5 Network diagram for BGP load balancing

III. Configuration procedure

# Configure Router A

```
[Router A] router id 11.1.1.1
[Router A] ip route-static 9.0.0.0 255.0.0.0 null0
[Router A] bgp 100
[Router A-bgp] group ex external
[Router A-bgp] peer 1.1.1.2 group ex as-number 200
[Router A-bgp] import-route static
```

# Configure Router B

```
[Router B] router id 12.1.1.1
[Router B] ip route-static 9.0.0.0 255.0.0.0 null0
[Router B] bgp 100
[Router B-bgp] group ex external
[Router B-bgp] peer 2.1.1.2 group ex as-number 200
[Router B-bgp] import-route static
```

# Configure Router C

```
[Router C] bgp 200
```

```
[Router C-bgp] group ex external
[Router C-bgp] peer ex as-number 100
[Router C-bgp] peer 1.1.1.1 group ex
[Router C-bgp] peer 2.1.1.1 group ex
[Router C-bgp] group in internal
[Router C-bgp] peer 3.1.1.2 group in
```

# Configure Router D

```
[Router D] bgp 200
[Router D-bgp] group in internal
[Router D-bgp] peer 3.1.1.1 group in
```

Execute the **display bgp** command on Router C and it shows that there are two effective routes 9.0.0.0/8, one of which is the optimal route. Execute the **display ip routing** command and it shows that the next hop of the optimal route is 1.1.1.1.

Perform the following configuration on Router C:

```
[RouterC] bgp 200
[RouterC-bgp] balance 2
```

Execute the **display ip routing** command on Router C again, and the routing table shows that the BGP route 9.0.0.0/8 has two next-hops, being 1.1.1.1 and 2.1.1.1 respectively.

Execute the **display fib** command on Router C and it shows that the routing entry 9.0.0.0/8 in the forward table has two next-hops, being 1.1.1.1 and 2.1.1.1 respectively.

6.5 Troubleshooting BGP

Symptom 1: The neighboring relationship cannot be established (The Established state cannot be entered).

Troubleshooting:

The establishment of BGP neighborhood needs the router able to establish TCP session through port 179 and exchange Open packets correctly. Perform the check according to the following steps:

- Check whether the configuration of the neighbor's AS number is correct.
- Check whether the neighbor's IP address is correct.
- If using the loopback interface, check whether the **connect-source loopback** has been configured. By default, the router uses the optimal local interface to establish the TCP connection, rather than uses the loopback interface.
- If it is the EBGP neighbor not directly connected physically, check whether the **peer ebgp-max-hop** has been configured.
- Use the ping command to check whether the TCP connection is normal. Since one router may have several interfaces able to reach the peer, the extended **ping -a**

ip-address command should be used to specify the source IP address sending ping packet.

- If the Ping operation fails, use **display ip routing** command to check if there is available route in the routing table to the neighbor.
- If the Ping operation succeeds, check if there is an ACL denying TCP port 179.If the ACL is configured, cancel the denying of port 179.

6.6 MBGP Overview

6.6.1 Introduction to MBGP

As described at the beginning of this chapter, BGP, as the practical exterior gateway protocol, is widely used in interconnection between autonomous systems. The traditional BGP-4 can only manage the routing information of IPv4 and has limitation in inter-AS routing when used in the application of other network layer protocols (such as IPv6 etc).

In order to support multiple network layer protocols, IETF extended BGP-4 and formed MBGP (Multiprotocol Extensions for BGP-4, multiple protocols extension of BGP-4). The present MBGP standard is RFC2858.

MBGP is compatible, that is, a router supporting BGP extension can be interconnected with a router that does not support it.

6.6.2 MBGP Extension Attributes

In the packets BGP-4 uses, three pieces of information related to IPv4 are carried in the update packet. They are NLRI (Network Layer Reachability Information), Next_Hop (The next hop address) in path attribute and Aggregator in path attribute (This attribute includes the BGP speaker address which forms the summary route).

The BGP speaker running on the Internet usually has an IPv4 address. Therefore, it is only necessary for BGP-4 to reflect the information of the specified network layer protocol to NLRI and the Next_Hop in the route attribute to implement supporting to multiple network layer protocols.

Two new path attributes are introduced into MBGP:

- MP_REACH_NLRI: Multiprotocol Reachable NLRI. It is used to advertise reachable routes and next-hop information.
- MP_UNREACH_NLRI: Multiprotocol Unreachable NLRI. It is used to remove unreachable routes.

These two attributes are optional non-transitive. Therefore, the BGP speaker that does not provide multiple protocols ability will ignore the information of them nor transfer them to other peers.

6.6.3 MBGP Applied on the Router

The router adopts address family to differentiate different network layer protocols. For values of address family, refer to RFC1700.

The router provides various MBGP extended applications including extension of multicast and BGP/MPLS VPN etc. Different extended applications should be performed in their own address family views.

For MBGP applied in multicast, refer to "MBGP Multicast Extension" chapter in module "Multicast" of this manual. For MBGP applied in BGP/MPLS VPN, refer to "MPLS VPN" chapter in module "MPLS" of this manual.

6.7 MBGP Configuration

MBGP is the extension of BGP. Many concepts and configuration fundamentals of BGP are also applicable in MBGP.

When configuring MBGP, it is necessary to run BGP before entering corresponding address family view and configuring relevant parameters for different extended applications.

When configuring the MBGP peer/peer group, configure the AS number of the peer/peer group in BGP view first and then enter the corresponding address family view to enable the peer/peer group relation of the application.

Part commands in BGP view also exist in MBGP address family view. However, when configured in MBGP address family view, these commands are only effective to corresponding applications.

Commands in MBGP address family view that are related to specific applications are not described in this chapter. For corresponding contents, refer to module "Multicast" and module "MPLS" of this manual.

MBGP versatile configuration includes:

- Configure the address family
- Enable the peer group

6.7.1 Configuring the Address Family

After MBGP is introduced, IPv4 unicast address family view sometimes is used to indicate the normal BGP view.

Perform the following configuration in BGP view.

Table 6-45 Configure the Address Family

Operation	Command
Enter the MBGP multicast address family view	**ipv4-family multicast**

Operation	Command
Remove the MBGP multicast address family configuration	**undo ipv4-family multicast**
Enter MBGP vpn-instance address family view	**ipv4-family vpn-instance** *vpn-instance-name*
Remove MBGP vpn instance address family configuration	**undo ipv4-family vpn-instance** *vpn-instance-name*
Enter MBGP VPNv4 address family view	**ipv4-family vpnv4** [**unicast**]
Remove MBGP VPNv4 address family configuration	**undo ipv4-family vpnv4** [**unicast**]

Execute the **undo** form of the command to return to BGP view and delete corresponding MBGP extended application configuration.

6.7.2 Enabling Peer/Peer Group

To enable BGP peers to exchange routing information, it is necessary to activate a certain peer group under unicast address family, then add the peers existing under the unicast address family into the activated peer group.

Perform the following configuration in address family view.

Table 6-46 Enable peer/peer group

Operation	Command
Enable a specified peer group	**peer** *group-name* **enable**
Disable a specified peer group	**undo peer** *group-name* **enable**
Add peers into the enabled peer group	**peer** *peer-address* **group** *group-name*
Delete peers from the enabled peer group	**undo peer** *peer-address*

By default, only the peer group in the BGP IPv4 unicast address family is enabled; while other kinds of peers or peer groups are disabled and cannot exchange routing information.

6.8 Displaying and Debugging MBGP

For relevant content, refer to the module "Multicast" and module "MPLS" of this manual.

6.9 MBGP Configuration Example

MBGP is mainly applied to extension of some new services. Its configuration is similar to BGP. The following examples in networking and configuration are the same with those in the "BGP Typical Configuration Examples". The major difference lies in its configurations of entering MBGP address family view and enabling MBGP peer.

For MBGP configuration in specific services, refer to module "Multicast" and module "MPLS" in this manual.

6.9.1 Configuring MBGP Route Reflector

I. Network requirements

Router A, Router B, Router C and Router D have been configured with MBGP multicast extended applications. Router A and Router B are EBGP peers. Router C and Router B are IBGP peers, and Router C and Router D are IBGP peers respectively.

Router B receives an EBGP update packet from Router A and transmit it to Router C. Router C is configured as a route reflector, with two clients, Router B and Router D. When Router C receives the EBGP update packet from Router B, it reflects the information to Router D. IBGP connection needs not to be created between Router B and Router D, for Router C will reflect information to Router D.

II. Network diagram

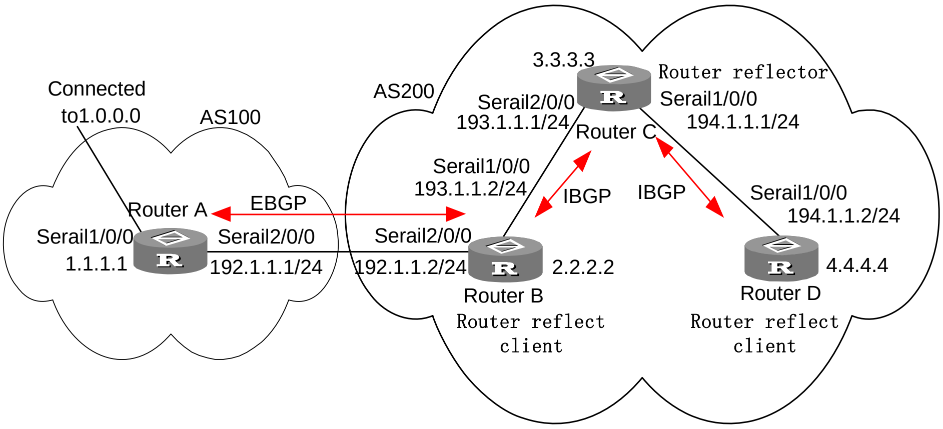


Figure 6-6 Configure MBGP route reflector

III. Configuration procedure

1) Configure Router A:

# Configure the interface.

```
[Router A] interface serial 2/0/0
[Router A-Serial2/0/0] ip address 192.1.1.1 255.255.255.0
[Router A-Serial2/0/0] quit
```

# Configure MBGP of Router A.

```
[Router A] bgp 100
[Router A-bgp] group ex external
[Router A-bgp] peer 192.1.1.2 group ex as-number 200
[Router A-bgp] ipv4-family multicast
[Router A-bgp-af-mul] peer ex enable
[Router A-bgp-af-mu] peer 192.1.1.2 group ex
[Router A-bgp] network 1.0.0.0 255.0.0.0
```

2) Configure Router B:

# Configure the interface.

```
[Router B] interface serial 2/0/0
[Router B-Serial2/0/0] ip address 192.1.1.2 255.255.255.0
[Router B-Serial2/0/0] quit
[Router B] interface serial 1/0/0
[Router B-Serial1/0/0] ip address 193.1.1.2 255.255.255.0
[Router B-Serial1/0/0] quit
```

# Configure OSPF.

```
[Router B] ospf
[Router B-ospf] area 0
[Router B-ospf-area-0.0.0.0] network 193.1.1.0 0.0.0.255
[Router B-ospf-area-0.0.0.0] quit
[Router B-ospf-1] quit
```

# Configure MBGP of Router B.

```
[Router B] bgp 200
[Router B-bgp] group ex external
[Router B-bgp] peer 192.1.1.1 group ex as-number 100
[Router B-bgp] group in internal
[Router B-bgp] peer in next-hop-local
[Router B-bgp] peer 193.1.1.1 group in
[Router B-bgp] import-route ospf
[Router B-bgp] import-route direct
[Router B-bgp] ipv4-family multicast
[Router B-bgp-af-mul] peer in next-hop-local
[Router B-bgp-af-mul] peer ex enable
[Router B-bgp-af-mul] peer in enable
[RouterB-bgp-af-mul] peer 192.1.1.1 group ex
[RouterB-bgp-af-mul] peer 193.1.1.1 group in
```

3) Configure Router C:

# Configure the interface.

```
[Router C] interface serial 2/0/0
```

```
[Router C-Serial2/0/0] ip address 193.1.1.1 255.255.255.0
[Router C-Serial2/0/0] quit
[Router C] interface serial 1/0/0
[Router C-Serial1/0/0] ip address 194.1.1.1 255.255.255.0
[Router C-Serial1/0/0] quit
```

# Configure OSPF.

```
[RouterC] ospf
[RouterC-ospf] area 0
[RouterC-ospf-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[RouterC-ospf-area-0.0.0.0] network 193.1.1.0 0.0.0.255
[RouterC-ospf-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

# Configure MBGP of Router C.

```
[RouterC] bgp 200
[Router C-bgp] group in internal
[Router C-bgp] peer 193.1.1.2 group in
[Router C-bgp] peer 194.1.1.2 group in
[Router C-bgp] peer in reflect-client
[Router C-bgp] ipv4-family multicast
[Router C-bgp-af-mul] peer in enable
[Router C-bgp] peer in reflect-client
[Router C-bgp-af-mul] peer 193.1.1.2 group in
[Router C-bgp-af-mul] peer 194.1.1.2 group in
```

4) Configure Router D:

# Configure the interface.

```
[Router D] interface serial 1/0/0
[Route D-Serial1/0/0] ip address 194.1.1.2 255.255.255.0
[Router D-Serial1/0/0] quit
```

# Configure OSPF.

```
[Router D] ospf
[Router D-ospf] area 0
[Router D-ospf-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[Router D-ospf-area-0.0.0.0] quit
[Router D-ospf-1] quit
```

# Configure MBGP of Router D.

```
[RouterD] bgp 200
[RouterD-bgp] group in internal
[RouterD-bgp] peer 194.1.1.1 group in
[RouterD-bgp] ipv4-family multicast
[RouterD-bgp-af-mul] peer in enable
```

```
[RouterD-bgp-af-mul] peer 194.1.1.1 group in
```

Use the **display bgp multicast routing** command on Router B to display the BGP routing table. It should be noted that Router B has known the existence of the network 1.0.0.0.

Use the **display bgp multicast routing** command on Router D to view the BGP routing table. It should be noted that Router D has known the existence of the network 1.0.0.0.

Chapter 7 IP Routing Policy Configuration

7.1 IP Routing Policy Overview

When a router distributes or receives routing information, it possibly needs to implement some policies to filter the routing information, so as to receive or distribute the routing information which can meet the specified condition only. A routing protocol, e.g. RIP, maybe need to redistribute the routing information discovered by other protocols to enrich its routing knowledge. While redistributing the routing information, it possibly only needs to redistribute the information meeting the conditions and set some special attributes to make them meet its requirement.

To implement the routing policy, you need define a set of matching rules by specifying the characteristics of the routing information in the routing policy under implementation. You can set the rules based on such attributes as destination address and source address of the information. The matching rules can be set in advance and then used in the routing policy to advertise, receive and redistribute routes.

Five kinds of filters, namely route-policy, ACL, AS-path, community-list and IP-prefix, are provided on a router for routing protocols to redistribute. The following will introduce each kind of filter respectively.

I. route-policy

routing policy is used for matching some attributes in given routing information and the attributes of the information will be set if the conditions are satisfied.

A routing policy can comprise multiple nodes. Each node is a unit for matching test, and the nodes will be matched on the basis of their node numbers. Each node comprises a set of **if-match** and **apply** clauses. The **if-match** clauses define the matching rules. The matching objects are some attributes of routing information. The different **if-match** clauses on the same node is in logic AND relationship. Only when the matching requirements specified by all the **if-match** clauses on a node are satisfied, can the matching test on the node be passed. The **apply** clause specifies the actions performed after the node matching test, concerning the attribute settings of the routing information.

The different nodes of a route-policy is in logic OR relationship. The system will check each node of route-policy one by one. Once the test on a route-policy node is passed, it indicates the matching test of the route-policy is passed (the test on the next-node will not proceed).

II. ACL

There are three kinds of ACLs: **advanced** represents advanced ACL, **basic** represents basic ACL and **interface** represents interface-based ACL.

Normally, basic ACL and advanced ACL are adopted to filter routing information. If you use the basic ACL, you must specify a range of IP addresses or subnets when defining ACL so as to match the source address of routing information. If you use the advanced ACL, you can specify protocol type, source/destination address or port number which will be used for matching.

For ACL configuration, refer to the contents about Firewall Configuration in the security part of this manual.

III. IP-prefix

The IP-prefix plays a role similar to ACL. But it is more flexible than ACL and easier to understand. When IP-prefix is applied for filtering of routing information, its matching object is the destination address information field of routing information. Moreover, for IP-prefix, the user can specify the **gateway** option so as to indicate that only routing information advertised by certain routers will be received.

An IP-prefix is identified by the ip-prefix name. Each IP-prefix can include multiple items, and each item, which is identified by an index-number, can independently specify the matching range of the network prefix forms. The *index-number* specifies the matching sequence in the IP-prefix list.

During the matching, the router checks list items identified by the *index-number* in the ascending order. If any one list item meets the condition, it means that it has passed the IP-prefix filtering (will not enter the testing of the next list item).

IV. AS-path-acl

AS-path-acl only applies to BGP. In the BGP routing information packet, there is an AS-path domain (During BGP routing information exchange, the AS path where routing information passes will be recorded in the domain). As-path specifies matching conditions according to the AS-path field.

The definition of the AS-path has already been implemented in the BGP configuration. For the related configurations, please refer to the **ip as-path-acl** command in the chapter BGP Configuration.

V. Community-list

The community-list only applies to BGP. The routing information packet of the BGP includes a community attribute domain to identify a community. Targeting at the community attribute, the community-list specifies the match condition.

The definition of the community-list has already been implemented in the BGP configuration. For the relevant configurations, please refer to the **ip community-list** command in the BGP Configuration.

7.2 Configuring IP Routing Policy

You can use two methods to implement the routing policy: use filtering lists such as ACL, ip-prefix, as-path-acl, and community-list to directly filter routes or route attributes, or configure route-policy to set route attributes meeting the matching conditions.

The following configurations are covered in this chapter:

1) Configuring route filtering

- Define IP prefix list or ACL
- Configure route filtering of received routes
- Redistribute routes from other routing protocols (for OSPF and ISIS route filtering only)
- Configuring to filter distributed routes (redistributed routes for OSPF and ISIS)

2) Configuring route-policy to implement routing policy

- Define a route-policy
- Define **if-match** clauses for a route-policy
- Define **apply** clauses for a route-policy
- Filter redistributed routes by a route-policy

For information about BGP route filtering by as-path-acl and community-list, refer to the part related to BGP.

7.2.1 Configuring Route Filtering

I. Defining filtering conditions

1) Defining IP Prefix List

An ip-prefix list is identified by the ip-prefix name. Each ip-prefix can include multiple items, and each item can independently specify the matching range of the network prefix forms. The *index-number* specifies the matching sequence in the ip-prefix list.

Perform the following configuration in system view.

Table 7-1 Define IP prefix list

Operation	Command
Define IP prefix list	**ip ip-prefix** *ip-prefix-name* [**index** *index-number*] { **permit** | **deny** } *network len* [**greater-equal** *greater-equal* | **less-equal** *less-equal*]
Remove IP prefix list	**undo ip ip-prefix** *ip-prefix-name* [**index** *index-number* | **permit** | **deny**]

During the matching, the router checks list items identified by the *index-number* in the ascending order. If any one list item meets the condition, it means that it has passed the ip-prefix filtering (will not enter the testing of the next list item).

Pay attention to the following:

- If more than one ip-prefix item are defined, then the match mode of at least one list item should be the **permit** mode.
- The list items of the **deny** mode can be firstly defined to rapidly filter the routing information not satisfying the requirement, but if all the items are in the **deny** mode, any routes will not pass the ip-prefix filtering.
- You can define an item of **permit** 0.0.0.0/0 **greater-equal** 0 **less-equal** 32 after the multiple list items in the **deny** mode so as to let all the other routes pass.

For instance, the following configuration will filter out routes from segments 10.1.0.0, 10.2.0.0, and 10.3.0.0, while allowing routing information from other segments to pass through.

```
[Router] ip ip-prefix 1 deny 10.1.0.0 16
[Router] ip ip-prefix 2 deny 10.2.0.0 16
[Router] ip ip-prefix 3 deny 10.3.0.0 16
[Router] ip ip-prefix 4 permit 0.0.0.0/0 greater-equal 0 less-equal 32
```

2) Defining ACL

Refer to the part related to security.

II. Configuring to filter received routes

Perform the following configuration in routing protocol view.

Define a policy rule to filter unqualified routing information during route reception by redistributing an ACL or IP-prefix. The keyword parameter **gateway** indicates only update packets from specific peer routers will be received.

Table 7-2 Configure to filter the redistributed routes

Operation	Command
Configure to filter the received routing information redistributed by the specified address	**filter-policy gateway** *ip-prefix-name* **import**
Cancel the filtering of the received routing information redistributed by the specified address	**undo filter-policy gateway** *ip-prefix-name* **import**
Configure to filter the received global routing information	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } [**gateway**] **import**
Cancel the filtering of the received routing information	**undo filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } [**gateway**] **import**

The **filter-policy import** command allows a routing protocol to filter routes received from the same routing protocol and to block the routing information filtered out from being added to the routing table. This command, however, does not take effect on the routes redistributed from other routing protocols, because those routing entries have been added to the routing table before a blocking action can be taken.

The filtering performed by a link-state protocol is different from that performed by a distance-vector protocol.

A link-state protocol can block routing information from being added to the routing table but cannot filter LSAs. This, however, does not prevent the related LSAs from being advertised to neighbors.

A distance-vector protocol, on the contrary, filters routing tables received from neighbors and the routing information filtered out does not appear in the routing table.

III. Redistributing Routing Information Discovered by Other Routing Protocols

A routing protocol can redistribute the routes discovered by other routing protocols to enrich its route information. When other protocol routing information is to be redistributed, the route-policy can be used for route information filtering to implement the purposeful redistribution. If the destination routing protocol redistributing the routes cannot directly reference the route costs of the source routing protocol, you should satisfy the requirement of the protocol by specifying a route cost for the redistributed route.

Perform the following configuration in routing protocol view.

Table 7-3 Redistribute routes from other protocols

Operation	Command
Set to redistribute routes from other protocols	**import-route** *protocol* [**med** *med* **| cost** *cost*] [**tag** *value*] [**type** { **1** | **2** }]
Cancel the setting for redistributing routes of other protocols	**undo import-route** *protocol*

By default, the routes discovered by other protocols will not be distributed.

Note:

In different routing protocol views, the parameter options are different. For details, respectively refer to the **import-route** command in different protocols.

IV. Configuring to filter the distributed routes

Define a policy concerning route distribution to filter the routing information not satisfying the conditions while redistributing routes by redistributing an ACL or address ip-prefix list. Filter routing information only about the distributed *routing-process* by specifying *routing-process*.

Perform the following configuration in routing protocol view.

Table 7-4 Configure to filter the distributed routes

Operation	Command
Configure to filter the routes distributed by the protocol	**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*routing-process*]
Cancel the filtering of the routes distributed by the protocol	**undo filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*routing-process*]

For OSPF and ISIS, the **filter-policy export** command filters the redistributed routes, and must be used with the **import-route** command; otherwise, it takes no effect. By specifying the *routing-process* argument, you may filter redistributed routes of a particular type. If you do not specify the argument, the command will filter all redistributed routes.

For RIP and BGP, the **filter-policy export** command can filter the routing table without the **import-route** command, It filters advertised routes in this situation.

By far, the routing policy supports redistributing the routes discovered by the following protocols into the routing table:

direct: The hop (or host) to which the local interface is directly connected.
static: Static route.
rip: Route discovered by RIP.
ospf: Route discovered by OSPF.
ospf-ase: External route discovered by OSPF.
ospf-nssa: NSSA route discovered by OSPF.
isis: Route discovered by IS-IS.
bgp: Route acquired by BGP.

By default, no route filtering is performed.

7.2.2 Implementing Routing Policy by route-policy

I. Defining a route-policy

A route-policy can comprise multiple nodes. Each node is a unit for matching operation. The nodes are tested according to *sequence-number*.

Perform the following configuration in system view.

Table 7-5 Define a route-policy

Operation	Command
Enter routing policy view	**route-policy** *route-policy-name* { **permit** | **deny** } **node** *node-number*
Remove the specified route-policy	**undo route-policy** *route-policy-name* [**permit** | **deny** | **node** *node-number*]

The argument **permit** specifies the matching mode for a defined node in the route-policy to be in permit mode. If a route satisfies all the **if-match** clauses of the node, it will pass the filtering of the node, and the **apply** clauses for the node will be executed without taking the test of the next node. If not, however, the route should take the test of the next node.

The **deny** argument specifies the matching mode for a defined node in the route-policy to be in deny mode. In this mode, the **apply** clauses will not be executed. If a route satisfies all the **if-match** clauses of the node, it will be denied by the node and will not take the test of the next node. If not, however, the route will take the test of the next node.

The nodes have the "OR" relationship. In other words, the router will test the route against the nodes in the route-policy in sequence, once a node is matched, the route-policy filtering will be passed.

By default, the route-policy is not defined.

Note: if multiple nodes are defined in a route-policy, at least one of them should be in permit mode. Apply the route-policy to filter routing information. If the routing information does not match any node, the routing information will be denied by the route-policy. If all the nodes in the route-policy are in deny mode, all routing information will be denied by the route-policy.

II. Defining if-match clauses for a route-policy

The **if-match** clauses define the matching rules. That is, the filtering conditions that the routing information should satisfy for passing the route-policy. The matching objects are some attributes of routing information.

Perform the following configuration in route-policy view.

Table 7-6 Define if-match conditions

Operation	Command
Match the AS path domain of the BGP routing information	**if-match as-path** *aspath-acl-number*
Cancel the matched AS path domain of the BGP routing information	**undo if-match as-path**

Operation	Command
Match the community attribute of the BGP routing information	**if-match community** { *standard-community-number* [**whole-match**] | *extended-community-number* }
Cancel the matched community attribute of the BGP routing information	**undo if-match community**
Match the destination address of the routing information	**if-match** { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* }
Cancel the matched destination address of the routing information	**undo if-match** { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* }
Match the next-hop interface of the routing information	**if-match interface** [*interface-type number*]
Cancel the matched next-hop interface of the routing information	**undo if-match interface**
Match the next-hop of the routing information	**if-match ip next-hop** { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* }
Cancel the matched next-hop of the routing information	**undo if-match ip next-hop** [**ip-prefix**]
Match the routing cost of the routing information	**if-match cost** *value*
Cancel the matched routing cost of the routing information	**undo if-match cost**
Match the tag field of the OSPF routing information	**if-match tag** *value*
Remove the tag field matching OSPF routing information	**undo if-match tag**

By default, no matching will be performed.

Pay attention to the following:

- The **if-match** clauses for a node in the route-policy have the relationship of "AND" for matching. That is, the route must satisfy all the clauses to match the node before the actions specified by the **apply** clauses can be executed.
- If no **if-match** clauses are specified, all the routes will pass the filtering on the node.

III. Defining apply clauses for a route-policy

The **apply** clauses specify actions, which are the configuration commands executed after a route satisfies the filtering conditions specified by the **if-match** clauses. Thereby, some attributes of the route can be modified.

Perform the following configuration in route-policy view.

Table 7-7 Define **apply** clauses

Operation	Command
Add the specified AS number before the as-path series of the BGP routing information	**apply as-path** *as-number-1* [*as-number-2* [*as-number-3* ...]]
Cancel the specified AS number added before the as-path series of the BGP routing information	**undo apply as-path**
Set the community attribute in the BGP routing information	**apply community** { { *aa:nn* | **no-export-subconfed** | **no-advertise** | **no-export** }… [**additive]** | **additive** | **none** }
Cancel the set community attribute in the BGP routing information	**undo apply community**
Set the next-hop address of the routing information	**apply ip-address** [**default**] { **next-hop** *ip-address* [*ip-address*] | **acl** *acl-number* }
Cancel the next-hop address of the routing information	**undo apply ip-address** [**default**] [**next-hop** *ip-address* [*ip-address*] | **acl** *acl-number*]
Redistribute the route to isis level-1, level-2 or level-1-2	**apply isis** [**level-1** | **level-2** | **level-1-2**]
Remove the function of redistributing the route to IS-IS	**undo apply isis**
Set the local preference of the BGP routing information	**apply local-preference** *localpref*
Cancel the local preference of the BGP routing information	**undo apply local-preference**
Set the routing cost of the routing information	**apply cost** *value*
Cancel the routing cost of the routing information	**undo apply cost**
Set the cost type of the routing information	**apply cost-type** [**internal** | **external**]
Remove the setting of the cost type	**undo apply cost-type**
Set the route origin of the BGP routing information	**apply origin** { **igp** | **egp** *as-number* | **incomplete** }
Cancel the route origin of the BGP routing information	**undo apply origin**
Set the tag field of the OSPF routing information	**apply tag** *value*
Cancel the tag field of the OSPF routing information	**undo apply tag**

By default, no configuration is performed.

Please note that if the routing information meets the match conditions specified in the route-policy and also notifies the MED value configured with **apply cost-type internal** when notifying the IGP route to the EBGP peers, then this value will be regarded as the MED value of the IGP route. The preference configured with the **apply cost-type internal** is lower than that configured with the **apply cost** command, but higher than that configured with the **default med** command.

IV. Applying route-policy

Perform the following configuration in routing protocol view.

Table 7-8 Redistribute routes from other protocols

Operation	Command
Configure to redistribute routes from other protocols	**import-route** *protocol* [**med** *med* **|** **cost** *cost*] [**tag** *value*] [**type** **1** **|** **2**] **route-policy** *route-policy-name*
Disable redistributing routes from other protocols	**undo import-route** *protocol*

By default, routing information from other protocols is not redistributed.

🕮 **Note:**

Different routing protocol views include different optional parameters. For specific information, refer to the description of the **import-route** command corresponding to the routing protocol in the manual.

For BGP, you can also configure route-policy of the peer group to control routes redistributed from the peer/peer group or advertised to the peer group. Members of the peer group cannot be configured with a outbound route update policy different from that of the group, but can be configured with different inbound policies.

Table 7-9 Configure route-policy for a peer

Operation	Command
Configure route-policy for a peer	**peer** *peer-address* **route-policy** *route-policy-name* **import**
Disable the route-policy of a peer	**undo peer** *peer-address* **route-policy** *policy-name* **import**

7.3 Displaying and Debugging the Routing Policy

After the above configuration, execute **display** command in all views to display the running of the routing policy configuration, and to verify the effect of the configuration.

Table 7-10 Display and debug the routing policy

Operation	Command
Display the routing-policy	**display route-policy** [*route-policy-name*]
Display the path information of the AS filter in BGP	**display ip as-path-acl** [*aspath-acl-number*]
Display the address prefix list information	**display ip ip-prefix** [*ip-prefix-name*]

7.4 Routing Policy Configuration Example

7.4.1 Configuring to Redistribute Routing Information from Other Protocols

I. Network requirements

This example shows how OSPF protocol redistributes RIP routing information selectively.

A router connects a campus network to an area network. The campus network uses RIP as its internal routing protocol, and the area network uses OSPF routing protocol. The router advertises some routing information of the campus network to the area network. To achieve this function, the OSPF protocol on the router filters RIP routing information by redistributing a route-policy. The route-policy comprises two nodes, making OSPF protocol advertises the routing information of 192.1.0.0/24 and 128.2.0.0/16 with different routing metric values.

II. Network diagram

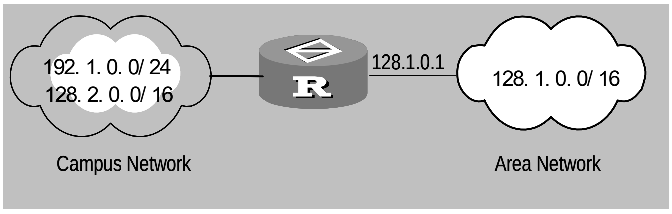


Figure 7-1 Configure OSPF to redistribute RIP routing information

III. Configuration procedure

# Define ip-prefix lists.

```
[Router] ip ip-prefix  p1 permit 192.1.1.0 24
```

```
[Router] ip ip-prefix  p2 permit 128.2.0.0 16
```

# Configure a route-policy.

```
[Router] route-policy r1 permit node 10
[Router-route-policy] if-match ip-prefix p1
[Router-route-policy] apply cost 120
[Router-route-policy] route-policy r1 permit node 20
[Router-route-policy] if-match ip-prefix p2
[Router-route-policy] apply cost 100
[Router-route-policy] quit
```

# Configure OSPF.

```
[Router] ospf
[Router-ospf-1] area 0
[Router -ospf-1-area-0.0.0.0] network 128.1.0.0 0.0.0.255
[Router -ospf-1-area-0.0.0.0] quit
[Router-ospf-1] import-route rip route-policy r1
[Router-ospf-1] quit
[Router] interface ethernet 0/0/0
[Router-Ethernet0/0/0] ip address 128.1.0.1 255.255.255.0
```

7.4.2 Configuring RIP to Filter the Advertised Routing Information

I. Network requirements

This example shows how RIP advertises routing information selectively.

A router connects campus network A to campus network B, both of which use RIP as their internal routing protocol. The router advertises the routes on the two segments (192.1.1.0/24 and 192.1.2.0/24) of campus network A to campus network B. To achieve this function, you can use the **filter-policy** command to enable RIP on the router to filter the advertised routing information. By referencing an IP-prefix list, the router filters the advertised routing information.

II. Network diagram

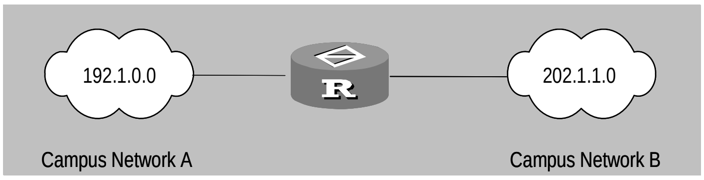


Figure 7-2 Configure to filter advertised routing information

III. Configuration procedure

# Configure an IP-prefix list.

```
[Router] ip ip-prefix p1 permit 192.1.1.0 24
[Router] ip ip-prefix p1 permit 192.1.2.0 24
```

# Configure RIP.

```
[Router] rip
[Router-rip] network 192.1.0.0
[Router-rip] network 202.1.1.0
[Router-rip] filter-policy ip-prefix p1 export
```

7.4.3 Configuring OSPF to Filter the Received Routing Information

I. Network requirements

- Router A communicates with Router B, the link layer is encapsulated with the PPP protocol. OSPF protocol is enabled on both routers.
- Configure the OSPF route process on Router A and redistribute three static routes.
- With the application of the route filtering rule configured in Router B, make the received three static routes partially visible and partially shielded---the routes of network segments 20.0.0.0 and 40.0.0.0 are visible, and the route of network segment 30.0.0.0 is shielded.

II. Network diagram

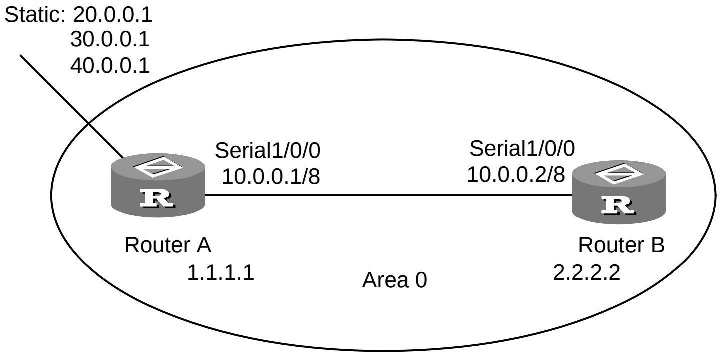


Figure 7-3 Configure to filter the received routing information

III. Configuration procedure

1) Configure Router A:

# Configure the IP address of interface Serial1/0/0 and encapsulate the PPP protocol.

```
[Router A] interface serial 1/0/0
[Router A-Serial1/0/0] ip address 10.0.0.1 255.0.0.0
[Router A-Serial1/0/0] link-protocol ppp
[Router A-Serial1/0/0] quit
```

# Configure three static routes:

```
[Router A] ip route-static 20.0.0.1 32 serial 1/0/0
[Router A] ip route-static 30.0.0.1 32 serial 1/0/0
[Router A] ip route-static 40.0.0.1 32 serial 1/0/0
```

# Enable the OSPF protocol and specify the area ID of the interface.

```
[Router A] router id 1.1.1.1
[Router A] ospf
[Router A-ospf] area 0
[Router A--ospf-area-0.0.0.0] network 10.0.0.0 0.0.0.255
```

# Redistribute the static routes

```
[Router A-ospf] import-route static
```

2) Configure Router B:

# Configure the IP address of interface Serial1/0/0 and encapsulate the PPP protocol.

```
[Router B] interface serial 1/0/0
[Router B-Serial1/0/0] ip address 10.0.0.2 255.0.0.0
[Router B-Serial1/0/0] link-protocol ppp
[Router B-Serial1/0/0] quit
```

# Configure ACL.

```
[Router B] acl number 2001
[Router B-acl-basic-2001] rule deny source 30.0.0.0 0.255.255.255
[Router B-acl-basic-2001] rule permit source any
```

# Enable the OSPF protocol and specify the area ID of the interface.

```
[Router B] router id 2.2.2.2
[Router B] ospf
[Router B-ospf] area 0
[Router A-ospf-area-0.0.0.0] network 10.0.0.0 0.0.0.255
```

# Configure the OSPF to filter the received external routes.

```
[Router B-ospf] filter-policy 1 import
```

7.4.4 Configuring the BGP cost Attribute to Select Path

I. Network requirements

This example illustrates how the administrator manages the routing via BGP attributes.

All routers are configured with BGP, and IGP in AS200 adopts OSPF.

Router A is in AS100, Router B, Router C and Router D are in AS200. EBGP is enabled on Router A, Router B and Router C. IBGP is enabled on Router B, Router C and Router D.

II. Network diagram

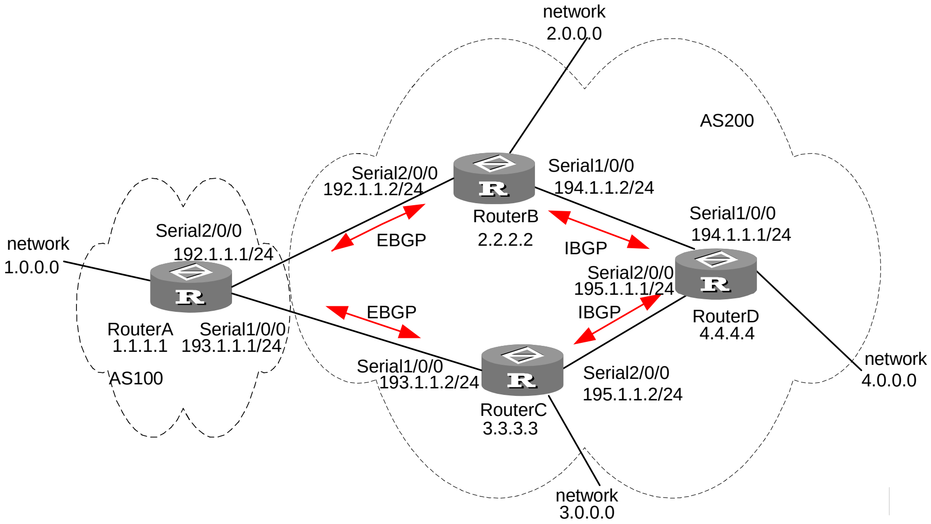


Figure 7-4 Configure BGP routing

III. Configuration procedure

1) Configure Router A:

```
[Router A] interface serial 2/0/0
[Router A-Serial2/0/0] ip address 192.1.1.1 255.255.255.0
[Router A-Serial2/0/0] interface serial 1/0/0
[Router A-Serial1/0/0] ip address 193.1.1.1 255.255.255.0
[Router A-Serial1/0/0] quit
[Router A] bgp 100
[Router A-bgp] network 1.0.0.0
[Router A-bgp] group ex192 external
[Router A-bgp] peer 192.1.1.2 group ex192 as-number 200
[Router A-bgp] group ex193 external
[Router A-bgp] peer 193.1.1.2 group ex193 as-number 200
[Router A-bgp] quit
```

# Configure the MED attribute of Router A.

# Add ACL to Router A and permit the network 1.0.0.0.

```
[Router A] acl number 2001
[Router A-acl-basic-2001] rule permit source 1.0.0.0 0.255.255.255
```

# Define two routing policies, one called apply_med_50 and the other apply_med_100. The MED attribute set by the former for network 1.0.0.0 is 50, while the MED attribute set by the latter is 100.

```
[Router A] route-policy apply_med_50 permit node 10
[Router A-route-policy] if-match acl 2001
[Router A-route-policy] apply cost 50
```

```
[Router A-route-policy] quit
[Router A] route-policy apply_med_100 permit node 10
[Router A-route-policy] if-match acl 2001
[Router A-route-policy] apply cost 100
[Router A-route-policy] quit
```

# Apply apply_med_50 to egress route update of Router C (193.1.1.2), and apply apply_med_100 to the egress route update of Router B (192.1.1.2).

```
[Router A] bgp 100
[Router A-bgp] peer ex193 route-policy apply_med_50 export
[Router A-bgp] peer ex192 route-policy apply_med_100 export
```

2) Configure Router B:

```
[Router B] interface serial 2/0/0
[Router B-Serial2/0/0] ip address 192.1.1.2 255.255.255.0
[Router B-Serial2/0/0] interface serial 1/0/0
[Router B-Serial1/0/0] ip address 194.1.1.2 255.255.255.0
[Router B-Serial1/0/0] quit
[Router B] ospf
[Router B-ospf-1] import-route bgp
[Router B-ospf] area 0
[Router B-ospf-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[Router B-ospf-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[Router B] bgp 200
[Router B-bgp] undo synchronization
[Router B-bgp] group ex external
[Router B-bgp] peer 192.1.1.1 group ex as-number 100
[Router B-bgp] group in internal
[Router B-bgp] peer 194.1.1.1 group in
[Router B-bgp] import-route ospf
```

3) Configure Router C:

```
[Router C] interface serial 1/0/0
[Router C-Serial1/0/0] ip address 193.1.1.2 255.255.255.0
[Router C-Serial1/0/0] interface serial 2/0/0
[Router C-Serial2/0/0] ip address 195.1.1.2 255.255.255.0
[Router C-Serial2/0/0] quit
[RouterC] ospf
[Router C-ospf-1] import-route bgp
[Router C-ospf] area 0
[Router C-ospf-area-0.0.0.0] network 193.1.1.0 0.0.0.255
[Router C-ospf-area-0.0.0.0] network 195.1.1.0 0.0.0.255
[Router C] bgp 200
[Router C-bgp] group ex external
[Router C-bgp] peer 193.1.1.1 group ex as-number 100
```

```
[Router C-bgp] group in internal
[Router C-bgp] peer 195.1.1.1 group in
[Router C-bgp] import-route ospf
```

4) Configure Router D:

```
[RouterD] interface serial 1/0/0
[RouterD-Serial1/0/0] ip address 194.1.1.1 255.255.255.0
[RouterD-Serial1/0/0] interface serial 2/0/0
[RouterD-Serial2/0/0] ip address 195.1.1.1 255.255.255.0
[RouterD-Serial2/0/0] quit
[RouterD] ospf
[Router D-ospf-1] import-route bgp
[Router D-ospf] area 0
[Router D-ospf-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[Router D-ospf-area-0.0.0.0] network 195.1.1.0 0.0.0.255
[Router D-ospf-area-0.0.0.0] network 4.0.0.0 0.255.255.255
[Router D] bgp 200
[Router D-bgp] group in internal
[Router D-bgp] peer 195.1.1.2 group in as-number 200
[Router D-bgp] peer 194.1.1.2 group in as-number 200
[Router D-bgp] import-route ospf
```

To enable the configuration, all BGP peers will be reset via the **reset bgp all** command.

After above configuration, due to the fact that the MED attribute of route 1.0.0.0 discovered by Router C is less than that of Router B, Router D will first select the route 1.0.0.0 from Router C.

If the MED attribute of Router A is not configured, the local priority on Router C is configured as follows:

# Configure the local priority attribute of Router C.

- Add ACL 2001 on Router C and permit network 1.0.0.0.

```
[Router C] acl number 2001
[Router C-acl-basic-2001] rule permit source 1.0.0.0 0.255.255.255
```

- Define a routing policy named localpref. Set the local preference of routes matching ACL 2001 as 200, and that of those not matching as 100.

```
[Router C] route-policy localpref permit node 10
[Router C-route-policy] if-match acl 2001
[Router C-route-policy] apply local-preference 200
[Router C-route-policy] route-policy localpref permit node 20
[Router C-route-policy] apply local-preference 100
[Router C-route-policy] quit
```

- Apply such routing policy to routing information from BGP neighbor 193.1.1.1 (Router A).

```
[RouterC] bgp 200
```

```
[RouterC-bgp] peer 193.1.1.1 route-policy localpref import
```

By then, due to the fact that the local preference attribute value (200) of the route 1.0.0.0 learned by Router C is greater than that of Router B (Router B is not configured with local preference attribute, 100 by default), Router D will also first select the route 1.0.0.0 from Router C.

7.4.5 Configuring Routing Policy Based on next-hop/as-path/origin/ local-preference

I. Network requirements

RouterA and RouterB are in AS300, RouterD is in AS100, and RouterC is in AS200. Configure RouterA and D, RouterB and C, RouterC and D to be EBGP peers; configure RouterA and B to be IBGP peers; configure RouterA and B to use the RIP protocol between them.

II. Network diagram

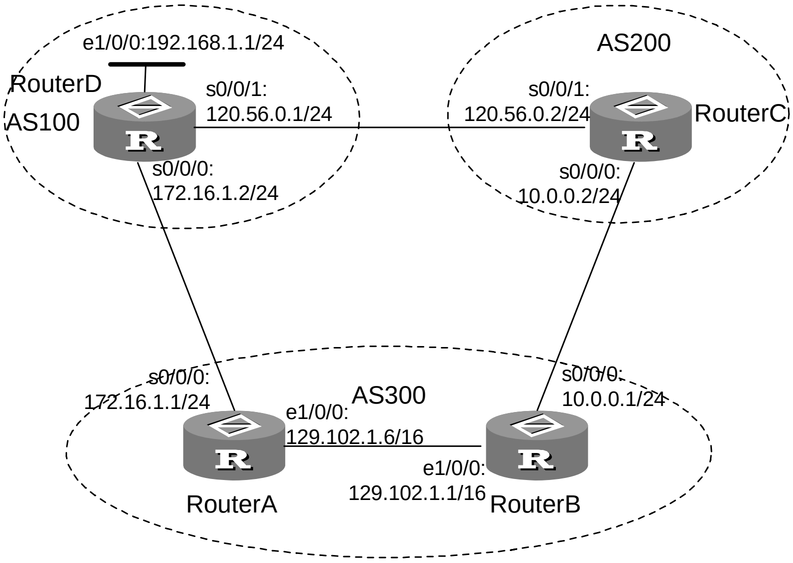


Figure 7-5 Configure routing policy based on next-hop/as-path/origin/ local-preference

III. Configuration procedure

1) Configure RouterA:

# Configure the IP addresses of the interfaces.

```
[RouterA] interface serial 0/0/0
[RouterA-serial 0/0/0] ip address 172.16.1.1 255.255.255.0
[RouterA-serial 0/0/0] interface ethernet 1/0/0
[RouterA-ethernet 1/0/0] ip address 129.102.1.6 255.255.255.0
[RouterA-ethernet 1/0/0] quit
```

# Configure the RIP protocol.

```
[RouterA] rip
[RouterA-rip] network 129.102.1.6
[RouterA-rip] quit
```

# Configure BGP internal and external neighbors.

```
[RouterA] bgp 300
[RouterA-bgp] undo synchronization
[RouterA-bgp] import-route rip
[RouterA-bgp] group ex100 external
[RouterA-bgp] peer 172.16.1.2 group ex100 as-number 100
[RouterA-bgp] group in300 internal
[RouterA-bgp] peer 129.102.1.1 group in300
```

2) Configure RouterB:

```
[RouterB] interface serial 0/0/0
[RouterB-serial 0/0/0] ip address 10.0.0.1 255.255.255.0
[RouterB-serial 0/0/0] interface ethernet 1/0/0
[RouterB-ethernet 1/0/0] ip address 129.102.1.1 255.255.255.0
[RouterB-ethernet 1/0/0] quit
[RouterB] rip
[RouterB-rip] network 129.102.1.1
[RouterB-rip] quit
[RouterB] bgp 300
[RouterB-bgp] import-route rip
[RouterB-bgp] undo synchronization
[RouterB-bgp] group in300 internal
[RouterB-bgp] peer 129.102.1.6 group in300
[RouterB-bgp] group ex200 external
[RouterB-bgp] peer 10.0.0.2 group ex200 as-number 200
```

3) Configure RouterC:

```
[RouterC] interface serial 0/0/0
[RouterC-interface serial 0/0/0] ip address 10.0.0.2 255.255.255.0
[RouterC-interface serial 0/0/0] interface serial 0/0/1
[RouterC-interface serial 0/0/1] ip address 120.56.0.2 255.255.255.0
[RouterC-interface serial 0/0/1] quit
[RouterC] bgp 200
[RouterC-bgp] group ex100 external
[RouterC-bgp] peer 120.56.0.1 group ex100 as-number 100
[RouterC-bgp] group ex300 external
[RouterC-bgp] peer 10.0.0.1 group ex300 as-number 300
```

4) Configure RouterD:

```
[RouterD] interface serial 0/0/0
[RouterD- serial 0/0/0] ip address 172.16.1.2 255.255.255.0
```

```
[RouterD- serial 0/0/0] interface serial 0/0/1
[RouterD- serial 0/0/1] ip address 120.56.0.1 255.255.255.0
[RouterD- serial 0/0/1] interface ethernet 1/0/0
[RouterD- ethernet 1/0/0] ip address 192.168.1.1 255.255.255.0
[RouterD- ethernet 1/0/0] quit
[RouterD] bgp 100
[RouterD-bgp] network 192.168.1.0
[RouterD-bgp] group ex300 external
[RouterD-bgp] peer 172.16.1.1 group ex300 as-number 300
[RouterD-bgp] group ex200 external
[RouterD-bgp] peer 120.56.0.2 group ex200 as-number 200
[RouterD-bgp] network 192.168.1.0 mask 255.255.255.0
[RouterD-bgp] quit
[RouterD] quit
```

After completing the above configurations, perform the **display bgp routing** command on RouterA and B, respectively. You will see that the next hop of 192.168.1.0 is 172.16.1.2, and the origin attribute is igp.

- If you add as-path on RouterD:

```
[RouterD] bgp 100
[RouterD] peer ex300 route-policy AS300 export
[RouterD] quit
[RouterD] route-policy AS300 permit node10
[RouterD- route-policy] if-match acl 2001
[RouterD-route-policy] apply as-path 300
[RouterD- route-policy] quit
[RouterD] acl number 2001 match-order auto
[RouterD-acl-2001] rule permit ip source any
[RouterD-acl-2001] quit
[RouterD] quit
```

You will see that the next hop of 192.168.1.0 is changed to 10.0.0.2, with as-path being 200, 100; while the original AS300 routes are filtered out.

- If you specify the IP address of the next hop on RouterA:

```
[RouterA] bgp 300
[RouterA] peer ex100 route-policy AS100 export
[RouterA] quit
[RouterA] route-policy AS100 permit node 10
[RouterA-route-policy] if-match acl 2001
[RouterA-route-policy] apply ip-address 10.0.0.2
[RouterA-route-policy] quit
[RouterA] acl number 3001
[RouterA-acl-3001] rule permit ip destination 192.168.1.0
```

```
[RouterA-acl-3001] quit
[RouterA] quit
```

You will see that the next hop of 192.168.1.0 is changed to 10.0.0.2.

If you configure the origin attribute on RouterD:

```
[RouterD] bgp 100
[RouterD] peer ex300 route-policy AS300 export
[RouterD] quit
[RouterD] route-policy AS300 permit node10
[RouterD--route-policy] if-match acl 2001
[RouterD--route-policy] apply origin Incomplete
[RouterD--route-policy] quit
[RouterD] acl number 2001 match-order auto
[RouterD-acl-2001] rule permit ip source 192.168.1.0
[RouterD-acl-2001] quit
[RouterD] quit
```

You will see that the origin attribute is changed to Incomplete.

If you configure the local-preference attribute on RouterB:

```
[RouterB] bgp 200
[RouterB] peer ex200 route-policy AS200 export
[RouterB] quit
[RouterB] route-policy AS200 permit node10
[RouterB-route-policy] if-match acl 2001
[RouterB-route-policy] apply local-preference 150
[RouterB-route-policy] quit
[RouterB] acl number 2001 match-order auto
[RouterB-acl-2001] rule permit ip destination 192.168.1.0
[RouterB-acl-2001] quit
[RouterB] quit
```

You will see that the next hop of 192.168.1.0 is changed to 10.0.0.2.

7.4.6 Configuring Routing policy Based on the BGP Community Attribute

I. Network requirements

RTA, RTB, and RTC are BGP peers of one another, where RTB and RTC distribute routing information with the community attribute to their peers, while RTA does not distribute the community attribute to its peers.

II. Network diagram

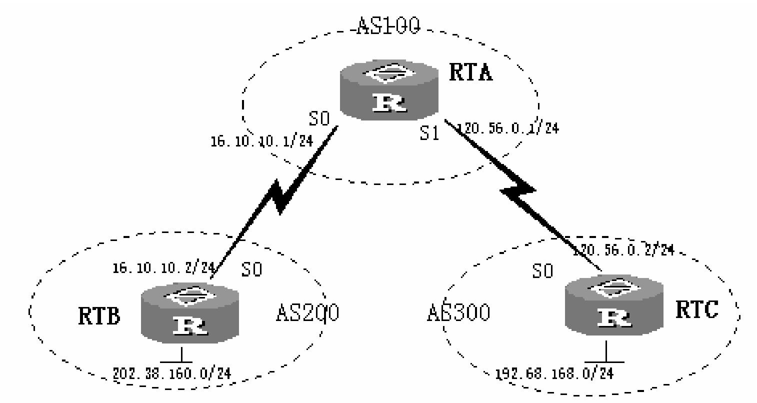


Figure 7-6 Configure routing policy based on the BGP community attribute

III. Configuration procedure

1) Configure RTA:

```
[RouterA] bgp 100
```

# Configure peer ex200, and set to filter received routes by routing policy SETNOEXP.

```
[RouterA-bgp] group ex200 external
[RouterA-bgp] peer 16.10.10.2 group ex200 as-number 200
[RouterA-bgp] peer ex200 route-policy SETNOEXP import
```

# Configure peer ex300, and set to filter received routes.

```
[RouterA-bgp] group ex300 external
[RouterA-bgp] peer 120.56.0.2 group ex300 as-number 300
[RouterA-bgp] peer ex300 route-policy SETNOEXP import
[RouterA-bgp] quit
```

# Configure community-list.

```
[RouterA ] ip community-list 10 permit 100:200
[RouterA ] ip community-list 20 permit 100:300
```

# Configure routing policies for ex200 and ex300.

```
[RouterA ] route-policy SETNOEXP permit node 10
[RouterA- route-policy ] if-match community 10
[RouterA- route-policy ] apply community no-export
[RouterA- route-policy ] route-policy SETNOEXP permit node 20
[RouterA- route-policy ] if-match community 20
[RouterA- route-policy ] apply community no-export
```

2) Configure RTB:

```
[RTB] bgp 200
```

# Configure peer ex100, and set to distribute the community attribute to peers.

```
[RTB-bgp] group ex100 external
```

```
[RTB-bgp] peer 16.10.10.1 group ex100 as-number 100
[RTB-bgp] peer ex100 advertise-community
```

# Configure routing policy for distributing routes to ex100.

```
[RTB-bgp] peer ex100 route-policy SET_COMM export
[RTB-bgp] quit
```

# Configure as-path-acl to include all routes.

```
[RTB ] ip as-path-acl 10 perm ^$
[RTB ] ip as-path-acl 10 deny .*
```

# Configure all routes as100 distributes with community number 100:200.

```
[RTB ] route-policy SET_COMM permit node 10
[RTB-route-policy ] if-match as-path 10
[RTB-route-policy ] apply community 100:200
```

3) Configure RTC:

```
[RTC ] bgp 300
```

# Configure peer ex100, and set to distribute the community attribute to peers.

```
[RTC-bgp ] group ex100 external
[RTC-bgp ] peer 120.56.0.1 group ex100 as-number 100
[RTC-bgp ] peer ex100 advertise-community
```

# Configure routing policy for distributing routes to ex100.

```
[RTC-bgp ] peer ex100 route-policy SET_COMM export
[RTC-bgp ] quit
```

# Configure as-path-acl to include all routes.

```
[RTC] ip as-path-acl 10 perm ^$
[RTC] ip as-path-acl 10 deny .*
```

# Configure all routes as100 distributes with community number 100:300.

```
[RTC] route-policy SET_COMM perm node 10
[RTC- route-policy] if-match as-path 10
[RTC- route-policy] apply community 100:300
```

RTB and RTC are configured to set routes distributed outward with community attributes 100:200 and 100:300, respectively; RTA is configured to set routes received from ex200 and ex300 with community attribute no-export, i.e. those routes will not be distributed to the outside. So, as the result of the configurations, RTA has routes to 202.38.160.0 and 192.68.168.0, while RTB has no route to 192.68.168.0, and RTC has no route to 202.38.160.0.

7.5 Troubleshooting Routing Policy

Symptom 1: Routing information filtering cannot be implemented in normal operation of the routing protocol

Troubleshooting:

Check the following requirements:

- The if-match mode of at least one node of the route-policy should be the **permit** mode. When a route-policy is used for the routing information filtering, if a piece of routing information does not pass the filtering of any node, then it means that the route information does not pass the filtering of the route-policy. When all the nodes of the route-policy are in the **deny** mode, then all the routing information cannot pass the filtering of the route-policy.
- The if-match mode of at least one list item of the ip-prefix should be the **permit** mode. The list items of the **deny** mode can be firstly defined to rapidly filter the routing information not satisfying the requirement, but if all the items are in the **deny** mode, any routes will not pass the ip-prefix filtering. You can define an item of "**permit** 0.0.0.0/0 less-equal 32" after the multiple list items in the deny mode so as to let all the other routes pass the filtering (If less-equal 32 is not specified, only the default route will be matched).

Chapter 8 Route Capacity Configuration

8.1 Route Capacity Configuration Overview

8.1.1 Introduction to Route Capacity Configuration

In practical networking applications, there are always a large number of routes in the routing table especially OSPF routes and BGP routes. The routing information is usually stored in the memory of the router. When the size of the routing table increases, the memory used also increases, but the total memory of the router will not change (unless the hardware is upgraded but upgrade cannot be guaranteed to solve all problems). When the memory is exhausted, the router will not work.

In order to solve such problem, the router provides a mechanism to control the size of the routing table: Monitor the free memory in the system to determine whether to add new routes to the routing table and whether to keep connection with a routing protocol.

📖 **Note:**

It should be noted that the default value meets the requirements normally. The user is not recommended to modify the configuration to avoid improper configuration to avoid reducing of stability and availability of the system.

8.1.2 Route Capacity Limitation

Usually, the huge size of the routing table is caused by BGP routes and OSPF routes. Therefore, the route capacity limitation is only effective to these two types of routes and has no impact on static routes and other dynamic routing protocols.

When the free memory of a router reduces to the lower limit value, the system will disconnect BGP and OSPF and remove corresponding routes from the routing table so that the memory occupied is released. The system checks the free memory periodically. When the free memory is detected to restore to the safety value, BGP and OSPF connection will be restored.

8.2 Route Capacity Configuration

Route capacity configuration includes:

- Configure/restore the lower limit and the safety value of the router memory
- Disable automatic recovery of the disconnected routing protocol

- Enable automatic recovery of the disconnected routing protocol

8.2.1 Configuring the Lower Limit and the Safety Value of the Router Memory

When the router memory is equal to or lower than the lower limit, BGP and OSPF will be disconnected.

When the free memory value reduces to the safety value but does not reach the lower limit value yet, the **display memory limit** command can be used to see that the router is in an exigent state.

If memory automatic restoration is enabled, when the free memory of the router exceeds the safety value, the disconnected BGP and OSPF will be restored.

Perform the following configuration in system view.

Table 8-1 Configure the lower limit and the safety value of the router memory

Operation	Command
Configure the lower limit and the safety value of the router memory	**memory** { **safety** *safety-value* **|** **limit** *limit-value* }*
Restore the lower limit and the safety value of the router memory to their default values	**undo memory** { **safety** *safety-value* | **limit** *limit-value* }*

The default of *safety-value* depends on the capacity of the memory. For a router with 128 Mbytes memory, *safety-value* defaults to 5 Mbytes; for a router with 256 Mbytes memory, *safety-value* defaults to 50 Mbytes.

The default of *limit-value* depends on the capacity of the memory. For a router with 128 Mbytes memory, *limit-value* defaults to 3 Mbytes; for a router with 256 Mbytes memory, *limit-value* defaults to 40 Mbytes.

Note:

safety-value must be configured to be greater than *limit-value*.

8.2.2 Disabling Automatic Recovery of the Disconnected Routing Protocol

If the automatic recovery function of a router is disabled, disconnected BGP and OSPF connections will not be restored even if the free memory is larger than the safety value. Perform this configuration cautiously.

Perform the following configuration in system view.

Table 8-2 Disable the automatic recovery function

Operation	Command
Disable the automatic recovery function	**memory auto-establish disable**

By default, the automatic recovery function is enabled.

8.2.3 Enabling Automatic Recovery of the Disconnected Routing Protocol

Perform the following configuration in system view.

Table 8-3 Enable the automatic recovery function

Operation	Command
Enable the automatic recovery function	**memory auto-establish enable**

By default, the automatic recovery function is enabled.

8.3 Displaying and Debugging Route Capacity

After the above configuration, execute **display** command in all views to display the running of the route capacity configuration and to verify the effect of the configuration.

Table 8-4 Display and debug route capacity

Operation	Command
Display memory setting and state information related to route capacity	**display memory** [**limit**]

Multicast Protocol

Table of Contents

Chapter 1 IP Multicast

1.1 IP Multicast Overview

Various transmission methods can be used when the information (including data, voice and video) is to be sent to a limited number of users on the network. You can use the unicast method to establish an independent data transmission path for each user, or the broadcast method to send information to all users on the network, regardless of their need. For example, if the same information is required by 200 users on the network, the traditional solution is to send the information 200 times respectively in unicast mode so that every of these users can receive the data they need. In the broadcast mode, the data is broadcast over the entire network and whoever needs the data can get it directly from the network. Both occupy too much of the bandwidth resources. In addition, the broadcast mode decreases security and privacy of the information.

IP multicast technology solves these problems. It allows the multicast source to send the information once only, and ensures that the information will not be duplicated or distributed unless it reaches a fork in the tree route established by the multicast routing protocol (see Figure1-1). Therefore, the information can be correctly sent to whoever needs it with high efficiency.

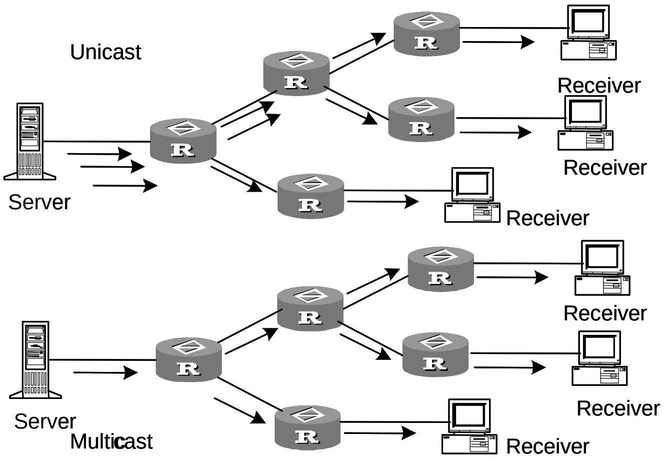


Figure 1-1 Comparison between the unicast and multicast transmission

Note that a multicast source does not necessarily belong to a multicast group. It sends data to the multicast group which is not necessarily a receiver. Multiple sources can send packets to a multicast group simultaneously.

If there is a router that does not support multicast, a multicast router can encapsulate the multicast packets in unicast IP packets with tunneling and send them to the neighboring multicast router. The neighboring multicast router will remove the unicast IP header and continue the multicast transmission. That protects the network architecture from great change.

The following are the benefits of multicast:

- High efficiency: It reduces network traffic, alleviating load of servers and the involved devices
- Optimized performance: It eliminates traffic redundancy.
- Distributed application: It enables multipoint application.

1.2 Multicast Addresses

1.2.1 IP Multicast Addresses

Class D IP addresses are used in the destination addresses of multicast packets, ranging from 224.0.0.0 to 239.255.255.255. Class D addresses cannot appear in the source IP address fields of IP packets.

During unicast data transmission, a packet is transmitted "hop-by-hop" from the source address to the destination address. However, in IP multicast environment, a packet has more than one destination address, or a group of addresses. All the information receivers are added to a group. Once a receiver joins the group, the data for this group of addresses start flowing to this receiver. All members in the group can receive the packets. Membership here is dynamic, and a host can join or leave the group at any time.

A multicast group can be permanent or temporary. The multicast addresses officially allocated form the permanent multicast group, and the others form temporary ones. The IP addresses of a permanent multicast group are unchangeable, but its membership is changeable, and the number of members is arbitrary. It is quite possible for a permanent group to not a single member.

For ranges and meanings of Class D addresses, see Table 1-1.

Table 1-1 Ranges and meanings of Class D addresses

Class D address range	Description
224.0.0.0 to 224.0.0.255	Reserved multicast addresses (addresses of permanent groups). All but 224.0.0.0 can be allocated by routing protocols.
224.0.1.0 to 238.255.255.255	Multicast addresses available for users (addresses of temporary groups). They are valid in the entire network.

Class D address range	Description
239.0.0.0 to 239.255.255.255	Multicast addresses for local management. They are valid only in the specified local range.

Reserved multicast addresses that are commonly used are described in the following table.

Table 1-2 Reserved multicast address list

Class D address	Description
224.0.0.0	Base Address (Reserved)
224.0.0.1	Addresses of all hosts
224.0.0.2	Addresses of all multicast routers
224.0.0.3	Not for allocation
224.0.0.4	DVMRP routers
224.0.0.5	OSPF routers
224.0.0.6	OSPF DR
224.0.0.7	ST routers
224.0.0.8	ST hosts
224.0.0.9	RIP-2 routers
224.0.0.10	IGRP routers
224.0.0.11	Active agents
224.0.0.12	DHCP server/Relay agent
224.0.0.13	All PIM routers
224.0.0.14	RSVP encapsulation
224.0.0.15	All CBT routers
224.0.0.16	Specified SBM
224.0.0.17	All SBMS
224.0.0.18	VRRP
……	……

1.2.2 Ethernet Multicast MAC Addresses

When a unicast IP packet is transmitted on the Ethernet, the destination MAC address is the MAC address of the receiver. However, for a multicast packet, the destination is no longer a specific receiver but a group with unspecific members. Therefore, the multicast MAC address should be used. A multicast MAC address corresponds with a group of multicast IP addresses. As Internet Assigned Number Authority (IANA) provisions, the high 24 bits of a multicast MAC address are 0x01005e and the low 23 bits of a MAC address is the low 23 bits of a multicast IP address.

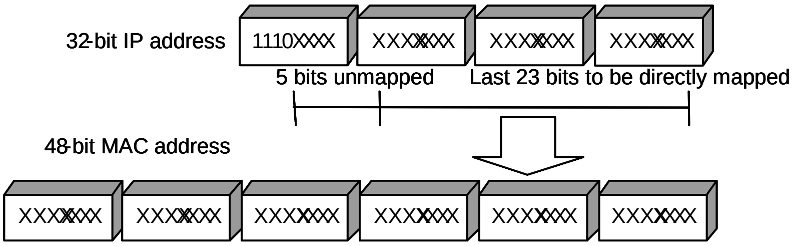


Figure 1-2 Mapping between a multicast IP address and an Ethernet MAC address

Because only 23 bits of the last 28 bits of an IP multicast address are mapped to the MAC address, a single MAC address represents 32 IP multicast addresses.

1.3 IP Multicast Protocols

Multicast involves multicast group management protocols and multicast routing protocols. Internet Group Management Protocol (IGMP), the basic signaling protocol for IP multicast, is the currently adopted multicast group management protocol. It runs between hosts and routers to inform the routers whether there are members of the multicast group on the network segment. A multicast routing protocol runs between multicast routers to create and maintain multicast routes for correct and efficient forwarding of multicast packet. At present, available multicast routing protocols are PIM-SM, PIM-DM and MSDP. The unicast routing protocol BGP, through multicast extension, can be used to transmit multicast routing information between domains.

1.3.1 Internet Group Management Protocols

Internet Group Management Protocol (IGMP) is the only protocol that can be used by hosts. It underlies the IP multicasting by defining a mechanism to establish and maintain the membership between hosts and routers. Through IGMP, a host can notify a router of the information of the related members, and a router can get from its connected host the information of other members within the group. If a user on a network declares to join a multicast group through IGMP, the multicast router on that network will transmit the information sent to this multicast group through the multicast routing protocol. Finally, that network will be added to the multicast tree as a branch. When the host, as a member of a multicast group, begins receiving the information, the router will query the group periodically to check whether other group members are still in. As long as one host is involved, the router will continue to receive data. When all users on the network quit the multicast group, the related branch will be removed from the multicast tree.

1.3.2 Multicast Routing Protocols

Multicast group uses the virtual address. In multicast, it is impossible to transmit packets directly from a source to destination as in unicast .Packets here are sent to a group of receivers (with multicast address) rather than one (with unicast address).

The multicast routing creates a loop-free data transmission path from one source to multiple receivers. The task of multicast routing protocols is to build up the distribution tree architecture. A multicast router can use multiple methods to build up a path for data transmission, that is, a distribution tree.

As in unicast routing, the multicast routing can also be intra-domain or inter-domain. Intra-domain multicast routing has been well-developed up till now. PIM-DM (Protocol Independent Multicast-Dense Mode) and PIM-SM (Protocol Independent Multicast-Sparse Mode) are the most widely used intra-domain routing protocols. The key issue for inter-domain routing is how to send routing information (or reachable information) across autonomous systems. As different autonomous systems may belong to different operators, the inter-domain routing information must contain policies of operators besides distance information. There lies the difference between the inter-domain and the intra-domain routing information.

I. Intra-domain multicast routing protocols

- PIM-DM (Protocol-Independent Multicast Dense Mode, PIM-DM)

PIM dense mode is suitable for small networks. It assumes that each subnet in the network contains at least one receiver that is interested in the multicast source. Therefore, multicast packets flood to all points over the network, causing the waste of related resources such as bandwidth and CPU of routers. To eliminate the waste, PIM dense mode prunes the branches of stations with no interest in the running multicast data flow, and periodically restores them back into forwarding status in case some stations along them turn out to need the data. To reduce the delay involved in this status recovery, PIM dense mode adopts automatic recovery by grafting mechanism. The periodical flooding and pruning are characteristics of PIM dense mode. Generally, the forwarding path of packets in dense mode is a "source tree" with a "source" root and "multicast group member" leaves. Since the source tree uses the shortest paths from the multicast source and the receivers, it is also called the shortest path tree (SPT).

- PIM-SM (Protocol-Independent Multicast Sparse Mode, PIM-SM)

The flooding-pruning technology adopted in PIM-DM is inapplicable to wide area network (WAN), where multicast members are more scattered. Sparse mode therefore predominates here. It presumes that no host needs to receive multicast packets unless there is an explicit request. A multicast router must send a join message to the corresponding RP (Rendezvous Point, which needs to be built up in the network and is the virtual place for data exchange) to ensure that the receiving stations it connects to can receive the multicast data stream. The path this join message takes through routers to the root (the RP) becomes a branch of the shared tree. Then multicast packets are sent to a RP first and then are forwarded along the shared tree which roots at this RP and stretches with "multicast member" leaves. To prevent the branches of the shared tree from being deleted before being updated, PIM sparse mode sends join messages to branches periodically to maintain the multicast distribution tree.

To send data to the specified address, the sending station should register with the RP before forwarding data to the RP. When the data reaches the RP, the multicast packet is replicated and sent to receivers along the path of the distribution tree. Replication only happens at the fork of the distribution tree. This process automatically repeats until the packets reach the destination.

II. Inter-domain multicast routing protocols

- MSDP (Multicast Source Discovery Protocol)

No ISP would like to forward multicast traffic depending on the RP of competitors, though it has to obtain information from the source and distribute it among its members, regardless of the location of the source RP. MSDP is proposed to solve this problem. It describes the interconnection mechanism of multiple PIM-SM domains and allows RPs from different domains to share the multicast source information as long as PIM-SM is the adopted intra-domain multicast routing protocol.

- MBGP multicast extension

The most popular inter-domain unicast routing protocol at present is BGP-4. Because the multicast topology may be different from the unicast topology, BGP-4 must be modified to implement the transmission of inter-domain multicast routing information. To construct inter-domain multicast routing trees, you need to know the unicast routing information as well as the information of multicast-supporting parts of the network, namely, the multicast network topology.

RFC2858 provisions the multi-protocol extension method for BGP. The extended BGP (MBGP, also written as BGP-4+) can not only carry IPv4 unicast routing information but also the routing information of other network layer protocols (such as multicast, IPv6). Carrying multicast routing information is only one of the extended functions.

1.4 IP Multicast Packet Forwarding

In the multicast model, the source host sends information to the host group represented by the multicast group address within the destination address fields of the IP packets. Different from the unicast model, the multicast model must forward the multicast packets to multiple external interfaces so that the packets can be sent to all receiving stations. Therefore, the multicast forwarding process is much more complex than the unicast forwarding process.

- RPF (Reverse Path Forwarding)

To ensure that multicast packets reach a router along the shortest path, the multicast router must check the receiving interface of multicast packets depending on the unicast routing table or a unicast routing table independently provided for multicast (such as the MBGP multicast routing table). This check mechanism is the basis for most multicast routing protocols to perform multicast forwarding, and is known as RPF (Reverse Path Forwarding) check. A multicast router uses the source address of a received multicast packet to query the unicast routing table or the independent multicast routing table to determine that the receiving interface is on the shortest path from the receiving station to the source. If a source tree is used, the source address is the address of the source host sending the multicast packet. If a shared tree is used, the source address is the RP address of the shared tree. A multicast packet arriving at the router will be forwarded according to the multicast forwarding entry if it passes the RPF check, or else, it will be discarded.

- Multicast policy routing

Multicast policy routing complements the routing table-based packet forwarding function and allows packets to be forwarded by specified policies. .

As an extension to unicast policy routing, multicast policy routing is implemented by configuring Route-policy, described by a group user-definable of IF-MATCH-APPLY statements. The IF-MATCH clauses define the matching rules, which when met, the multicast packet will be forwarded according to the actions configured by the user (described by APPLY clauses) as opposed to the usual process.

For specific configuration of multicast policy routing, please refer to the "Networking Protocol" section in this manual.

1.5 Application of Multicast

IP multicast technology effectively implements point to multi-point forwarding with high speed, saving a large amount of network bandwidth and relieving network loads. It facilitates also the development of new value-added services in the Internet information service area that include online live show, Web TV, distance education, distance medical treatment, network radio station and real-time audio/video conference. It takes a positive role in:

- Multimedia and streaming media application
- Occasional communication for training and cooperation
- Data storage and finance (stock) operation
- Point-to-multipoint data distribution

With the increasing popularity of multimedia services over IP network, multicast is gaining marketplace.

Chapter 2 Common Multicast Configuration

2.1 Common Multicast Configuration Overview

Both multicast group management protocol and multicast routing protocol are involved with common multicast configuration tasks that include enabling multicast, configuring multicast forwarding boundary, displaying multicast routing table and multicast forwarding table, etc.

2.2 Common Multicast Configuration

Basic common multicast configuration task is to:

- Enable Multicast

Advanced common multicast configuration tasks are to:

- Configure the minimum TTL of multicast packets
- Configure multicast forwarding boundary
- Configure the number limit of multicast routing entries
- Clear MFC forwarding entries or statistics
- Clear the routing entries in the multicast kernel routing table

2.2.1 Enabling Multicast

Enable multicast before enabling the multicast routing protocol.

Perform the following configuration in system view.

Table 2-1 Enable Multicast

Operation	Command
Enable Multicast	**multicast routing-enable**
Disable multicast	**undo multicast routing-enable**

By default, multicast is disabled.

⚠ **Caution:**

Only when multicast is enabled, can other multicast configurations become effective.

2.2.2 Configuring the Minimum TTL of Multicast Packets

TTL value for multicast forwarding can be configured on all interfaces that support multicast packet forwarding.

When a packet is forwarded from an interface (or a packet is sent by the local device), the minimum TTL value configured on the interface will be checked. The packet with a TTL value (The TTL of the packet has been reduced by 1 in the router) greater than the minimum value configured on the interface will be forwarded. The packet with a TTL value smaller than or equal to the minimum value configured on the interface will be discarded.

Perform the following configuration in interface view.

Table 2-2 Configure the minimum TTL of multicast packets

Operation	Command
Configure the minimum TTL of multicast packets	**multicast minimum-ttl** *ttl-value*
Remove the configuration	**undo multicast minimum-ttl**

By default, no minimum TTL is configured for multicast packet forwarding.

2.2.3 Configuring Multicast Forwarding Boundary

A multicast forwarding boundary can be configured on all interfaces that support multicast packet forwarding.

When the multicast forwarding boundary is configured on an interface, packets received and sent through the interface (including packets sent by the local device) will be filtered. Packets received from the interface are filtered before being processed with practical multicast policy routing.

Perform the following configuration in interface view.

Table 2-3 Configure multicast forwarding boundary

Operation	Command
Configure multicast forwarding boundary	**multicast packet-boundary** *acl-number*
Remove the configured multicast forwarding boundary	**undo multicast packet-boundary**

By default, no multicast boundary filtering is imposed on packets received or sent.

2.2.4 Configuring the Number Limit of Multicast Routing Entries

The number of multicast routing entries can be limited to prevent the router memory from being exhausted.

Perform the following configuration in system view.

Table 2-4 Configure the number limit of multicast routing entries

Operation	Command
Configure the number limit of multicast routing entries	**multicast route-limit** *limit*

By default, the number limit of multicast routing entries is the maximum value permitted by the system, which differs by the types of routers.

2.2.5 Clearing MFC Forwarding Entry or the Statistics

Perform the following command in user view.

Table 2-5 Clear MFC forwarding entry or the statistics

Operation	Command
Clear MFC forwarding entry or the statistics	**reset multicast forwarding-table** [**statistics**] **all** **reset multicast forwarding-table** [**statistics**] *group-address* [**mask** { *group-mask* | *group-mask-length* }] [*source-address* [**mask** { *source-mask* | *source-mask-length* }]] [**incoming-interface** *interface-type interface-number*] **reset multicast forwarding-table** [**statistics**] **slot** *slot-number*

Slot parameter **slot** *slot-number* is only used in distributed routing system.

2.2.6 Clearing Routing Entry from the Multicast Kernel Routing Table

Perform the following command in user view.

Table 2-6 Clear routing entry from the multicast kernel routing table

Operation	Command
Clear routing entry from the multicast kernel routing table	**reset multicast routing-table all** **reset multicast routing-table** *group-address* [**mask** { *group-mask* | *group-mask-length* }] [*source-address* [**mask** { *source-mask* | *source-mask-length* }]] [**incoming-interface** *interface-type interface-num*ber]

The forwarding entries in MFC are deleted along with the routing entries in the multicast kernel routing table.

2.3 Common Multicast Configuration Display and Debug

I. Displaying and Debugging

After the above configuration, execute the **display** commands in any view to display the information of multicast operating status, and to verify the effect of the configuration.

Execute the **debugging** commands in user view for the debugging of multicast.

Table 2-7 Display and debug common multicast configuration

Operation	Command
Display the multicast routing table	**display multicast routing-table** [*group-address* [**mask** { *mask* | *mask-length* }] | *source-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** }]*
Display the configuration of static multicast routes	**display multicast routing-table static** [**config**] *source-address* [*mask* | *mask-length*]
Display the multicast forwarding table	**display multicast forwarding-table** [*group-address* [**mask** { *mask* | *mask-length* }] | *source-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** }]*
Display the RPF routing information	**display multicast rpf-info** *source-address*
Enable multicast packet forwarding debugging	**debugging multicast forwarding**
Enable multicast status forwarding debugging	**debugging multicast status-forwarding**
Enable multicast kernel routing debugging	**debugging multicast kernel-routing**

Three types of multicast routing tables are involved in the multicast implementation of V 2.41: individual multicast routing tables of each multicast routing protocol; a multicast kernel routing table integrating the routing information of those individual routing tables; and a multicast forwarding table in conformity with the kernel routing table and in charge of the multicast packet forwarding.

Multicast forwarding table is mainly used in debugging. Generally, users can obtain required information by viewing multicast kernel routing table.

II. Tracing the Network Path of Multicast Data

You can use the **mtracert** command in any view to trace the network path multicast data take from multicast source to destination receiver and locate the faults.

Table 2-8 Trace the network path of multicast data

Operation	Command
Trace the network path multicast data take from multicast source to destination receiver	**mtracert** *source-address* [*last-hop-address*] [*group-address*]

- If only multicast source address is specified, the last hop address defaults to the address of a physical interface of the local router, and the group address defaults to 0.0.0.0. In that case, trace reversely hop by hop from the local router to the first hop router that connects directly to multicast source, following RPF rule.
- If only multicast source address and the last hop address are specified, the group address defaults to 0.0.0.0. In that case, trace reversely hop by hop from the last hop router to the first hop router that connects directly to multicast source, following RPF rule.
- If only source address and group address are specified, the last hop address defaults to that of a physical interface of the local router. In that case, trace reversely from the local router to the first hop router which is directly connected with multicast source, following the associated entry (S, G) in the multicast kernel routing table of each router on the path.
- If multicast source address, destination address and group address are all specified, trace reversely from the last hop router to the first hop router which is directly connected with multicast source following the corresponding entry (S, G) in the multicast kernel routing table of each router on the path.
- The trace mode is called weak trace if the group address is 0.0.0.0.

Chapter 3 IGMP Configuration

3.1 IGMP Overview

3.1.1 Introduction to IGMP

IGMP (Internet Group Management Protocol) is a protocol in the TCP/IP suite responsible for management of IP multicast members. It is used to establish and maintain multicast membership between IP hosts and their directly connected neighboring routers. The transmission and maintenance of membership information among multicast routers are completed by multicast routing protocols. All the hosts participating in multicast must support IGMP.

An IP multicast host can join or exit a multicast group at any time and any where. There is no restriction on the total number of group members. A multicast router needs not and cannot save the membership information of all the hosts. It only checks the network segment connected with each interface by IGMP to see whether there are receivers of a multicast group, namely group members. A host only needs to save the information telling to which multicast groups it joins.

IGMP is not symmetric between the host and the router. The host needs to reply, as a group member, to IGMP query messages from the multicast router. The router needs to send membership query messages periodically and to check if any host of a specified group joins to its subnet based on the received response messages. When the router receives a report on the quit of hosts, the router will send a group-specific query (IGMP Version 2) to find out if this group still has a group member.

Up till now, IGMP has three versions: IGMP Version 1 (defined by RFC1112), IGMP Version 2 (defined by RFC2236) and IGMP Version 3. At present, IGMP Version 2 is the most widely used version.

IGMP Version 2 excels Version 1 in:

I. Querier selection mechanism on a shared network segment

A shared network segment is a network segment with multiple multicast routers. In this case, all routers running IGMP on this network segment can receive the membership report from hosts. Therefore, only one router is necessary to send membership query messages. In this case, the querier selection mechanism is required to specify a router as the querier.

IGMP Version 1 selects the querier by the multicast routing protocol, while IGMP Version 2 decides on the multicast router with the lowest IP address as the querier.

II. Leave group mechanism

In IGMP Version 1, hosts leave the multicast group quietly without informing any multicast router. Only when a query message times out, can the multicast router know that a host has left the group. In IGMP Version 2, when a host replying to the last membership query message leaves a multicast group, it should send a leave group message to the all-routers multicast group.

III. Group-specific query

In IGMP Version 1, the query message of multicast router aims at all the multicast groups in the network segment. This query is called general query.

IGMP Version 2 adds group-specific query, where the IP address of a multicast group is taken as the destination IP address and the group address domain of the query message, to prevent the member hosts of other groups from replying to this message.

IV. Maximum response time

The Max Response Time is added in IGMP Version 2. It is used to dynamically adjust the allowed maximum time for a host to reply to the membership query message.

3.1.2 Introduction to IGMP Proxy

A lot of leaf networks (leaf domains) are involved in the application of a multicast routing protocol (PIM-DM for example) over a large-scaled network. It is a hard work to configure and manage these leaf networks.

To reduce the configuration and management work without affecting the multicast connection of leaf networks, you can configure an IGMP Proxy in a leaf network router (Router B in the figure). The router will then forward IGMP join or IGMP leave messages sent by the connected hosts. After the configuration of IGMP Proxy, the leaf router is no longer a PIM neighbor but a host for the exterior network. Only when the router has directly connected members, can it receive the multicast data of associated group.

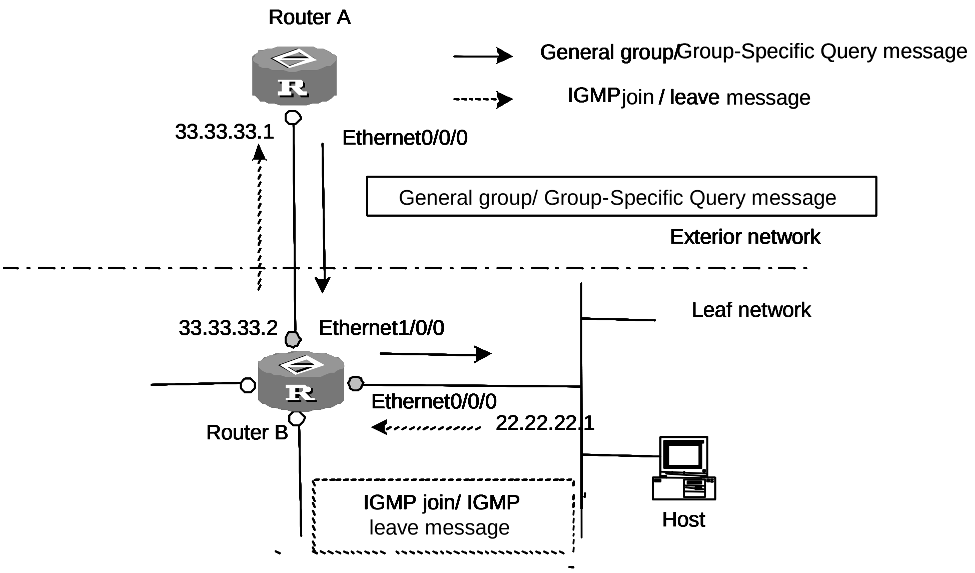


Figure 3-1 IGMP Proxy diagram

Figure 3-1 is an IGMP Proxy diagram for a leaf network.

First of all, configure PIM on Ethernet0/0/0 and Ethernet1/0/0 of Router B. Then on Ethernet0/0/0 configure Ethernet1/0/0 as the outbound IGMP proxy interface of Ethernet0/0/0 to external networks (by configuring the **igmp proxy** command).

Then configure **pim neighbor-policy** on Ethernet0/0/0 interface of Router A to filter PIM neighbors on network segment 33.33.33.0/24. That is, Router A does not consider Router B as its PIM neighbor.

In this case, when Router B of leaf network receives from Ethernet0/0/0 interface an IGMP join or IGMP leave message sent by the host, it will change the source address of the IGMP information to the outbound interface address to Router A (Ethernet 1/0/0 interface address: 33.33.33.2) and send the information to Ethernet0/0/0 interface of Router A. This works as if there is a host directed connected to Ethernet 0/0/0 interface of Router A. Similarly, when Router B receives the general group or group-specific query message from Router A, it will also change the source address of the query message to the outbound interface address of the host (Ethernet0/0/0 interface address: 22.22.22.1) and send the information from Ethernet0/0/0 interface.

In Figure 3-1, Ethernet0/0/0 interface of Router B is called the client and Ethernet1/0/0 interface of Router B is called the proxy.

3.2 IGMP Configuration

After multicast is enabled, IGMP must be enabled on the interface before other IGMP configurations.

Basic configuration tasks of IGMP include:

- Enable multicast

- Enable IGMP on an interface
- Configure IGMP proxy

Advanced configuration tasks of IGMP include:

- Configure a router as a group member
- Control the access to IP multicast group
- Configure IGMP query interval
- Configure IGMP version
- Configure Other querier present interval
- Configure IGMP Max query response time
- Limit the number of IGMP groups on an interface
- Configure Last member query interval
- Configure Last member query count
- Delete the IGMP group from the interface

3.2.1 Enabling Multicast

Multicast-related configuration will not take effect if multicast is not enabled.

Refer to “Chapter 2 Common Multicast Configuration”.

3.2.2 Enabling IGMP on an Interface

This configuration task is to enable IGMP on the interface which needs to perform multicast membership maintenance. You should execute this operation before other IGMP configurations.

Perform the following configuration in interface view.

Table 3-1 Enable IGMP on the interface

Operation	Command
Enable IGMP on the current interface	**igmp enable**
Disable IGMP on the current interface	**undo igmp enable**

By default, IGMP is disabled on the interface.

🕮 **Note:**

When running multicast, if the Ethernet interface of a router is configured with a secondary IP address, the Ethernet interfaces of other routers in the same segment must be configured with secondary IP addresses too, furthermore, all of these secondary IP address must be in the same segment.

3.2.3 Configuring IGMP Proxy

IGMP proxy can be configured to reduce the configuration and management work of the leaf network without affecting the multicast connection there.

After IGMP proxy is configured on the leaf network router, the leaf router acts as a host to the exterior network. Only when the router has directly connected members, can it receive the multicast data of the associated group.

Perform the following configuration in interface view.

Table 3-2 Configuring IGMP proxy

Operation	Command
Specify the proxy interface of the current interface	**igmp proxy** *interface-type interface-number*
Disable IGMP proxy of the interface	**undo igmp proxy**

By default, IGMP proxy is disabled.

⚠ **Caution:**

You must enable PIM on the interface before you configure the **igmp proxy** command. One interface can not be the IGMP proxy interface of two or more interfaces.

3.2.4 Configuring a Router as a Group Member

Generally, an IGMP host will reply to IGMP query messages of the multicast router. In case it fails to, the multicast router may assume there is no members of that multicast group on the network segment and cancel the path.

To avoid this situation, an interface of the router can be configured as a multicast group member. When the interface receives IGMP query message, the router will reply, and thereby the network segment of the interface can continue to receive multicast packets.

Perform the following configuration in interface view.

Table 3-3 Configure a router as group member

Operation	Command
Configure a router as a group member	**igmp host-join** *group-address*
Cancel the configuration	**undo igmp host-join** *group-address*

By default, a router does not join any multicast group.

3.2.5 Controlling the Access to IP Multicast Group

Multicast router determines the group membership of a network by received IGMP response messages. A filter can be set on each interface through access control to limit the multicast group range the interface serves.

Perform the following configuration in interface view.

Table 3-4 Controlling the access to IP multicast group

Operation	Command
Limit the multicast group range of the interface serves	**igmp group-policy** *acl-number* [**1** | **2**]
Cancel the filter configured on the interface	**undo igmp group-policy**

By default, no filter is configured on the interface, which then permits any multicast group.

3.2.6 Configuring IGMP Query Interval

The router finds out which multicast groups on its connected network segment have members by sending IGMP query messages periodically. Upon the reception of a response message, the router refreshes the membership information of the corresponding multicast group. The timeout time of the membership query message is 3 times that of the query interval.

Perform the following configuration in interface view.

Table 3-5 Configure query interval

Operation	Command
Configure query interval	**igmp timer query** *seconds*
Restore the default value of query interval	**undo igmp timer query**

When there are multiple multicast routers on a network segment, the querier is responsible to send IGMP query messages to all the hosts on the LAN.

By default, the interval is 60 seconds.

3.2.7 Configuring IGMP Version

Perform the following configuration in interface view.

Table 3-6 Configure IGMP version

Operation	Command
Select the IGMP version used by the router	**igmp version** { **1** | **2** }
Restore the default configuration	**undo igmp version**

By default, Version 2 is used.

⚠ **Caution:**

IGMP cannot convert automatically among its versions. All the routers on a subnet therefore should be configured to a same IGMP version.

3.2.8 Configuring Other Querier Present Interval

The Other Querier Present Interval is the length of time that must pass before a multicast router decides that there is no longer another multicast router which should be the querier after the querier stops sending query messages.

Perform the following configuration in Interface view.

Table 3-7 Configure the other querier present interval

Operation	Command
Configure the other querier present interval	**igmp timer other-querier-present** *seconds*
Restore the default value of the other querier present interval	**undo igmp timer other-querier-present**

By default, if a router has not received the query message for twice the query interval specified by the **igmp timer query** command, or for the other querier present interval if configured, it resumes the role of Querier.

⚠ **Caution:**

The other querier present interval shall be longer than the query interval, otherwise, the querier changes too frequent, reducing network robustness.

3.2.9 Configuring IGMP Max Query Response Time

The host, when receiving a query message from the router, will configure a timer for each multicast group it belongs to. The value of the timer is selected arbitrarily between 0 and the maximum response time. When the value of any timer reduces to 0, the host will send the membership report information for that multicast group.

Proper configuration of the maximum response time ensures that the host can reply to the query messages quickly and that the router can know the membership information of multicast groups timely.

Perform the following configuration in Interface view.

Table 3-8 Configure the maximum query response time of IGMP

Operation	Command
Configure the max query response time of IGMP	**igmp max-response-time** *seconds*
Restore the max query response time to the default value	**undo igmp max-response-time**

The shorter the max response time is, the faster the router interdicts a group. Practically, the response time is an arbitrary value within configurable range (from 1 to 25 seconds), which by default is 10 seconds.

3.2.10 Limiting the Number of IGMP Groups on an Interface

If there is no limit to the number of IGMP groups joining on a router interface or a router, the router memory may be exhausted, causing the router to fail.

The limit to IGMP groups on a router interface can be configured by users, while that to the total of IGMP groups on a router can not. It is defined by the system.

Perform the following configuration in interface view.

Table 3-9 Limit the number of IGMP groups on an interface

Operation	Command
Limit the number of IGMP groups on the interface	**igmp group-limit** *limit*
Restore the default value	**undo igmp group-limit**

By default, the maximum number of IGMP groups on an interface is 1024.

The maximum numbers of IGMP groups on interfaces differ by the router type. For a centralized router, it is 4096.

If the number of IGMP groups on an interface has exceeded the specified value during configuration, no IGMP group will be deleted.

3.2.11 Configuring Last Member Query Interval

When an IGMP querier receives an IGMP Leave Group message from a host, the last member query interval can be specified for Group-Specific Queries.

The concerned commands are valid only to IGMP Version 2, since a host running IGMP Version 1 does not send IGMP Leave Group message when it leaves a group.

Perform the following configuration in interface view.

Table 3-10 Set the last member query interval

Operation	Command
Set the last member query interval	**igmp lastmember-queryinterval** *seconds*
Restore the default value of the interval	**undo igmp lastmember-queryinterval**

By default, the interval is 1 second.

3.2.12 Configuring Last Member Query Count

When an IGMP querier receives an IGMP Leave Group message from a host, the last member query count can be specified, indicating the times of Group-Specific Queries to be sent before the router assumes there are no local members.

The concerned commands are valid only to IGMP Version 2, since a host running IGMP Version 1 does not send IGMP Leave Group message when it leaves a group.

Perform the following configuration in interface view.

Table 3-11 Set the last member query count

Operation	Command
Set the last member query count	**igmp robust-count** *robust-value*
Restore the default value of queries	**undo igmp robust-count**

By default, an IGMP group-specific query message is sent twice.

3.2.13 Deleting IGMP Group from Interface

You can delete all the IGMP groups of one or all router interfaces, or a IGMP group address or group address network segment from a specified interface.

Perform the following configuration in user view.

Table 3-12 Delete IGMP Group from Interface

Operation	Command
Delete IGMP Group from Interface	**reset igmp group** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [*group-mask*] } }

Note:

A deleted group can join in again.

3.3 IGMP Display and Debug

After the above configuration, execute the **display** commands in any view to display the running information of IGMP, and to verify the effect of the configuration.

Execute the **debugging** commands in user view for the debugging of IGMP.

Table 3-13 Display and debug IGMP

Operation	Command
Display the information about members of an IGMP multicast group	**display igmp group** [*group-address* | **interface** *interface-type interface-number* | **local**]
Display the IGMP configuration and running information of an interface	**display igmp interface** [*interface-type interface-number*]
Enable the IGMP debugging	**debugging igmp** { **all** | **event** | **host** | **packet** | **timer** }

3.4 Typical IGMP Configuration Example

I. Network requirements

Enable IGMP and PIM-DM on the interfaces of Routers A and B as shown in Figure 3-2.

Assign interface Ethernet0/0/0 to multicast group 224.0.1.1 and use interface Ethernet1/0/0 as its IGMP proxy on Router B. (Refer to the next chapter for the PIM-DM configuration.)

Note:

This example only provides the configurations of IGMP and IGMP proxy.

II. Network diagram

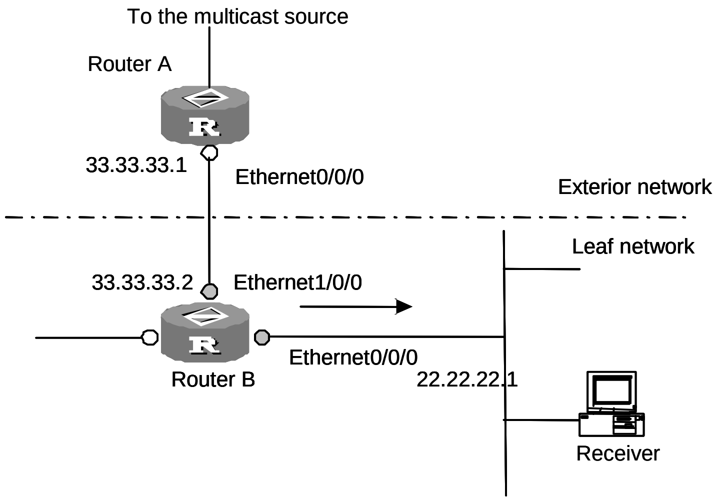


Figure 3-2 IGMP network diagram

III. Configuration procedure

1) Configure Router B:

# Enable multicast.

```
[RouterB] multicast routing-enable
```

# Enable IGMP and PIM-DM on interfaces Ethernet0/0/0 and Ethernet1/0/0.

```
[RouterB] interface ethernet 0/0/0
[RouterB-Ethernet0/0/0] ip address22.22.22.1 24
[RouterB-Ethernet0/0/0] igmp enable
[RouterB-Ethernet0/0/0] pim dm
[RouterB-Ethernet0/0/0] igmp host-join 224.0.1.1
[RouterB-Ethernet0/0/0] interface ethernet 1/0/0
[RouterB-Ethernet1/0/0] ip address 33.33.33.2 24
[RouterB-Ethernet1/0/0] igmp enable
[RouterB-Ethernet1/0/0] pim dm
[RouterB-Ethernet1/0/0] quit
```

# Configure the interface Ethernet1/0/0 as the IGMP proxy interface of Ethernet0/0/0.

```
[RouterB] interface ethernet 0/0/0
[RouterB-Ethernet0/0/0] igmp proxy ethernet1/0/0
```

2) Configure Router A:

# Enable multicast.

```
[RouterA] multicast routing-enable
```

# Enable IGMP and PIM-DM on the interface Ethernet0/0/0.

```
[RouterA] interface ethernet 0/0/0
```

```
[RouterA-Ethernet0/0/0] igmp enable
[RouterA-Ethernet0/0/0] pim dm
```

# Configure interface Ethernet0/0/0 to exclude 33.33.33.2 as one of its PIM neighbors.

```
[RouterA-Ethernet0/0/0] pim neighbor-policy 2001
[RouterA-Ethernet0/0/0] quit
[RouterA] acl number 2001
[RouterA-acl-basic-2001] rule deny source 33.33.33.2 0
[RouterA-acl-basic-2001] rule permit source any
```

3) Configure Receiver

Receiver sets up an HTTP connection to the multicast source first, listing the current programs of the multicast source on the client software. Each of these programs is associated with a different multicast address or multicast group. When a program is selected, the client software sends automatically an IGMP message to join this multicast group. Then, Receiver can receive the multicast program.

Chapter 4 PIM Configuration

4.1 PIM Overview

4.1.1 PIM-DM

PIM-DM (Protocol Independent Multicast, Dense Mode) is a kind of multicast routing protocol suitable for small-scaled networks where multicast group members are relatively dense.

The operation of PIM-DM includes neighbor discovery, flooding and pruning, and grafting.

I. Neighbor discovery

The PIM-DM router discovers neighbors by sending Hello message when it starts. Hello messages are periodically sent among network nodes to keep them in contact.

II. Flooding and Pruning

PIM-DM assumes that all hosts on the network are ready to receive multicast data.

When a router receives a multicast packet from a multicast source "S" to a multicast group "G", it begins with RPF check by the unicast routing table. If the RPF check passes, the router will create an entry(S, G) and forward the packet to all the downstream PIM-DM nodes. That is the process of flooding. If the RPF check fails, that is, the multicast packet arrives at a wrong interface, the packet will be discarded, but a (S, G) entry is created in the PIM-DM multicast domain.

If there is no multicast group member in the downstream nodes, the router will send a prune message to the upstream nodes to inform them not to forward data any more. The upstream nodes, as informed, will remove the relative interface from the outgoing interface list corresponding to the multicast forwarding entry (S, G). In this way, a SPT (Shortest Path Tree) rooted at source S is built. The pruning process is initiated by routers.

The above process is called "Flooding and Pruning". Each pruned nodes are provided with timeout mechanism to restart "Flooding and Pruning" operation periodically.

III. RPF check

PIM-DM builds upon the present unicast routing table a data source-rooted multicast forwarding tree to conduct RPF check. When a multicast packet arrives, the router first checks the path. If the interface this packet reaches is the one along the unicast route towards the multicast source, the path is considered correct. Otherwise, the multicast packet will be discarded as a redundant one. The concerned unicast routing information can be of any unicast routing protocol such as RIP or OSPF.

IV. Assert mechanism

As shown in Figure 4-1, Routers A and B are on the same LAN network segment, but have different paths to the multicast source S. Therefore, both will forward the multicast packet received from S over the LAN, and the multicast router C at the downstream node will receive two identical multicast packets.

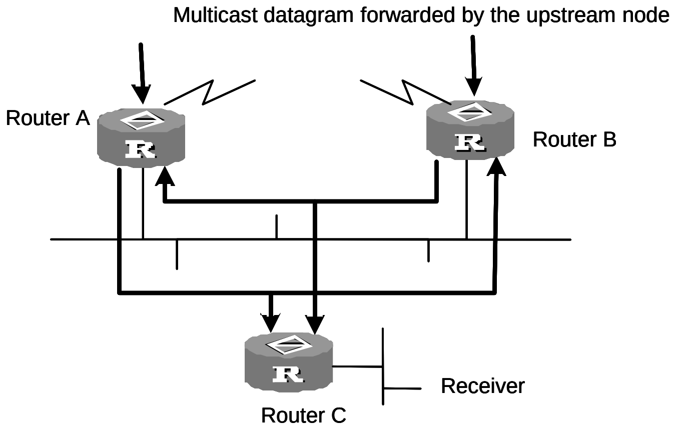


Figure 4-1 Assert mechanism diagram

Assert mechanism helps in choosing a single forwarder in that case. By sending Assert packet, a router can find the shortest path. If two or more paths have the same priority and cost, decide by the IP address of the forwarding routers along the paths. The one with greater IP address is to be selected as the upstream neighbor of the (S, G) entry, which is responsible for forwarding the (S, G) multicast packet.

V. Grafting

When a pruned downstream node needs to be restored to the forwarding state, it may send a graft packet to the upstream node.

4.1.2 PIM-SM

PIM-SM (Protocol Independent Multicast, Sparse Mode) is a kind of multicast routing protocol mainly used in the large-scaled networks where group members are scattered sparsely.

As opposed to PIM-DM, PIM-SM assumes that no host needs the multicast packets, unless there is an explicit request.

PIM-SM sends multicast information to all PIM-SM routers by configuring the RP (Rendezvous Point) and the BSR (Bootstrap Router), and builds the RP-rooted shared tree (RPT) using the join/prune information of the routers to reduce the bandwidth occupied by data packets and control packets as well as the processing costs. Multicast data flows along the shared tree to the network segments where the multicast group members are. When the data traffic is massive, the SPT (Shortest Path Tree) rooted on the source can be used to reduce network delay.

PIM-SM depends on whichever present unicast routing table to perform the RPF check instead of an unicast routing protocol.

I. PIM-SM Working Principle

The operation of PIM-SM includes neighbor discovery, Rendezvous point tree (RPT) establishment, multicast source registration and SPT switching. Neighbor discovery mechanism is the same with that of PIM-DM and will not be addressed here.

1) Rendezvous point tree (RPT) establishment

A leaf router locates the corresponding RP when it notices through IGMP packets that a host directly connected to it joins in the multicast group G. It then sends the join message to the upstream node towards the RP. Each router along the path between the leaf router and the RP generates a (*, G) entry in the forwarding table, covering all packets sent to the multicast group G, regardless of the sources. When receiving a packet sent to multicast group G, the RP forwards it through the established path to the leaf router and then to the host. In this way, an RP-rooted tree (RPT) is built as shown in the following figure.

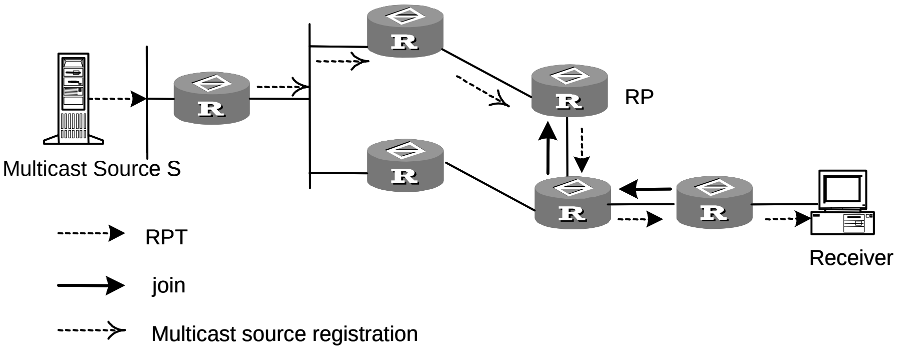


Figure 4-2 RPT diagram

2) Multicast source registration

The multicast source S sends a multicast packet to the multicast group G. When the PIM-SM multicast router directly connected to S receives the packet, it will encapsulate the packet into a register packet and send it to the corresponding RP in unicast form. If there are multiple PIM-SM multicast routers on a network segment, the Designated Router (DR) will be responsible to send the multicast packet.

3) SPT switching

When a multicast router detects that the multicast packet with the destination address of G from the RP is sent at a rate greater than the threshold, the multicast router will send a join message to the node of a higher level toward the source S, which results in switching from the RPT to the SPT.

II. Preparation before configuring PIM-SM

1) Configure Candidate-RPs

In a PIM-SM network, multiple Candidate-RPs (C-RPs) can be configured. Each C-RP is responsible for forwarding multicast packets with the destination addresses in a certain range, implementing RP load balancing. These C-RPs are equal. All multicast routers calculate the RP for a connected multicast group by the same algorithm after receiving the RP information reported by the BSR.

It should be noted that one RP can serve multiple or all multicast groups, while a multicast group can have one RP at a time.

2) Configure BSR

BSR is the management kernel of the PIM-SM networks. It is responsible for collecting and broadcasting the information sent by C-RPs.

There can be only one BSR in a network but multiple Candidate-BSRs (C-BSRs). In this case, if the BSR fails, a candidate can assume its role by automatic election..

3) Configure static RP

RP is the kernel router for the multicast routing. If the dynamic RP elected by BSR mechanism fails, a static RP can be configured. As the backup of dynamic RP, static RP improves robustness and operability of the multicast network.

4.2 PIM-DM Configuration

Basic configuration tasks of PIM-DM include:

- Enable Multicast
- Enable IGMP on an interface
- Enter PIM view
- Enable PIM-DM

Advanced configuration tasks of PIM-DM include:

- Configure the interval of Hello messages
- Configure multicast source (group) policy
- Configure PIM neighbor policy
- Limit the number of PIM neighbors of an interface

4.2.1 Enabling Multicast

Refer back to the chapter “Common Multicast Configuration”.

4.2.2 Enabling IGMP on an Interface

Refer back to the chapter "IGMP Configuration".

4.2.3 Enabling PIM-DM

If enabled on an interface, PIM-DM sends PIM Hello message periodically and process protocol packets from PIM neighbors.

Perform the following configuration in interface view.

Table 4-1 Enable PIM-DM

Operation	Command
Enable PIM-DM on an interface	**pim dm**
Disable PIM-DM from an interface	**undo pim dm**

Only after the multicast route is enabled, can PIM-DM be valid. PIM-DM or PIM-SM are exclusive on a same interface.

When the router runs in the PIM-DM domain, it is recommended to enable PIM-DM on all the interfaces of the non-border router.

4.2.4 Entering PIM View

To configure PIM-related global parameters, you need to enter PIM view.

Perform the following configuration in system view.

Table 4-2 Enter PIM view

Operation	Command
Access PIM view	**pim**
Clear all the configurations in PIM view	**undo pim**

⚠ **Caution:**

Using the **undo pim** command clears all the configurations in PIM view.

4.2.5 Configuring Hello Message Interval

Once enabled on an interface, PIM will send periodically Hello messages.

Perform the following configuration in interface view.

Table 4-3 Configuring the interval of Hello messages

Operation	Command
Configure the Hello message interval on an interface	**pim timer hello** *seconds*
Restore the default value of the interval	**undo pim timer hello**

By default, Hello messages are sent at an interval of 30 seconds.

4.2.6 Configuring Multicast Source (Group) Policy

Received multicast data packets or register packets can be filtered by the contained source/group addresses to enhance the network security.

Perform the following configuration in PIM view.

Table 4-4 Configure multicast source (group) policy

Operation	Command
Filter the received multicast data packets by their source/group addresses	**source-policy** *acl-number*
Cancel the configuration	**undo source-policy**

If the basic access control list is configured, all the multicast data packets received will have their source addresses matched. The packets with source addresses beyond those in the list will be discarded.

If the advanced access control list is configured, all the multicast data packets received will have their source and group addresses matched. The packets with source addresses and/or group addresses beyond those in the list will be discarded.

4.2.7 Configuring PIM Neighbor Policy

You can filter among routers for PIM neighbors of the current interface by configuring Access control list.

Perform the following configuration in interface view.

Table 4-5 Configure PIM neighbor policy

Operation	Command
Filter among routers for PIM neighbor	**pim neighbor-policy** *acl-number*
Cancel the configuration	**undo pim neighbor-policy**

4.2.8 Limiting the Number of PIM Neighbors on an Interface

The maximum number of PIM neighbors of an router interface can be configured to avoid exhausting EMS memory of the router or router faults. The maximum number of PIM neighbors of a router however is defined by the system, and is not open for modification.

Perform the following configuration in interface view.

Table 4-6 Configure the maximum number of PIM neighbors of an interface

Operation	Command
Configure the maximum number of PIM neighbors of an interface	**pim neighbor-limit** *limit*
Restore the default value	**undo pim neighbor-limit**

By default, the maximum number of PIM neighbors of an interface is 128.

You cannot delete those PIM neighbors beyond the configured limit however, if they exist before you configure the limit.

4.3 PIM-SM Configuration

Basic configuration tasks of PIM-SM include:

- Enable Multicast
- Enable IGMP on an interface
- Enable PIM-SM
- Enter PIM view
- Configure PIM-SM domain boundary
- Configure Candidate-BSR
- Configure Candidate-RP
- Configure static RP

Advanced configuration tasks of PIM-SM include:

- Configure Hello message interval
- Configure multicast source (group) policy
- Configure PIM neighbor policy
- Limit the number of PIM neighbors of an interface
- Configure RP register policy
- Configure the threshold to switch from RPT to SPT
- Configure BSR policy
- Configure C-RP policy
- Clear PIM routing entries
- Clear PIM neighbors

It is noteworthy that at least one router in an entire PIM-SM domain should be configured with Candidate-RP and Candidate-BSR.

4.3.1 Enabling Multicast

Refer back to the chapter “Common Multicast Configuration”.

4.3.2 Enabling IGMP on the Interface

Refer backup to the chapter “IGMP Configuration”.

4.3.3 Enabling PIM-SM

This configuration can be effective only after multicast is enabled.

Perform the following configuration in interface view.

Table 4-7 Enable PIM-SM

Operation	Command
Enable PIM-SM on an interface	**pim sm**
Disable PIM-SM from the interface	**undo pim sm**

Repeat this operation to enable PIM-SM on other interfaces. Only one multicast routing protocol can be enabled on an interface at a time. Once PIM-SM is enabled on an interface, PIM-DM cannot be enabled on it, and vice versa.

4.3.4 Entering PIM View

Refer back to the section “PIM-DM Configuration” in this chapter.

4.3.5 Configuring PIM-SM Domain Boundary

If the PIM-SM domain boundary is configured, bootstrap messages cannot cross it in any direction. In this way, the PIM-SM domain can be split.

Perform the following configuration in interface view.

Table 4-8 Configure PIM-SM domain boundary

Operation	Command
Configure PIM-SM domain boundary	**pim bsr-boundary**
Remove the configured PIM-SM domain boundary	**undo pim bsr-boundary**

By default, no domain boundary is configured. If configured, it confines bootstrap messages but not other PIM packets, thus effectively dividing the network into domains using different BSRs.

4.3.6 Configuring Candidate-BSR

In a PIM domain, one or more C-BSRs should be configured. A BSR (Bootstrap Router) is elected automatically among C-BSRs, to take charge of RP information collecting and broadcasting. The automatic election among C-BSRs is described as follows:

One PIM-SM-enabled interface shall be specified when configuring a router as a C-BSR.

At first, every C-BSR regards itself as the BSR of the PIM-SM domain and sends Bootstrap message, taking the IP address of the specified interface as the BSR address.

When receiving a Bootstrap message from another router, the C-BSR compares the BSR address and the priority of that router with those of itself. When they are of equal priority, the one with greater BSR address is considered the BSR. Specifically, if the BSR address of the received message is greater, the C-BSR will replace its BSR address with it and stop regarding itself as the BSR. Otherwise, it will keep its BSR address as well as the BSR role.

Perform the following configuration in PIM view.

Table 4-9 Configure a C-BSR

Operation	Command
Configure a C-BSR	**c-bsr** *interface-type interface-number hash-mask-len* [*priority*]
Cancel the configuration	**undo c-bsr**

C-BSRs should be configured on the routers in the backbone network. By default, no C-BSR is configured. The default value of the priority is 0.

⚠ **Caution:**

One router can only be configured with one candidate-BSR. When a new candidate-BSR is configured on another interface, it will replace the previous one.

For multicast BSR information learning through GRE-Tunnel, the multicast static route should be configured to guarantee the next hop towards BSR is a GRE interface.

The multicast static route should be reasonably configured to avoid the routing loopback.

4.3.7 Configuring Candidate-RP

In PIM-SM, a shared tree roots at an RP, with one or possibly many multicast groups mapped to the RP.

Perform the following configuration in PIM view.

Table 4-10 Configure a C-RP

Operation	Command
Configure a C-RP	**c-rp** *interface-type interface-number* [**group-policy** *acl-number*] [**priority** *priority-value*]
Cancel the configuration	**undo c-rp** { *interface-type interface-number* | **all** }

When configuring a C-RP, if the range of the served multicast groups is not specified, it will serve all multicast groups. Otherwise, it will serve only those within the specified range. It is suggested to configure C-RPs on routers over backbone network.

⚠ **Caution:**

In this command, parameter *acl-number* is not used to perform match filtering, but to define the range of a group. The range of groups under **permit** will be broadcasted as the served group range of RP. The other choices such as **deny** are disabled.

4.3.8 Configuring Static RP

RP is the core router in multicast routing. Since the dynamic RP elected through the BSR mechanism may fail, you can configure a static RP as a standby RP to enhance the robustness as well as the operability of the multicast network.

Perform the following configuration in PIM view.

Table 4-11 Configure a static RP

Operation	Command
Configure a static RP	**static-rp** *rp-address* [*acl-number*]
Remove the configured static RP	**undo static-rp**

If a static RP is in use, all routers in the PIM domain must adopt the same configuration. If the configured static RP address is the interface address of the local router under UP state, the router will function as the static RP. It is unnecessary to enable PIM on the interface that functions as static RP.

Basic ACL can be used to control the range of multicast group served by a static RP.

When the RP elected by BSR mechanism is valid, static RP does not work.

4.3.9 Configuring Hello message Interval

After PIM is enabled on an interface, it will send Hello messages at specified intervals.

Perform the following configuration in interface view.

Table 4-12 Configuring Hello message interval

Operation	Command
Configure the Hello message interval on an interface	**pim timer hello** *seconds*
Restore the default value of the interval	**undo pim timer hello**

By default, Hello message are sent at the interval of 30 seconds.

4.3.10 Configuring Multicast Source (Group) Policy

Refer back to the section “PIM-DM Configuration” in this chapter.

4.3.11 Configuring PIM Neighbor Policy

Refer back to the section “PIM-DM Configuration” in this chapter.

4.3.12 Limiting the Number of PIM Neighbors on an Interface

Refer back to the section “PIM-DM Configuration” in this chapter.

4.3.13 Configuring RP Register Policy

In the PIM-SM network, the register packet filtering mechanism helps an RP to decide the groups a source sends packets to, namely the packets to receive and forward.

Perform the following configuration in PIM view.

Table 4-13 Configure RP register policy

Operation	Command
Configure RP register policy on the packets from DR	**register-policy** *acl-number*
Cancel the configured policy	**undo register-policy**

If the entry (S, G) of a source group is denied or not defined by the ACL, or there is no ACL, the RP will send RegisterStop information to the DR to stop the registration of this multicast data stream.

⚠ **Caution:**

Only the register packets matching the ACL **permit** clause will be accepted by the RP. Specifying an undefined ACL will cause the RP to deny all register packets.

4.3.14 Configuring the Threshold to Switch from RPT to SPT

The PIM-SM routers use the shared tree to forward multicast data packets initially. If the traffic rate exceeds the specified threshold, the last hop router the packet passes will initiate the switch from the shared tree to the shortest path tree.

Perform the following configuration in PIM view.

Table 4-14 Configure the threshold to switch from the RPT to the SPT

Operation	Command
Set the threshold to switch from the RPT to the SPT	**spt-switch-threshold** { *traffic-rate* | **infinity** } [**group-policy** *acl-number*]
Restore the default configuration	**undo spt-switch-threshold** { *traffic-rate* | **infinity** } [**group-policy** *acl-number*]

By default, the threshold is 0. In that case, the last hop router turns to the shortest path tree when it receives the first multicast datagram.

4.3.15 Configuring BSR Policy

To prevent the valid BSRs from being maliciously replaced or BSR spoofing, BSR policy can be configured to specify the valid BSR range. Information from BSRs out of this range will not be accepted.

Perform the following configuration in the appropriate view.

Table 4-15 Configuring BSR policy

Operation	Command
Specify the range of valid BSRs (in PIM view)	**bsr-policy** *acl-number*
Restore the normal state without any range limitation (in PIM view)	**undo bsr-policy**

Operation	Command
Create an ACL (in system view)	**acl number** *acl-number* [**basic** | **advanced** | **interface**]
Define rules for a basic ACL (in basic ACL view)	**rule** [*rule-id*] { **permit** | **deny** } [**source** *sour-addr sour-wildcard* | **any**]

For the details of the **bsr-policy** command, refer to *Command Manual*.

4.3.16 Configuring C-RP Policy

To prevent C-RP spoofing, C-RP policy can be configured to specify the range of valid C-RPs and of groups served by each C-RP.

Perform the following configuration in the appropriate view.

Table 4-16 Configure C-RP policy

Operation	Command
Specify the range of valid C-RPs (in PIM view)	**crp-policy** *acl-number*
Restore the normal state without any range limitation (in PIM view)	**undo crp-policy**
Create an ACL (in system view)	**acl number** *acl-number* [**basic** | **advanced** | **interface**]
Define rules for a basic ACL (in advanced ACL view)	**rule** [*rule-id*] { **permit** | **deny** } *protocol* [**source** *sour-addr sour-wildcard* | **any**] [**destination** *dest-addr dest-mask* | **any**]

For the details of the **crp-policy** command, refer to *V 2.41 Command Manual*.

4.3.17 Clearing PIM Routing Entries

Perform the following command in user view.

Table 4-17 Clearing PIM routing entries

Operation	Command
Clear PIM routing entries	**reset pim routing-table** { **all** | { *group-address* [**mask** *group-mask* | **mask-length** *group-mask-length*] | *source-address* [**mask** *source-mask* | **mask-length** *source-mask-length*] | { **incoming-interface** { *interface-type interface-number* | **null** } } } * }

4.3.18 Clearing PIM Neighbors

Perform the following command in user view.

Table 4-18 Clear PIM neighbors

<table>
<tr><th>Operation</th><th>Command</th></tr>
<tr><td>Clear PIM neighbors</td><td><b>reset pim neighbor</b> { <b>all</b> | { <i>neighbor-address</i> | <b>interface</b> <i>interface-type interface-number</i> } * }</td></tr>
</table>

4.4 PIM Display and Debugging

Upon the above configuration, you can use the **display** commands in any view to display the running information of PIM, and to verify the effect of the configuration.

Execute the **debugging** commands in user view for the debugging of PIM.

Table 4-19 Display and debug PIM

<table>
<tr><th>Operation</th><th>Command</th></tr>
<tr><td>Display a PIM multicast routing table</td><td><b>display pim routing-table</b> [{ { <b>*g</b> [<i>group-address</i> [<b>mask</b> { <i>mask-length</i> | <i>mask</i> }]] | <b>**rp</b> [<i>rp-address</i> [<b>mask</b> { <i>mask-length</i> | <i>mask</i> }]] } | { <i>group-address</i> [<b>mask</b> { <i>mask-length</i> | <i>mask</i> }] | <i>source-address</i> [<b>mask</b> { <i>mask-length</i> | <i>mask</i> }] } <b>*</b> } | <b>incoming-interface</b> { <i>interface-type interface-num</i> | <b>null</b> } | { <b>dense-mode</b> | <b>sparse-mode</b> }] <b>*</b></td></tr>
<tr><td>Display the information of a PIM interface</td><td><b>display pim interface</b> [<i>interface-type interface-number</i>]</td></tr>
<tr><td>Display the information about PIM neighboring routers</td><td><b>display pim neighbor</b> [<b>interface</b> <i>interface-type interface-number</i>]</td></tr>
<tr><td>Display BSR information</td><td><b>display pim bsr-info</b></td></tr>
<tr><td>Display RP information</td><td><b>display pim rp-info</b> [<i>group-address</i>]</td></tr>
<tr><td>Enable PIM debugging</td><td><b>debugging pim common</b> { <b>all</b> | <b>event</b> | <b>packet</b> | <b>timer</b> }</td></tr>
<tr><td>Enable PIM-DM debugging</td><td><b>debugging pim dm</b> { <b>alert</b> | <b>all</b> | <b>mrt</b> | <b>timer</b> | <b>warning</b> | { <b>recv</b> | <b>send</b> } { <b>all</b> | <b>assert</b> | <b>graft</b> | <b>graft-ack</b> | <b>join</b> | <b>prune</b> } }</td></tr>
<tr><td>Enable PIM-SM debugging</td><td><b>debugging pim sm</b> { <b>all</b> | <b>mbr</b> | <b>register-proxy</b> | <b>mrt</b> | <b>timer</b> | <b>verbose</b> | <b>warning</b> | { <b>recv</b> | <b>send</b> } { <b>assert</b> | <b>bootstrap</b> | <b>crpadv</b> | <b>jp</b> | <b>reg</b> | <b>regstop</b> } }</td></tr>
</table>

Note:

The **debugging pim sm register-proxy** command can only be used to enable the debugging in distributed routers where the interface board substitutes the main control board to send register packets.

4.5 PIM Configuration Example

4.5.1 PIM-DM Configuration

I. Network requirements

In the following figure, RECEIVER1 and RECEIVER 2 are two receivers of the Movies Online program provided by Multicast Source.

Note:

In practice, a network may comprise routing devices of different vendors that run different routing protocols. In this example, the routing protocol is OSPF.

II. Network diagram

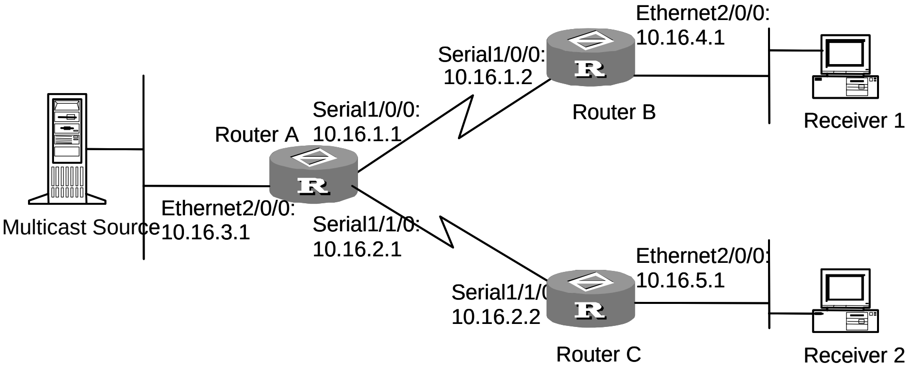


Figure 4-3 Network diagram for PIM-DM configuration

III. Configuration procedure

1) Configure Router A:

# Enable multicast.

```
<3Com> system-view
[3Com] multicast routing-enable
```

# Enable PIM-DM on the interfaces Ethernet2/0/0, Serial1/0/0 and Serial1/1/0 respectively.

```
[3Com] interface serial 1/0/0
[3Com-Serial1/0/0] pim dm
[3Com-Serial1/0/0] ip address 10.16.1.1 24
[3Com-Serial1/0/0] quit
[3Com] interface serial 1/1/0
[3Com-Serial1/1/0] pim dm
[3Com-Serial1/1/0] ip address 10.16.2.1 24
[3Com-Serial1/1/0] quit
[3Com] interface ethernet 2/0/0
[3Com-Ethernet2/0/0] pim dm
[3Com-Ethernet2/0/0] ip address 10.16.3.1 24
[3Com-Ethernet2/0/0] quit
```

# Enable OSPF on interfaces Ethernet2/0/0, Serial1/0/0, and Serial1/1/0.

```
[3Com] ospf
[3Com-ospf-1] area 0
[3Com-ospf-1-area-0.0.0.0] network 10.16.1.0 0.0.0.255
[3Com-ospf-1-area-0.0.0.0] network 10.16.2.0 0.0.0.255
[3Com-ospf-1-area-0.0.0.0] network 10.16.3.0 0.0.0.255
[3Com-ospf-1-area-0.0.0.0] quit
[3Com-ospf-1] quit
```

2) Configure Router B:

# Enable multicast.

```
<3Com> system-view
[3Com] multicast routing-enable
```

# Enable PIM-DM on interface Serial1/0/0.

```
[3Com] interface serial 1/0/0
[3Com-Serial1/0/0] pim dm
[3Com-Serial1/0/0] ip address 10.16.1.2 24
[3Com-Serial2/0/0] quit
```

# Enable PIM-DM on interface Ethernet2/0/0.

```
[3Com] interface ethernet 2/0/0
[3Com-Ethernet2/0/0] igmp enable
[3Com-Ethernet2/0/0] pim dm
[3Com-Ethernet2/0/0] ip address 10.16.4.1 24
```

# Enable OSPF on interfaces Ethernet2/0/0 and Serial1/0/0.

```
[3Com] ospf
[3Com-ospf-1] area 0
[3Com-ospf-1-area-0.0.0.0] network 10.16.1.0 0.0.0.255
```

```
[3Com-ospf-1-area-0.0.0.0] network 10.16.4.0 0.0.0.255
[3Com-ospf-1-area-0.0.0.0] quit
[3Com-ospf-1] quit
```

3) Configure Router C:

# Enable multicast.

```
<3Com> system-view
[3Com] multicast routing-enable
```

# Enable PIM-DM on the interfaces Serial1/1/0 and Ethernet2/0/0.

```
[3Com] interface serial 1/1/0
[3Com-Serial1/1/0] pim dm
[3Com-Serial1/1/0] ip address 10.16.2.2 24
[3Com-Serial1/1/0] quit
[3Com] interface ethernet 2/0/0
[3Com-Ethernet2/0/0] igmp enable
[3Com-Ethernet2/0/0] pim dm
[3Com-Ethernet2/0/0] ip address 10.16.5.1 24
```

# Enable OSPF on interfaces Ethernet2/0/0 and Serial1/1/0.

```
[3Com] ospf
[3Com-ospf-1] area 0
[3Com-ospf-1-area-0.0.0.0] network 10.16.1.0 0.0.0.255
[3Com-ospf-1-area-0.0.0.0] network 10.16.5.0 0.0.0.255
[3Com-ospf-1-area-0.0.0.0] quit
[3Com-ospf-1] quit
```

4) Configure Multicast Source

On Multicast Source associate multicast programs with multicast addresses, for example, Movie Online with 224.0.1.1.

5) Configure Receiver1/2

Connect Receiver to Multicast Source using HTTP, and select the Movie Online program on the client software.

4.5.2 PIM-SM Configuration

I. Network requirements

In the following figure, Host A is a receiver of the Movies Online program provided by Multicast Source. On Router B, specify interface Serial1/0/0 as an RP candidate and BSR candidate.

Note:

In practice, a network may comprise routing devices of different vendors that run different routing protocols. In this example, the routing protocol is OSPF.

II. Network diagram

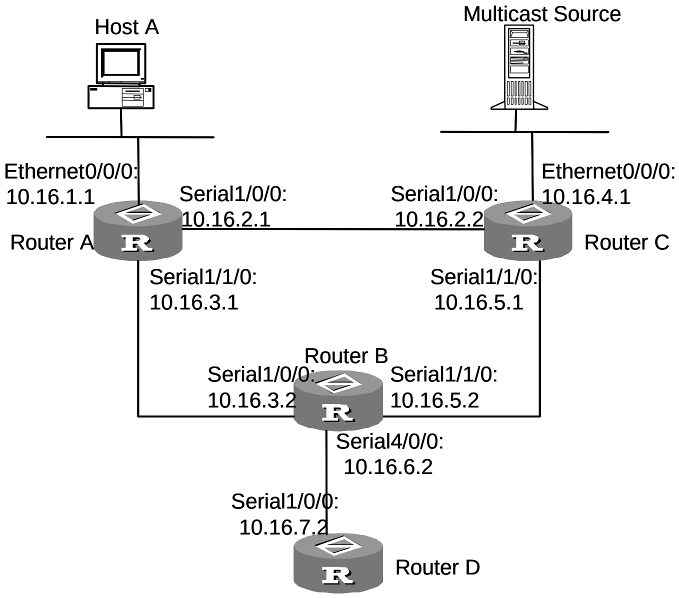


Figure 4-4 Network diagram for PIM-SM configuration

III. Configuration procedure

1) Configure Router A:

# Enable PIM-SM.

```
<RouterA> system-view
[RouterA] multicast routing-enable
[RouterA] interface ethernet 0/0/0
[RouterA-Ethernet0/0/0] pim sm
[RouterA-Ethernet0/0/0] igmp enable
[RouterA-Ethernet0/0/0] ip address 10.16.1.1 24
[RouterA-Ethernet0/0/0] quit
[RouterA] interface serial 1/0/0
[RouterA-Serial1/0/0] pim sm
[RouterA-Serial1/0/0] ip address 10.16.2.1 24
[RouterA-Serial1/0/0] quit
[RouterA] interface serial 1/1/0
[RouterA-Serial1/1/0] pim sm
[RouterA-Serial1/1/0] ip address 10.16.3.1 24
```

# Configure the threshold for a specified multicast group to switch from the shared tree to the shortest path tree to 10 kbps.

```
[RouterA] acl number 2005
[RouterA-acl-basic-2005] rule permit source 224.0.1.1 0.0.0.255
[RouterA-acl-basic-2005] quit
[RouterA] pim
[RouterA-pim] spt-switch-threshold 10 group-policy 2005
```

# Enable OSPF on interfaces Ethernet0/0/0, Serial1/0/0, and Serial1/1/0.

```
[RouterA] ospf
[RouterA-ospf-1] area 0
[RouterA-ospf-1-area-0.0.0.0] network 10.16.1.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 10.16.2.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] network 10.16.3.0 0.0.0.255
[RouterA-ospf-1-area-0.0.0.0] quit
[RouterA-ospf-1] quit
```

2) Configure Router C:

# Enable PIM-SM.

```
<RouterC> system-view
[RouterC] multicast routing-enable
[RouterC] interface ethernet 0/0/0
[RouterC-Ethernet0/0/0] pim sm
[RouterC-Ethernet0/0/0] ip address 10.16.4.1 24
[RouterC-Ethernet0/0/0] quit
[RouterC] interface serial 1/0/0
[RouterC-Serial1/0/0] pim sm
[RouterC-Ethernet0/0/0] ip address 10.16.2.2 24
[RouterC-Serial1/0/0] quit
[RouterC] interface serial 1/1/0
[RouterC-Serial1/1/0] pim sm
[RouterC-Ethernet0/0/0] ip address 10.16.5.1 24
```

# Enable OSPF on interfaces Ethernet0/0/0, Serial1/0/0, and Serial1/1/0.

```
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 10.16.4.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 10.16.2.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 10.16.5.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

3) Configure Router B:

# Enable PIM-SM.

```
<RouterB> system-view
[RouterB] multicast routing-enable
[RouterB] interface serial 1/0/0
[RouterB-Serial1/0/0] pim sm
[RouterB-Serial1/0/0] ip address 10.16.3.2 24
[RouterB-Serial1/0/0] quit
[RouterB] interface serial 1/1/0
[RouterB-Serial1/1/0] pim sm
[RouterB-Serial1/1/0] ip address 10.16.5.2 24
[RouterB-Serial1/1/0] quit
[RouterB] interface serial 4/0/0
[RouterB-Serial4/0/0] pim sm
[RouterB-Serial4/0/0] ip address 10.16.6.2 24
[RouterB-Serial4/0/0] quit
```

# Configure a BSR candidate.

```
[RouterB] pim
[RouterB-pim] c-bsr serial 1/0/0 30 2
[RouterB-pim] quit
```

# Configure an RP candidate.

```
[RouterB] acl number 2005
[RouterB-acl-basic-2005] rule permit source 224.0.1.1 0 0.255.255.255
[RouterB-acl-basic-2005] quit
[RouterB] pim
[RouterB-pim] c-rp serial 1/0/0 group-policy 2005
[RouterB-pim] quit
```

# Configure PIM boundary.

```
[RouterB] interface serial4/0/0
[RouterB-Serial4/0/0] pim bsr-boundary
```

# Enable OSPF on interfaces Serial4/0/0, Serial1/0/0, and Serial1/1/0.

```
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 10.16.3.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 10.16.5.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 10.16.6.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
[RouterC-ospf-1] quit
```

4) Configure Host A

Connect Host to Multicast Source using HTTP, and select the Movie Online program on the client software.

5) Configure Multicast Source

On Multicast Source associate multicast programs with multicast addresses, for example, Movie Online with 224.0.1.1.

After you configure the boundary on interface Serial4/0/0, Router D can no longer receive BSR information from Router B as being excluded from the IPM domain.

Suppose Host A is a receiver of the Movie Online program and Multicast Source sends data with the destination address of 224.0.1.1. In the beginning, Router A receives the data through Router B. When the rate of multicast data exceeds 10 kbps, Router A joins the shortest path tree and directly receives data through Router C.

4.6 PIM Troubleshooting

Fault 1: The router fails to establish the multicast routing table.

Troubleshooting: Follow the steps below:

Make sure that the unicast routes are correct before settling to the problem.

- PIM-SM requires support from the RP and the BSR. Use the **display pim bsr-info** command to check for BSR information. If none, check for the unicast routes towards the BSR. Then use the **display pim rp-info** command to check for RP information. If none, also check the unicast routes.
- Use the **display pim neighbor** command to check whether the neighbor relationship has been established correctly.

Chapter 5 MSDP Configuration

5.1 MSDP Overview

Multicast Source Discovery Protocol (MSDP) is used to discover multicast source information in other PIM-SM domains. A RP configured with MSDP peer notifies all of its MSDP peers of the active multicast source message in its domain via SA message. In this way, multicast source information in a PIM-SM domain is transmitted to another PIM-SM domain.

MSDP peer relationship can be established between RPs in different domains or in a same domain, between a RP and a common router, or between common routers. The connection between MSDP peers is TCP connection.

MSDP makes a PIM-SM domain independent of the RP in another PIM-SM domain. After getting multicast source information in that domain, the receiver here can join directly to the SPT of the multicast source in that domain.

Another application of MSDP is Anycast RP. In a domain, configure a certain interface (usually Loopback interface) on each router with a same IP address; designate these interfaces as candidate RPs; and create MSDP peer relationship among them. After the unicast route convergence, the multicast source can select the nearest RP for registration, and the receiver can also select the nearest RP to add into its RPT. The RPs exchange individual registration source information via MSDP peers. Therefore, every RP knows all multicast sources of the entire domain; and every receiver on each RP can receive multicast data from all the multicast sources in the entire domain.

By initiating registration and RPT joining to the nearest RP, MSDP implements RP load sharing. Once an RP turns invalid, its original registered source and receivers will select another nearest RP, implementing redundant RP backup.

In addition, MSDP excludes redundant SA messages through RPF check mechanism, and prevents the flooding of SA messages among MSDP peers by Mesh Group.

5.1.1 MSDP Working Principles

As shown in Figure 5-1, RPs in PIM-SM domain 1, domain 2 and domain 3 are in MSDP peer relationship, and there is a group member in domain 3. If a multicast source in domain 1 sends data to this group in domain 3, the whole process till the group member in domain 3 receives the multicast data covers:

1) The multicast source in PIM-SM domain 1 begins to send datagram.
2) The DR connected to the multicast source encapsulates the datagram into a Register packet and forward to the RP in domain 1.

3) The RP in domain 1 decapsulates the packet and forwards it along the RPT to all the members within the domain. The domain members can choose to take the path along SPT.
4) The RP in domain 1 generates an SA (Source Active) message for the MSDP peers (the RPs in PIM-SM domain 2 and domain 3). The SA message contains multicast source IP address, multicast group address, the RP address as well as the multicast this RP first receives.
5) If there is any group member in the domain of an MSDP peer (in the figure, it is PIM-SM domain 3), the RP in this domain sends the multicast data encapsulated in the SA message to group members along the RPT and the join message to multicast source.
6) After the reverse forwarding path is created, the multicast source data is sent directly to the RP in domain 3, which then RP forwards the data along the RPT. In this case, the last hop router connected with the group member in domain 3 can choose whether to switch to SPT.

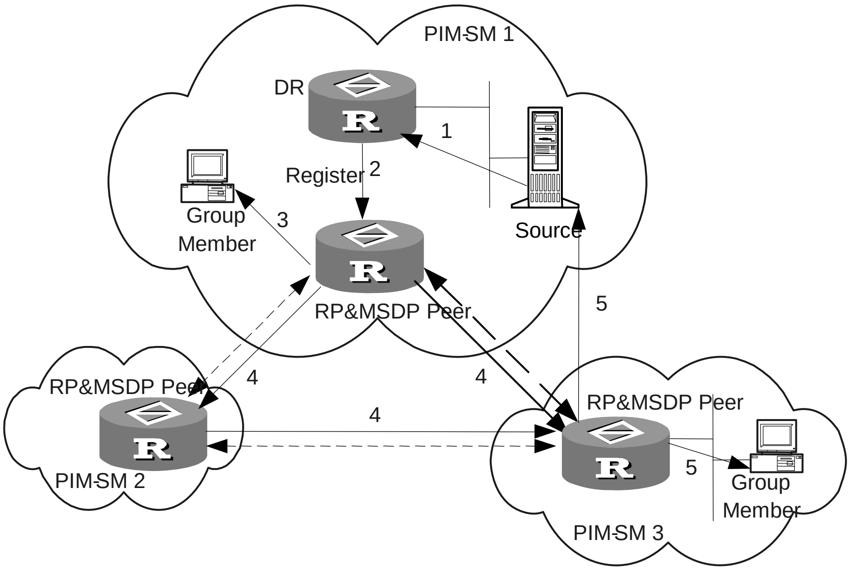


Figure 5-1 MSDP working principles I

As shown in Figure 5-2, RTA, RTB, RTC, RTD, RTE and RTF belong to domain 1, domain 2 and domain 3 respectively. MSDP peer relationship is established between them, indicated with bi-directional arrows in the figure. Among them, Mesh Group is created among RTB, RTC and RTD. The SA message forwarding and RPF check among these MSDP peers are illustrated as follows:

1) If the SA message is from an MSDP peer that is the RP of the multicast source as from RTA to RTB, it is received and forwarded to other peers.
2) If the SA message is from an MSDP peer that has only one peer as from RTB to RTA, it is received.

3) If the SA message is from a static RPF peer as from RTD to RTE, it is received and forwarded to other peers.
4) If the SA message is from an MSDP peer in Mesh Group as from RTB to RTD, it is received and forwarded to the peers outside the Mesh Group.
5) If the SA message is sent from an MSDP peer in a same domain, and the peer is the next hop along the optimal path to the RP in the domain of source, as in the case when the message is from RTE to ETF, it is received and forwarded to other peers.
6) If the SA message is sent from an MSDP peer in a different domain which is the next autonomous domain along the optimal path to the RP in the domain of source, as from RTD to RTF, it is received and forwarded to other peers
7) For other SA messages, they are neither received nor forwarded.

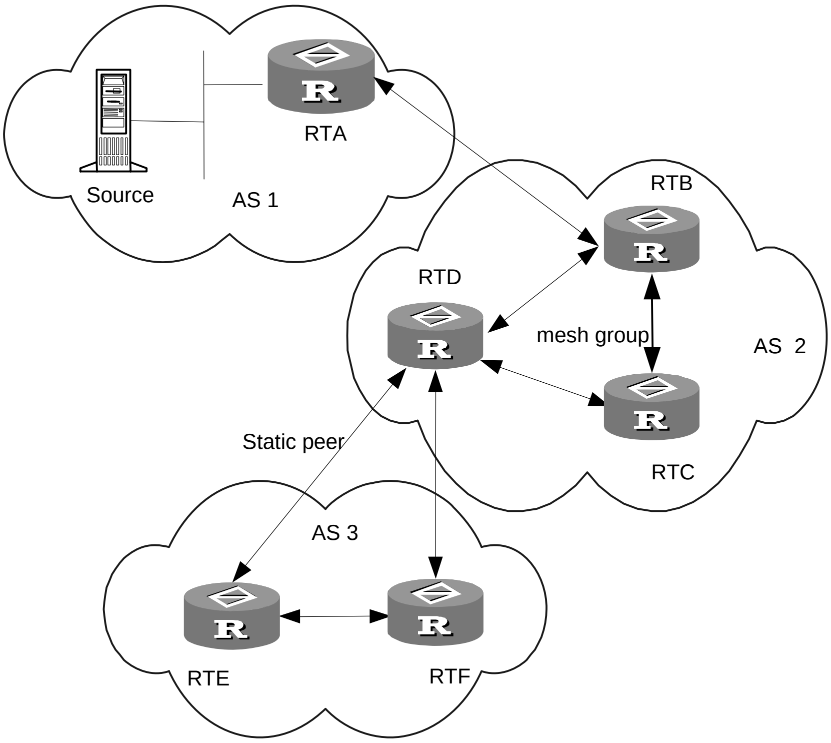


Figure 5-2 MSDP working principles II

Note:

The router operating with MSDP must also run BGP or MBGP. It is recommended to use the same IP address of the MSDP peer with that of the BGP peer or MBGP peer. If neither BGP nor MBGP is in operation, a static RPF peer should be configured.

5.2 MSDP Configuration

Basic configuration tasks of MSDP include:

- Enable MSDP
- Configure an MSDP peer

Advanced configuration tasks of MSDP include:

- Configure a static RPF peer
- Configure Originating RP
- Cache SA
- Configure the maximum number of SAs cached
- Request the source information from an MSDP peer
- Control the source information created
- Control the source information forwarded
- Control the source information received
- Configure an MSDP Mesh Group
- Configure MSDP connection retry interval
- Disable an MSDP Peer
- Clear MSDP connection, statistics and SA cache

5.2.1 Enabling MSDP

To configure MSDP, you must enable MSDP first.

Perform the following configuration in system view.

Table 5-1 Enable MSDP

Operation	Command
Enable MSDP and enter MSDP view	**msdp**
Clear all configurations of MSDP	**undo msdp**

5.2.2 Configuring an MSDP Peer

To run MSDP, you need to configure MSDP peers locally.

Perform the following configuration in MSDP view.

Table 5-2 Configure an MSDP peer

Operation	Command
Configure an MSDP peer	**peer** *peer-address* **connect-interface** *interface-type interface-number*
Remove the configuration of MSDP peer	**undo peer** *peer-address*
Add a description to an MSDP peer	**peer** *peer-address* **description** *text*

Operation	Command
Remove the description	**undo peer** *peer-address* **description** *text*

The command for description is optional.

If the local router is also in BGP Peer relation with an MSDP peer, the MSDP peer and the BGP peer should use the same IP address.

5.2.3 Configuring a Static RPF Peer

Perform the following configuration in MSDP view.

Table 5-3 Configure a static RPF peer

Operation	Command
Configure a static RPF peer	**static-rpf-peer** *peer-address* [**rp-policy** *list*]
Remove the configured static RPF peer	**undo static-rpf-peer** *peer-address*

By default, no static RPF peer is configured.

The **peer** command must be configured before the configuration of **static-rpf-peer** command.

If only one MSDP peer is configured via the **peer** command, the MSDP peer will be regarded as the static RPF peer.

To configure multiple static RPF peers at the same time, take any of the two methods:

- Using **rp-policy** parameters universally: Multiple static RPF peers take effect at the same time and SA messages are filtered by the RP addresses contained according to the configured prefix list. If multiple static RPF peers using the same **rp-policy** parameter are configured, any peer that receives an SA message will forward it to the other peers.
- Not using the **rp-policy** parameter universally: According to the configuration sequence, only the first static RPF peer whose connection state is UP is activated. All SA messages from the peer will be received and those from other static RPF peers will be discarded. Once the activated static RPF peer turns invalid (possibly out of configuration removed or connection interrupted), the following first static RPF peer with UP connection state according to the configuration sequence will assume its role.

5.2.4 Configuring Originating RP

During the creation of SA message, an MSDP peer can be configured to use the IP address of a specified interface as the RP address in its SA message.

Perform the following configuration in MSDP view.

Table 5-4 Configure Originating RP

Operation	Command
Configure an MSDP peer to use the IP address of a specified interface as the RP address of its SA message	**originating-rp** *interface-type interface-number*
Remove the above operation	**undo originating-rp**

By default, the RP address in SA message is the one configured by PIM.

5.2.5 Caching SA

When SA messages are cached on a router, the new join-in groups can directly access all the active sources and join the corresponding source tree, instead of waiting for the arrival of the next SA message.

Perform the following configuration in MSDP view.

Table 5-5 Cache SA

Operation	Command
Cache SA	**cache-sa-enable**
Disable SA caching	**undo cache-sa-enable**

By default, the router caches the SA state, or rather the (S, G) entry when receiving an SA message.

Some memory is consumed as the join delay of groups is shortened by this configuration.

5.2.6 Configuring the Maximum Number of SAs Cached

To prevent DoS (Deny of Service) attacks, you can set the maximum number of SAs cached on the router.

Perform the following configuration in MSDP view.

Table 5-6 Configure the maximum number of SAs cached

Operation	Command
Configure the maximum number of SAs cached	**peer** *peer-address* **sa-cache-maximum** *sa-limit*
Restore the default configuration	**undo peer** *peer-address* **sa-cache-maximum**

By default, the maximum number of SAs cached is 2048.

5.2.7 Requesting the Source Information from an MSDP Peer

When a new group joins, the router will send a SA request message to the specified MSDP peer, and the MSDP peer will respond with the SA messages it caches. If the MSDP peer does not enable the SA caching, the configuration is invalid.

Perform the following configuration in MSDP view.

Table 5-7 Request the source information from an MSDP peer

Operation	Command
Configure the router to send SA request message to the specified MSDP peer when receiving the join message of a group	**peer** *peer-address* **request-sa-enable**
Restore the default configuration	**undo peer** *peer-address* **request-sa-enable**

The SA request message sent by a local RP will get the immediate response about all active sources.

By default, the router does not send SA request message to its MSDP peer when receiving the join message of a group. Instead, it waits for the arrival of SA message of the next period.

5.2.8 Controlling the Source Information Created

I. Filtering the multicast routing entries imported

RP filters the registered sources to control the information of the active sources advertised in SA message. MSDP peers can be configured to only advertise the qualified (S, G) entries in the multicast routing table when creating SA messages, that is, to control the (S,G) entries imported from the multicast routing table to the domain.

Perform the following configuration in MSDP view.

Table 5-8 Filter the multicast routing entries imported

Operation	Command
Advertise only the (S, G) entries permitted by the ACL	**import-source** [**acl** *acl-number*]
Remove the above configuration	**undo import-source**

By default, only intra-domain sources are advertised in SA messages.

If the **import-source** command without **acl** parameter is executed, no source is advertised in SA messages.

II. Filtering SA request messages

Perform the following configuration in MSDP view.

Table 5-9 Filter SA request messages

Operation	Command
Filter all the SA request messages from a specified MSDP peer	**peer** *peer-address* **sa-request-policy**
Filter the SA request messages of the groups of a specified MSDP peer permitted by the basic ACL from	**peer** *peer-address* **sa-request-policy acl** *acl-number*
Remove the configuration of filtering SA request messages	**undo peer** *peer-address* **sa-request-policy**

By default, only the routers caching SA messages can respond to SA request messages; and routers receive all the SA request messages sent by their MSDP peers.

Multicast group addresses are described in ACL. If no ACL is specified, all SA request messages sent by the corresponding MSDP peer will be ignored. If ACL is specified, only SA request messages of the groups permitted by the ACL will be processed.

5.2.9 Controlling the Source Information Forwarded

Controlling of source information also includes that of forwarding and receiving source information besides that of creating source information. The outbound filter or time to live (TTL) threshold of SA messages can be used to control the SA message forwarding. By default, all SA messages are forwarded to other MSDP peers.

I. Using MSDP outbound filter

MSDP outbound filter of are functional in:

- Filtering off all the (S, G) entries
- Forwarding only the SA messages permitted by the advanced ACL

Perform the following configuration in MSDP view.

Table 5-10 Use MSDP outbound filter to control the source information forwarded

Operation	Command
Filter off all the SA messages to a specified MSDP peer	**peer** *peer-address* **sa-policy export**
Forward the SA messages permitted by the advanced ACL to a specified MSDP peer	**peer** *peer-address* **sa-policy export** [**acl** *acl-number*]
Cancel the filtering over the source information forwarded	**undo peer** *peer-address* **sa-policy export**

II. Using TTL to filter SA messages with encapsulated data

An SA message with encapsulated data can reach the specified MSDP peer only when the TTL in its IP header is no less than the threshold. Therefore, the forwarding of SA messages with encapsulated data can be controlled by configuring the TTL threshold.

For an SA message with encapsulated data whose TTL is less than or equal to 10, you can set the TTL threshold to 10 to prevent it from traveling outside the domain, or to any number larger than 10 to allow it to travel beyond the domain.

Perform the following configuration in MSDP view.

Table 5-11 Use TTL to filter SA messages with encapsulated data

Operation	Command
Filter off the multicast data encapsulated in the first SA message aiming at a specified MSDP peer	**peer** *peer-address* **minimum-ttl** *ttl*
Cancel the TTL threshold configuration	**undo peer** *peer-address* **minimum-ttl**

The default value of TTL threshold is 0.

5.2.10 Controlling the Source Information Received

Perform the following configuration in MSDP view.

Table 5-12 Control the source information received

Operation	Command
Filter the SA messages from a specified MSDP peer	**peer** *peer-address* **sa-policy import**
Receive the SA messages permitted by the advanced ACL from a specified MSDP peer	**peer** *peer-address* **sa-policy import** [**acl** *acl-number*]

Operation	Command
Cancel the filtering rule over received source information	**undo peer** *peer-address* **sa-policy import**

Similar to MSDP outbound filter in function, MSDP inbound filter controls the received SA messages.. By default, the SA messages from all peers are accepted.

5.2.11 Configuring an MSDP Mesh Group

Mesh Group is useful when full connection among MSDP peers is required but SA message flooding shall be prevented.

In a Mesh group, the SA messages from outside the group are forwarded to other members in the group, but the SA messages from peers inside the group will not be performed with Peer-RPF check or forwarded in the group. In this case, the overflow of SA messages is avoided and Peer-RPF is simplified, as BGP or MBGP is not required between MSDP peers.

Perform the following configuration in MSDP view.

Table 5-13 Configure an MSDP mesh group

Operation	Command
Configure an MSDP peer to be a member of an MSDP Mesh Group	**peer** *peer-address* **mesh-group** *name*
Delete that member from the Group	**undo peer** *peer-address* **mesh-group** *name*

If an MSDP peer is configured into different mesh groups, only the last configuration is valid.

5.2.12 Configuring MSDP Connection Retry Interval

Perform the following configuration in MSDP view.

Table 5-14 Configure the MSDP connection retry period

Operation	Command
Configure MSDP connection retry interval	**timer retry** *seconds*
Restore the default value of MSDP connection retry interval	**undo timer retry**

By default, MSDP connection is retried at the interval of 30 seconds.

5.2.13 Disabling an MSDP Peer

The session between MSDP peers can be cut off and re-activated as needed.

If a session between MSDP peers is cut off, the TCP connection will break with no retry effort, but the configuration information will be reserved.

Perform the following configuration in MSDP view.

Table 5-15 Disable an MSDP peer

Operation	Command
Disable a specified MSDP peer	**shutdown** *peer-address*
Remove the disabling configuration	**undo shutdown** *peer-address*

By default, MSDP peer is enabled.

5.2.14 Clearing MSDP Connection, Statistics and SA Cache

Perform the following configuration in user view.

Table 5-16 Clear MSDP connection, statistics and SA cache

Operation	Command
Clear a specified TCP connection and reset the counters of all MSDP information	**reset msdp peer** *peer-address*
Clear MSDP peer statistics	**reset msdp statistics** [*peer-address*]
Clear SA cache entries of MSDP	**reset msdp sa-cache** [*group-address*]

5.3 MSDP Display and Debug

5.3.1 Displaying and Debugging MSDP

Upon the above configuration, execute the **display** commands in any view to display the running information of MSDP and to verify the effect of the configuration.

Execute the **debugging** commands in user view for the debugging of MSDP.

Table 5-17 Display and debug MSDP

Operation	Command
Display the numbers of sources and groups of SA messages from a specified autonomous domain	**display msdp sa-count** [*as-number*]

Operation	Command
Display the details of an MSDP peer	**display msdp peer-status** [*peer-address*]
Display the (S,G) state learnt from MSDP peer	**display msdp sa-cache** [*group-address* | [*source-address*]] [*autonomous-system-number*]
Display MSDP peer state	**display msdp brief**
Enable MSDP debugging	**debugging msdp** { **all** | **connect** | **event** | **packet** | **source-active** }

📖 **Note:**

Only after the **cache-sa-enable** command is executed, will the **display msdp sa-count** command have output.

5.3.2 Tracing the Transmission Path of an SA Message over the Network

The **mtracert** command can be used in any view to trace the network path of multicast data from the multicast source to the destination receiver and to locate faults.

Table 5-18 Trace the transmission path of an SA message over the network

Operation	Command
Trace the transmission path of an SA message on the network	**msdp-tracert** { *source-address* } { *group-address* } { *rp-address* } [**max-hops** *max-hops*] [**next-hop-info**] [**sa-info**] [**peer-info**] [**skip-hops** *skip-hops*]

Information loss and configuration faults can be reduced by tracing the network path of the specified (S, G, RP) entries. Once the transmission path of SA messages is determined, correct configuration can prevent the overflow of SA messages.

5.4 Typical MSDP Configuration Examples

5.4.1 Configuring Static RPF Peers

I. Network requirements

In the following networking environment, four routers are all in the PIM-SM domains with no BGP or MBGP running among them.

To enable Router D to receive the specified source information from PIM-SM domains 1, 2 and 3, you can configure static RPF peers with the parameter **rp-policy**.

After the configuration finishes, Router RTD will only receive SA messages permitted by the corresponding filtering policy from its static RPF peers.

II. Network diagram

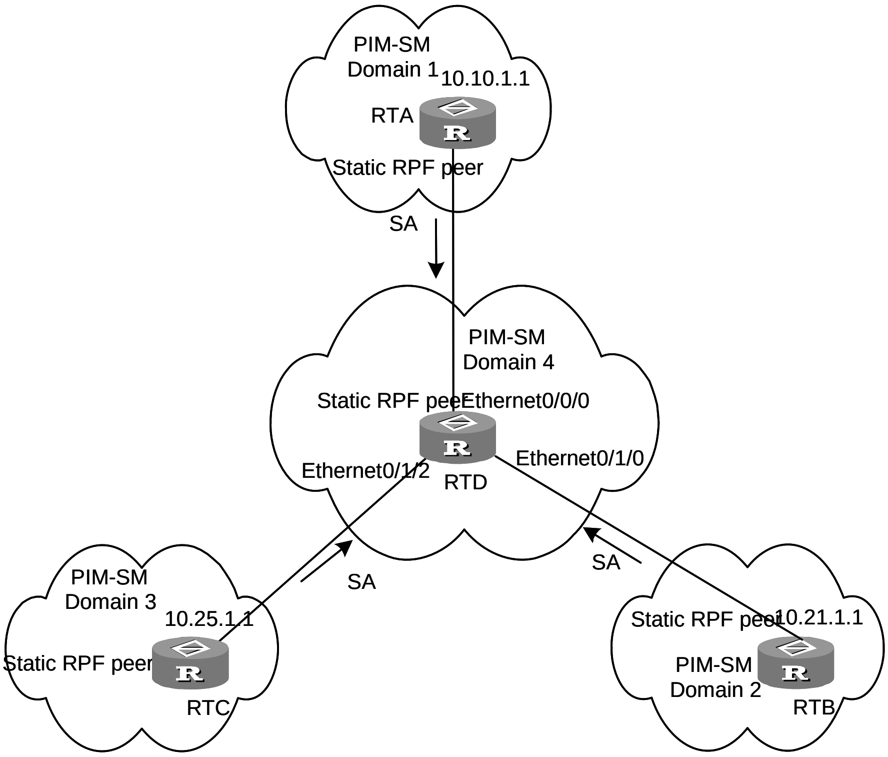


Figure 5-3 Configuring static RPF peers

III. Configuration procedure

# Configure RTA to be a static RPF peer of RTD.

```
<RTD> system-view
[RTD] ip ip-prefix list-a permit 10.10.0.0 16
[RTD] msdp
[RTD-msdp] peer 10.10.1.1 connect-interface ethernet 0/0/0
[RTD-msdp] static-rpf-peer 10.10.1.1 rp-policy list-a
```

# Configure RTB to be a static RPF peer of RTD.

```
[RTD] ip ip-prefix list-b permit 10.21.0.0 16
[RTD] msdp
[RTD-msdp] peer 10.21.1.1 connect-interface ethernet 0/1/0
[RTD-msdp] static-rpf-peer 10.21.1.1 rp-policy list-b
```

# Configure RTC to be a static RPF peer of RTD.

```
[RTD] ip ip-prefix list-c permit 10.25.0.0 16
[RTD] msdp
[RTD-msdp] peer 10.25.1.1 connect-interface ethernet 0/1/2
[RTD-msdp] static-rpf-peer 10.25.1.1 rp-policy list-c
```

5.4.2 Configuring Anycast RP

I. Network requirements

To configure Anycast RP in the PIM-SM domain, establish MSDP peer relationship between RTA and RTB; use the address of loopback0 on RTA and RTB to send SA messages outside; set Loopback10 interface on RTA and RTB as BSR/RP and configure the Anycast RP address. In this way, when a unicast group member joins, the router directly connected to the host can originate a join message to the nearest RP in the topology.

Note:

This example focuses on the configuration of RTA and RTB. Configuration performed on RTE, RTD and RTC is omitted as it mainly concerns enabling multicast and enabling PIM-SM on the interfaces.

II. Network diagram

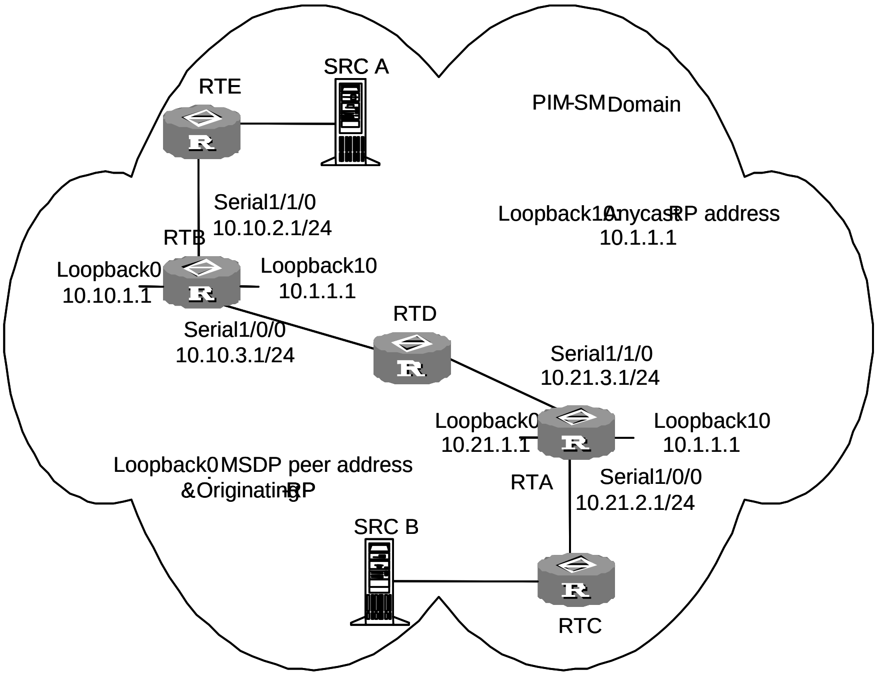


Figure 5-4 Configuring Anycast RP

III. Configuration procedure

1) Configure RTB:

# Enable multicast.

```
<RTB> system-view
[RTB] multicast routing-enable
```

# Configure the IP address of interface Loopback0.

```
[RTB] interface loopback0
[RTB-LoopBack0] ip address 10.10.1.1 255.255.255.255
[RTB-LoopBack0] quit
```

# Configure the IP address of interface Loopback10 and enable PIM-SM.

```
[RTB] interface loopback10
[RTB-LoopBack10] ip address 10.1.1.1 255.255.255.255
[RTB-LoopBack10] pim sm
[RTB-LoopBack10] quit
```

# Configure the IP address of interface Serial1/1/0 and enable PIM-SM.

```
[RTB] interface serial 1/1/0
[RTB-Serial1/1/0] ip address 10.10.2.1 255.255.255.0
[RTB-Serial1/1/0] pim sm
[RTB-Serial1/1/0] undo shutdown
[RTB-Serial1/1/0] quit
```

# Configure the IP address of interface Serial1/0/0 and enable PIM-SM.

```
[RTB] interface serial 1/0/0
[RTB-Serial1/0/0] ip address 10.10.3.1 255.255.255.0
[RTB-Serial1/0/0] pim sm
[RTB-Serial1/0/0] undo shutdown
[RTB-Serial1/0/0] quit
```

# Configure OSPF.

```
[RTB] ospf
[RTB-ospf-1] area 0
[RTB-ospf-1-area-0.0.0.0] network 10.10.2.0 0.255.255.255
[RTB-ospf-1-area-0.0.0.0] network 10.10.3.0 0.255.255.255
[RTB-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.0
[RTB-ospf-1-area-0.0.0.0] network 10.10.1.1 0.0.0.0
[RTB-ospf-1-area-0.0.0.0] quit
[RTB-ospf-1] quit
```

# Configure RTA as its MSDP peer.

```
[RTB] msdp
[RTB-msdp] peer 10.21.1.1 connect-interface loopback 0
```

# Configure Originating RP.

```
[RTB-msdp] originating-rp loopback0
[RTB-msdp] quit
```

# Configure the candidate RP and BSR.

```
[RTB] pim
[RTB-pim] c-rp loopback 10
[RTB-pim] c-bsr loopback 10 30
```

2) Configure RTA:

# Enable multicast.

```
[RTA] multicast routing-enable
```

# Configure the IP address of interface Loopback0.

```
[RTA] interface loopback0
[RTA-LoopBack0] ip address 10.21.1.1 255.255.255.255
[RTA-LoopBack0] quit
```

# Configure the IP address of interface Loopback10 and enable PIM-SM.

```
[RTA] interface loopback10
[RTA-LoopBack10] ip address 10.1.1.1 255.255.255.255
[RTA-LoopBack10] pim sm
[RTA-LoopBack10] quit
```

# Configure the IP address of interface Serial1/0/0 and enable PIM-SM.

```
[RTA] interface serial 1/0/0
[RTA-Serial1/0/0] ip address 10.21.2.1 255.255.255.0
[RTA-Serial1/0/0] pim sm
[RTA-Serial1/0/0] undo shutdown
[RTA-Serial1/0/0] quit
```

# Configure the IP address of interface Serial1/1/0 and enable PIM-SM.

```
[RTA] interface serial 1/1/0
[RTA-Serial1/1/0] ip address 10.21.3.1 255.255.255.0
[RTA-Serial1/1/0] pim sm
[RTA-Serial1/1/0] undo shutdown
[RTA-Serial1/1/0] quit
```

# Configure OSPF route.

```
[RTA] ospf
[RTA-ospf-1] area 0
[RTA-ospf-1-area-0.0.0.0] network 10.21.2.0 0.255.255.255
[RTA-ospf-1-area-0.0.0.0] network 10.21.3.0 0.255.255.255
[RTA-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.0
[RTA-ospf-1-area-0.0.0.0] network 10.21.1.1 0.0.0.0
[RTA-ospf-1-area-0.0.0.0] quit
```

```
[RTA-ospf-1] quit
```

# Configure RTB as its MSDP peer.

```
[RTA] msdp
[RTA-msdp] peer 10.10.1.1 connect-interface loopback 0
```

# Configure Originating RP.

```
[RTA-msdp] originating-rp loopback0
[RTA-msdp] quit
```

# Configure the candidate RP and BSR.

```
[RTA] pim
[RTA-pim] c-rp loopback 10
[RTA-pim] c-bsr loopback 10 30
```

5.4.3 MSDP Integrated Networking

I. Network requirements

In the following network, Multicast Source is located in PIM-SM domain 1, and the receivers of its Movie Online program are distributed in PIM-SM domains 2, 3, and 4.

Enable MSDP and configure an Anycast RP in PIM-SM domain 1; establish MSDP peer relationship among RPs across PIM-SM domains; and use MBGP between domains (For commands of this part, refer to the next chapter).

Note:

To present the configurations of MSDP and IGMP clearly, suppose no receivers exist in PIM-SM domain 1, and the receives added to a multicast group in domains 2 through 4 are connected to the Ethernet interfaces on the routers.

For configuration of RTF, refer to the configurations of RTA and RTE.

The configurations of RTC and RTD are simpler; you need only to enable multicast routing on them.

For configurations of RTH and RTI, refer to the configurations of RTG.

II. Network diagram

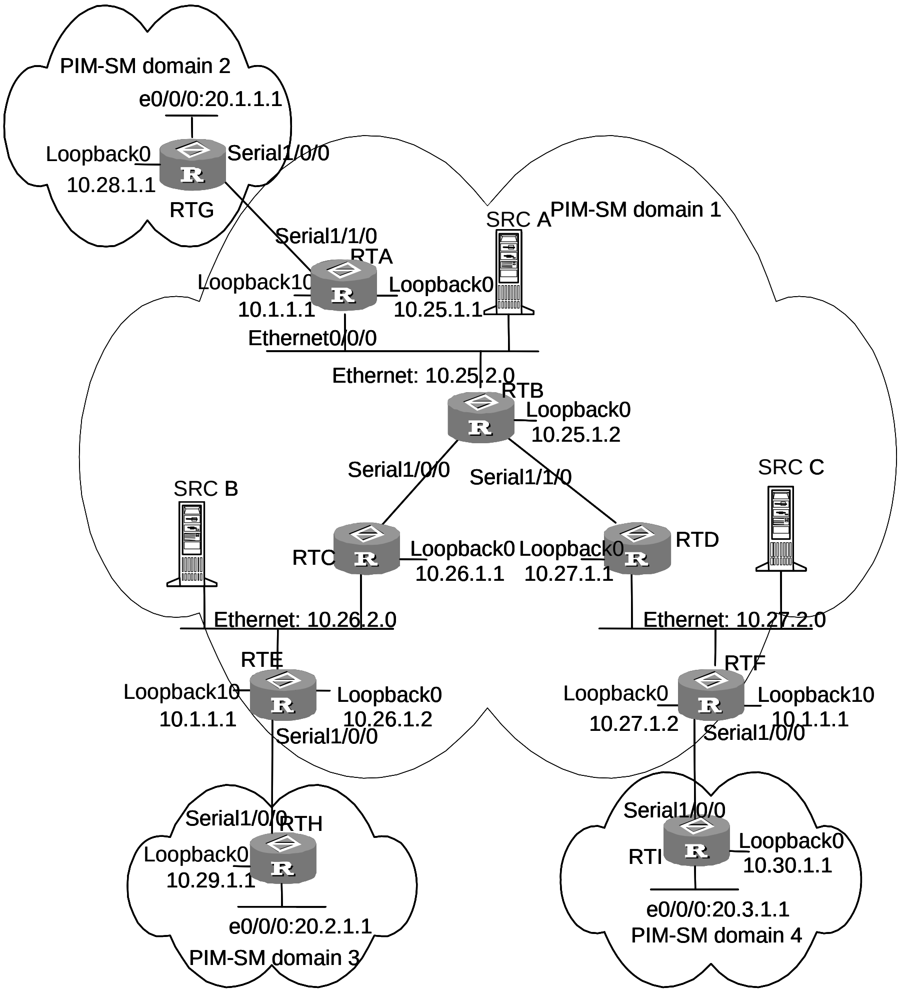


Figure 5-5 Network diagram for MSDP

III. Configuration Procedure

1) Configure RTA:

# Enable multicast.

```
<RTA> system-view
[RTA] multicast routing-enable
```

# Configure the IP address of interface loopback0 and enable PIM-SM.

```
[RTA] interface loopback0
[RTA-LoopBack0] ip address 10.25.1.1 255.255.255.255
[RTA-LoopBack0] pim sm
[RTA-LoopBack0] quit
```

# Configure the IP address of interface loopback10 and enable PIM-SM.

```
[RTA] interface loopback10
[RTA-LoopBack10] ip address 10.1.1.1 255.255.255.255
[RTA-LoopBack10] pim sm
[RTA-LoopBack10] quit
```

# Configure the IP address of interface Ethernet0/0/0 and enable PIM-SM.

```
[RTA] interface ethernet 0/0/0
[RTA-Ethernet0/0/0] ip address 10.25.2.3 255.255.255.0
[RTA-Ethernet0/0/0] pim sm
[RTA-Ethernet0/0/0] undo shutdown
[RTA-Ethernet0/0/0] quit
```

# Configure the IP address of interface Serial1/1/0 and enable PIM-SM.

```
[RTA] interface serial 1/1/0
[RTA-Serial1/1/0] ip address 10.25.3.1 255.255.255.0
[RTA-Serial1/1/0] pim sm
[RTA-Serial1/1/0] undo shutdown
[RTA-Serial1/1/0] quit
```

# Configure OSPF.

```
[RTA] ospf
[RTA-ospf-1] area 0
[RTA-ospf-1-area-0.0.0.0] network 10.25.2.0 0.0.0.255
[RTA-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.0
[RTA-ospf-1-area-0.0.0.0] network 10.25.1.1 0.0.0.0
[RTA-ospf-1-area-0.0.0.0] quit
[RTA-ospf-1] quit
```

# Configure the IBGP peer RTE.

```
[RTA] bgp 100
[RTA-bgp] undo synchronization
[RTA-bgp] group rte internal
[RTA-bgp] peer 10.26.1.2 group rte
[RTA-bgp] peer rte connect-interface loopback0
[RTA-bgp] peer rte next-hop-local
[RTA-bgp] ipv4-family multicast
[RTA-bgp-af-mul] peer rte enable
[RTA-bgp-af-mul] peer 10.26.1.2 group rte
[RTA-bgp-af-mul] peer rte next-hop-local
[RTA-bgp-af-mul] quit
```

# Configure the IBGP peer RTF.

```
[RTA-bgp] group rtf internal
[RTA-bgp] peer 10.27.1.2 group rtf
[RTA-bgp] peer rtf connect-interface loopback0
```

```
[RTA-bgp] peer rtf next-hop-local
[RTA-bgp] ipv4-family multicast
[RTA-bgp-af-mul] peer rtf enable
[RTA-bgp-af-mul] peer rtf next-hop-local
[RTA-bgp-af-mul] quit
```

# Configure the EBGP peer RTG.

```
[RTA-bgp] group rtg external
[RTA-bgp] peer 10.28.1.1 group rtg as-number 200
[RTA-bgp] peer rtg next-hop-local
[RTA-bgp] peer rtg default-route-advertise
[RTA-bgp] peer rtg ebgp-max-hop 255
[RTA-bgp] ipv4-family multicast
[RTA-bgp-af-mul] peer 10.28.1.1 group rtg
[RTA-bgp-af-mul] peer rtg enable
[RTA-bgp-af-mul] peer rtg next-hop-local
[RTA-bgp-af-mul] quit
[RTA-bgp] quit
```

# Configure MSDP peer, Mess Group and Originating RP.

```
[RTA] msdp
[RTA-msdp] static-rpf-peer 10.28.1.1
[RTA-msdp] peer 10.28.1.1 connect-interface loopback 0
[RTA-msdp] peer 10.26.1.2 connect-interface loopback 0
[RTA-msdp] peer 10.27.1.2 connect-interface loopback 0
[RTA-msdp] peer 10.26.1.2 mesh-group net
[RTA-msdp] peer 10.27.1.2 mesh-group net
[RTA-msdp] originating-rp loopback0
[RTA-msdp] quit
```

# Configure the candidate RP and BSR.

```
[RTA] pim
[RTA-pim] c-rp loopback 10
[RTA-pim] c-bsr loopback 0 30
```

2) Configure RTE:

# Enable multicast.

```
[RTE] multicast routing-enable
```

# Configure the IP address of interface Loopback0 and enable PIM-SM.

```
[RTE] interface loopback0
[RTE-LoopBack0] ip address 10.26.1.2 255.255.255.255
[RTE-LoopBack0] pim sm
[RTE-LoopBack0] quit
```

# Configure the IP address of interface loopback10 and enable PIM-SM.

```
[RTE] interface loopback10
[RTE-LoopBack10] ip address 10.1.1.1 255.255.255.255
[RTE-LoopBack10] pim sm
[RTE-LoopBack10] quit
```

# Configure the IP address of interface Ethernet 0/0/0 and enable PIM-SM.

```
[RTE] interface ethernet 0/0/0
[RTE-Ethernet0/0/0] ip address 10.26.2.3 255.255.255.0
[RTE-Ethernet0/0/0] pim sm
[RTE-Ethernet0/0/0] undo shutdown
[RTE-Ethernet0/0/0] quit
```

# Configure the IP address of interface Serial 1/0/0 and enable PIM-SM.

```
[RTE] interface serial 1/0/0
[RTE-Serial1/0/0] ip address 10.26.3.1 255.255.255.0
[RTE-Serial1/0/0] pim sm
[RTE-Serial1/0/0] undo shutdown
[RTE-Serial1/0/0] quit
```

# Configure OSPF.

```
[RTE] ospf
[RTE-ospf-1] area 0
[RTE-ospf-1-area-0.0.0.0] network 10.26.2.0 0.255.255.255
[RTE-ospf-1-area-0.0.0.0] network 10.1.1.1 0.0.0.0
[RTE-ospf-1-area-0.0.0.0] network 10.26.1.2 0.0.0.0
[RTE-ospf-1-area-0.0.0.0] quit
[RTE-ospf-1] quit
```

# Configure the IBGP peer RTA.

```
[RTE] bgp 100
[RTE-bgp] undo synchronization
[RTE-bgp] group rta internal
[RTE-bgp] peer 10.25.1.1 group rta
[RTE-bgp] peer rta connect-interface loopback0
[RTE-bgp] peer rta next-hop-local
[RTE-bgp] ipv4-family multicast
[RTE-bgp-af-mul] peer 10.25.1.1 group rta
[RTE-bgp-af-mul] peer rta enable
[RTE-bgp-af-mul] peer rta next-hop-local
[RTE-bgp-af-mul] quit
```

# Configure the IBGP peer RTF.

```
[RTE-bgp] group rtf internal
[RTE-bgp] peer 10.26.1.2 group rtf
[RTE-bgp] peer rtf connect-interface loopback0
```

```
[RTE-bgp] peer rtf next-hop-local
[RTE-bgp] ipv4-family multicast
[RTE-bgp-af-mul] peer 10.26.1.2 group rtf
[RTE-bgp-af-mul] peer rtf enable
[RTE-bgp-af-mul] peer rtf next-hop-local
[RTE-bgp-af-mul] quit
[RTE-bgp] quit
```

# Configure MSDP peer, Mess Group and Originating RP.

```
[RTE] msdp
[RTE-msdp] peer 10.29.1.1 connect-interface loopback 0
[RTE-msdp] static-rpf-peer 10.29.1.1
[RTE-msdp] peer 10.25.1.1 connect-interface loopback 0
[RTE-msdp] peer 10.27.1.2 connect- interface loopback 0
[RTE-msdp] peer 10.25.1.1 mesh-group net
[RTE-msdp] peer 10.27.1.2 mesh-group net
[RTE-msdp] originating-rp loopback0
[RTE-msdp] quit
[RTE] ip route-static 10.29.1.1 255.255.255.0 serial1/0/0
```

# Configure the candidate RP and BSR.

```
[RTE] pim
[RTE-pim] c-rp loopback 10
[RTE-pim] c-bsr loopback 0 30
```

3) Configure RTB:

# Enable multicast.

```
[RTB] multicast routing-enable
```

# Configure the IP address of interface Ethernet 0/0/0 and enable PIM-SM.

```
[RTB] interface ethernet 0/0/0
[RTB-Ethernet0/0/0] ip address 10.25.2.4 255.255.255.0
[RTB-Ethernet0/0/0] pim sm
[RTB-Ethernet0/0/0] undo shutdown
```

4) Configure RTG

# Enable multicast.

```
<RTG> system-view
[RTG] multicast routing-enable
```

# Assign an IP address to interface loopback0 and enable PIM-SM on it.

```
[RTG] interface loopback0
[RTG-LoopBack0] ip address 10.28.1.1 255.255.255.255
[RTG-LoopBack0] pim sm
[RTG-LoopBack0] quit
```

# Assign an IP address to interface serial 1/0/0 and enable PIM-SM on it.

```
[RTA] interface serial 1/0/0
[RTA-Serial1/0/0] ip address 10.25.3.2 255.255.255.0
[RTA-Serial1/0/0] pim sm
[RTA-Serial1/0/0] quit
```

# Assign an IP address to interface ethernet0/0/0 and enable PIM-SM and IGMP on it.

```
[RTG] interface ethernet0/0/0
[RTG-ethernet0/0/0] ip address 20.1.1.1 255.255.255.255
[RTG-ethernet0/0/0] pim sm
[RTG-ethernet0/0/0] igmp enable
[RTG-ethernet0/0/0] quit
```

# Configure an MSDP peer and Originating RP.

```
[RTA] msdp
[RTA-msdp] static-rpf-peer 10.28.1.1
[RTA-msdp] peer 10.25.1.1 connect-interface loopback 0
[RTA-msdp] originating-rp loopback0
[RTA-msdp] quit
```

# Configure RP and BSR candidates.

```
[RTA] pim
[RTA-pim] c-rp loopback 0
[RTA-pim] c-bsr loopback 0 30
```

5) Configure Multicast Source

On Multicast Source associate multicast programs with multicast addresses, for example, Movie Online with 224.0.1.1.

6) Configure the Receivers

Connect the Receivers to Multicast Source using HTTP, and select the Movie Online program on the client software.

Chapter 6 MBGP Multicast Extension Configuration

6.1 MBGP Multicast Extension

6.1.1 MBGP Multicast Extension Overview

At present, the most widely used inter-domain unicast routing protocol is BGP-4. Because the multicast topology may be different from the unicast topology, BGP-4 must be modified in order to implement the transmission of inter-domain multicast routing information. Some routers in the network may only support unicast rather than multicast and may not forward multicast packets since the particular policy requires that. To construct inter-domain multicast trees, the knowledge of multicast-supporting parts of the network (or the multicast network topology) is also necessary, other than that of the unicast routing information.

BGP-4 has been proved to be an effective and stable inter-domain unicast routing protocol. Therefore, it is more rational to enhance and extend the BGP-4 protocol than to construct a new protocol. RFC2858 specifies the methods of multi-protocol BGP extension. The extended BGP (Multi-protocol BGP, MBGP or BGP-4+) carries not only the IPv4 unicast routing information but also routing information of other network layer protocols (such as multicast and IPv6 etc). Carrying the multicast routing information is only one of the extension functions. This chapter describes mainly MBGP extension for multicast.

MBGP enables unicast and multicast routing information to be exchanged through the same process but stored in different routing tables. As MBGP is an enhanced version of BGP-4, all the common policies and configuration methods that BGP-4 supports can be applied to multicast.

6.1.2 MBGP Extension Attributes for Multicast

To enable MBGP to support multicast, RFC2858 defines two new path attributes MP_REACH_NLRI (Multiprotocol Reachable NLRI) and MP_UNREACH_NLRI (Multiprotocol Unreachable NLRI) in UPDATE packets. They are all optional non-transitive attributes, that is, routers that do not support MBGP can ignore the information in the attributes and not forward the attributes.

Among the information carried by MP_REACH_NLRI and MP_UNREACH_NLRI, AFI (Address Family Identifier) and SAFI (Subsequent Address Family Identifier) can identify for which address family the information is. SAFI is a complement to NLRI

(Network Layer Reachability Information), with 1 for the unicast mode of NLRI, and 2 for the multicast mode of NLRI.

I. MP_REACH_NLRI attribute

MP_REACH_NLRI is an optional non-transitive attribute, and can be used to:

- Send the routing information to a new protocol.
- Send the next hop information about the new protocol with the same coding mode as that of NLRI.
- Enable the router to report part or all of the SNPAs (Sub-network Points of Attachment) saved in the local system.

II. MP_UNREACH_NLRI attribute

The MP_UNREACH_NLRI is an optional non-transitive attribute that can be used for the purpose of withdrawing one or multiple unfeasible routes from service. It includes the following fields:

- AFI and SAFI.
- Withdrawn Routes: Contains one or multiple NLRIs, in which are the unreachable destination addresses.

An UPDATE packet that contains the MP_UNREACH_NLRI is not required to carry any other path attributes.

These two attributes enables MBGP to carry multi-protocol information. MSGP therefore supports both unicast and multicast by constructing different topology maps to implement appropriate policies. Besides, MBGP may construct different inter-domain routes for unicast and multicast under a same policy.

6.1.3 MBGP Operating Mode and Message Type

MBGP runs on a router in the following two modes:

- IBGP (Internal BGP)
- EBGP (External BGP)

MBGP running in an autonomous system is called IBGP; MBGP running across autonomous systems is called EBGP.

MBGP offers four types of messages:

- Open Message
- Update Message
- Notification Message
- Keepalive Message

Open Message is the first message sent after the TCP connection is established. It is used to establish BGP peer relationship. Notification Message is used to notify errors. Keepalive message is used to check the validity of a connection. Update Message is the most important information in the MBGP system, used to exchange routing information among peers. It consists of three parts at the most: MP_UNREACH_NLRI, Path Attributes and MP_REACH_NLRI.

6.2 MBGP Multicast Extension Configuration

Basic configuration tasks of MBGP multicast extension include:

- Enable MBGP Multicast Extension Protocol
- Specify the network route to be advertised by MBGP multicast extension

Advanced configuration tasks of MBGP multicast extension include:

- Configure the MED value for an AS
- Compare MED values from different AS neighbor paths
- Configure local preference
- Configure MBGP timer
- Configure MBGP Peer/Peer Group
- Configure MBGP Route Aggregation
- Configure an MBGP route reflector
- Configure the MBGP community attributes
- Configure the interaction between MBGP and IGP
- Define AS path list and routing policy
- Configure MBGP route filtering
- Reset BGP connections

🕮 **Note:**

Only configuration tasks in IPv4 multicast sub-address family view are detailed below. Other tasks configured in BGP or system view are only briefed. For the detailed configuration, refer to the “BGP Configuration” and “IP Routing policy" sections in “Routing Protocol” of this manual.

6.2.1 Enabling MBGP Multicast Extension Protocol

To enable the MBGP multicast extension protocol, enter the IPv4 multicast sub-address family view.

A router does not start receiving MBFP connection requests instantly after the MBGP multicast extension protocol is enabled. To have a router originate MBGP connection requests to neighboring routers, check the MBGP peer configurations. Once the MBGP multicast address family is removed, all established MBGP connections will be released.

Perform the following configuration in BGP view.

Table 6-1 Enable the MBGP Multicast Extension Protocol

Operation	Command
Enter the MBGP multicast address family view	**ipv4-family multicast**
Remove the MBGP multicast address family view	**undo ipv4-family multicast**

By default, the system does not run the MBGP multicast extension protocol.

6.2.2 Specifying Network Route to be Advertised by MBGP Multicast Extension

The **network** command is used to specify the network routes to be advertised to MBGP peers, as well as the mask and routing policy of this network route.

Perform the following configuration in IPv4 multicast sub-address family view.

Table 6-2 Specify the network routes to be advertised by MBGP multicast extension

Operation	Command
Configure the network routes to be advertised by the local MBGP	**network** *ip-address* [*address-mask*] [**route-policy** *policy-name*]
Remove the network routes to be advertised by the local MBGP	**undo network** *ip-address* [*address-mask*] [**route-policy** *policy-name*]

By default, no route is advertised by the local MBGP.

The **network** command advertises only the precisely matched route, the one with prefix and mask completely conforming to the configuration. If no mask is specified, match goes by the natural network segment.

6.2.3 Configuring the MED Value for an AS

The MED configured in BGP view is valid for both unicast and multicast.

For this configuration, refer to the “BGP Configuration” section in the “Routing Policy” of this manual.

6.2.4 Comparing MED Values from Different AS Neighbor Paths

Do not use this configuration unless you are sure that different ASs adopt the same IGP and route selection method. The configuration in BGP view works both in unicast and multicast.

For the configuration, refer to the “BGP Configuration” section in “Routing Protocol” of this manual.

6.2.5 Configuring Local Preference

Different local preference can be configured as a reference of the MBGP route selection. When an MBGP router has multiple routes to a same destination through different next hop neighbors, it will choose the route with the highest local preference.

The configuration works both in unicast and multicast.

For this configuration, refer to the “BGP Configuration” section in “Routing Protocol” of this manual.

6.2.6 Configuring MBGP Timer

After a router establishes MBGP connection with a peer, it sends Keepalive messages to the peer periodically to check for the smooth connection. If the router does not receive a single Keepalive message or any other kind of message from the peer within the defined connection Holdtime, it will think the MBGP connection broken and exit, and will process the routing information received through this connection as appropriate. Therefore, the Keepalive message sending interval and MBGP connection Holdtime are two parameters of great importance in MBGP mechanism.

The configuration works both in unicast and multicast.

For this configuration, refer to the “BGP Configuration” section in “Routing Protocol” of this manual.

6.2.7 Configuring MBGP Peer/Peer Group

The use of MBGP peer groups is to simplify configuration. When multiple peers with same configuration are necessary, you can create and configure a peer group, and then add the peers into the group, since all peers in a group have the same configuration with the group..

⚠ **Caution:**

Configure the peer group under the guide of technical support engineers.

Perform the configurations in the following subsections in IPv4 multicast sub-address family view.

I. Creating a peer group with members

By default, an IBGP peer will be added to a default peer group without configuration. Such default group is invisible. The configuration of the route updating policy on any IBGP peer is valid for the other group members only. If the router is not a route reflector, all the IBGP peers stay belong to a same group. Otherwise, all the route reflection clients belong to one group, and others to another.

EBGP peer group members must be in a same network segment. Otherwise, the route updating packets sent from a router might be discarded by some EBGP peers.

IBGP peer and EBGP peer cannot be added into one group.

Table 6-3 Create a peer group and adding members

Operation	Command
Create a peer group	**group** *group-name*
Delete the specified peer group	**undo group** *group-name*
Add a peer into the peer group	**peer** *peer-address* **group** *group-name*
Delete a peer from the peer group	**undo peer** *peer-address* **group** *group-name*
Reset the connection among all members in the peer group (in user view)	**reset bgp group** *group-name*

II. Enabling a peer/peer group

Table 6-4 Enable a peer/peer group

Operation	Command
Enable the specified peer/peer group	**peer** *group-name* **enable**
Disable the specified peer/peer group	**undo peer** *group-name* **enable**

III. Advertising MBGP community attributes to a peer/peer group

Table 6-5 Configure to advertise the community attributes to a peer/peer group

Operation	Command
Advertise the community attributes to a peer/peer group	**peer** *group-name* **advertise-community**
Configure not to advertise the community attributes to a peer/peer group	**undo peer** *group-name* **advertise-community**

By default, no community attribute is advertised to any peer/peer group.

IV. Configuring a peer/peer group as an MBGP route reflector client

Table 6-6 Configure a peer/peer group as an MBGP route reflector client

Operation	Command
Configure a peer/peer group as an MBGP route reflector client	**peer** *group-name* **reflect-client**
Remove the above configuration	**undo peer** *group-name* **reflect-client**

By default, there is no route reflector in an autonomous system.

It is generally unnecessary to configure this command for a peer group. This command is reserved for the occasional compatibility with the network equipments of other vendors.

V. Configuring the local address as the next hop when advertising routes

This involves removing the next hop configuration in the routing information advertised to a peer/peer group and configuring the local address as the next hop address. It is valid only for IBGP peers/peer groups.

Table 6-7 Configure the local address as the next hop when advertising routes

Operation	Command
Configure the local address as the next hop when advertising routing information	**peer** *group-name* **next-hop-local**
Cancel the above configuration	**undo peer** *group-name* **next-hop-local**

VI. Transmitting only public AS numbers with BGP updates

Table 6-8 Transmit only public AS numbers with BGP updates

Operation	Command
Transmit only public AS numbers with BGP updates.	**peer** *group-name* **public-as-only**
Transmit private AS numbers with BGP updates.	**undo peer** *group-name* **public-as-only**

By default, a private AS number is sent with BGP updates.

VII. Configuring the maximum times that the local AS number can be received

You may restrict the times that the local AS number is allowed to be present in the received routing updates.

Perform the following configuration in IPv4 multicast subaddress family view.

Table 6-9 Configure the times that the local AS number can be received

Operation	Command
Configure the times that the local AS number can be received.	**peer** { *group-name* | *peer-address* } **allow-as-loop** [*number*]
Cancel the above configuration.	**undo peer** { *group-name* | *peer-address* } **allow-as-loop**

The *number* argument defaults to 3.

6.2.8 Configuring MBGP to Filter Routes

Perform the following configuration in IPv4 multicast subaddress family view.

I. Specifying the routing policy for a peer/peer group

The routing update policy that the members in a peer group use must be the same as that of the peer group in the outgoing direction but not necessarily in the incoming direction. In other words, all peer group members must follow the same policy when advertising routes but not when redistributing routes.

Table 6-10 Specify the routing policy for a peer/peer group

Operation	Command
Configure MBGP to apply the specified routing policy to the routes received from the specified peer or peer group.	**peer** { *group-name* | *peer-address* } **route-policy** *policy-name* **import**
Cancel application of the routing policy in the incoming direction.	**undo peer** { *group-name* | *peer-address* } **route-policy** *policy-name* **import**
Configure MBGP to apply the specified routing policy to the routes advertised to the specified peer or peer group.	**peer** *group-name* **route-policy** *policy-name* **export**
Cancel application of the routing policy in the incoming direction.	**undo peer** *group-name* **route-policy** *policy-name* **export**

By default, no routing policy is applied to the received or advertised routes.

II. Configuring IP-ACL-based route filtering policy for a peer/peer group

Table 6-11 Configure the IP-ACL-based route filtering policy for a peer/peer group

Operation	Command
Configure MBGP to filter the routes received from the specified peer or peer group based on the specified ACL.	**peer** { *group-name* | *peer-address* } **filter-policy** *acl-number* **import**
Disable MBGP to filter the received routes.	**undo peer** { *group-name* | *peer-address* } **filter-policy** *acl-number* **import**
Configure MBGP to filter the routes advertised to the specified peer or peer group based on the specified ACL.	**peer** *group-name* **filter-policy** *acl-number* **export**
Disable MBGP to filter the advertised routes.	**undo peer** *group-name* **filter-policy** *acl-number* **export**

By default, MBGP does no filter the received or advertised routes.

III. Configuring AS-path-list-based route filtering policy for a peer/peer group

Table 6-12 Configure the AS-path-list-based route filtering policy for a peer/peer group

Operation	Command
Configure MBGP to filter the routes received from the specified peer or peer group based on the specified AS path list.	**peer** { *group-name* | *peer-address* } **as-path-acl** *number* **import**
Disable MBGP to filter the received routes.	**undo peer** { *group-name* | *peer-address* } **as-path-acl** *number* **import**
Configure MBGP to filter the routes advertised to the specified peer or peer group.	**peer** *group-name* **as-path-acl** *number* **export**
Disable MBGP to filter the routes advertise to the specified peer or peer group.	**undo peer** *group-name* **as-path-acl** *number* **export**

By default, MBGP does not filter the received or advertised routes.

IV. Configuring prefix-list-based route filtering policy for a peer/peer group

Table 6-13 Configure the prefix-list-based route filtering policy for a peer/peer group

Operation	Command
Configure MBGP to filter the routes received from the specified peer or peer group based on the specified ACL.	**peer** { *group-name* | *peer-address* } **ip-prefix** *prefixname* **import**

Operation	Command
Disable MBGP to filter the received routes.	**undo peer** { *group-name* | *peer-address* } **ip-prefix** *prefixname* **import**
Configure MBGP to filter the routes advertised to the specified peer or peer group based on the specified ACL.	**peer** *group-name* **filter-policy** *acl-number* **export**
Disable MBGP to filter the advertised routes.	**undo peer** *group-name* **filter-policy** *acl-number* **export**

By default, MBGP does no filter the received or advertised routes.

6.2.9 Configuring MBGP Route Aggregation

MBGP supports the manual aggregation of routes. Manual aggregation aggregates the local MBGP routes. A series of parameters can be configured during manual route aggregation.

Perform the following configuration in IPv4 multicast sub-address family view.

Table 6-14 Configure MBGP Route Aggregation

Operation	Command
Configure the aggregation of local routes	**aggregate** *address mask* [**as-set**] [**detail-suppressed**] [**suppress-policy** *route-policy-name*] [**origin-policy** *route-policy-name*] [**attribute-policy** *route-policy-name*]
Remove the aggregation of local routes	**undo aggregate** *address mask* [**as-set**] [**detail-suppressed**] [**suppress-policy** *route-policy-name*] [**origin-policy** *route-policy-name*] [**attribute-policy** *route-policy-name*]

By default, MBGP does not aggregate local routes.

6.2.10 Configuring MBGP Route Reflector

To ensure the interconnectivity among MBGP peers, it is necessary to establish fully-closed network among IBGP multicast peers. However, some internal MBGP multicast networks are very large, and it costs a good sum to establish a fully-closed network. Route reflector solves this problem. The core is to specify a router as the focus of the internal sessions. Multiple MBGP multicast routers can be peers of one central point, namely a multiple route reflector, which in turn creates peer relationship with other reflectors. The routers other than those reflectors are called clients. The clients exchange path selection information with a reflector in peer relationship; the reflector transmits (reflects) information to the clients in turn.

For the details of principles and configuration, refer to the “BGP Configuration” section in “Routing Protocol” of this manual.

6.2.11 Configuring MBGP Community Attributes

As for MBGP, a community is a group of destinations with common properties, with no physical boundary, like that of a network or an autonomous system.

For the detailed configuration, refer to the “BGP Configuration“ section in “Routing Protocol” of this manual.

6.2.12 Importing IGP Routing Information into MBGP

MBGP can send the local network information acquired through IGP to other autonomous systems.

Perform the following configuration in IPv4 multicast sub-address family view.

Table 6-15 Import IGP routing information

Operation	Command
Import IGP routing information into MBGP	**import-route** *protocol* [**route-policy** *policy-name*] [**med** *metric*]
Delete the imported IGP routing information	**undo import-route** *protocol*

By default, MBGP does not import any route of other protocols.

Parameter *Protocol* specifies the source routing protocols of import, which can be direct, static, rip, isis, ospf, ospf-ase or ospf-nssa at present.

6.2.13 Defining AS Path List and Routing Policy

To configure AS path list and routing polity is to:

- Configure the regular expression of autonomous systems (in system view);

The UPDATE information of MBGP contains an AS_PATH domain. The autonomous system paths for MBGP routing information exchange is recorded in this domain.

- Define the routing policy (in system view);
- Define matching rules (in routing policy view); and
- Define value assigning rules (in routing policy view)

For the detailed configuration of regular expression of autonomous system, refer to the “BGP Configuration” section in the “Routing Protocol” of this manual. For the other configuration, refer to the "IP Routing Policy" section in "Routing Protocol" of this manual.

6.2.14 Configuring MBGP Route Filtering

The route filtering configuration of MBGP is the same as that of unicast BGP.

For the detailed configuration, refer to the "BGP Configuration" section in "Routing Protocol" of this manual.

6.2.15 Resetting BGP Connections

After changing the MBGP policy or protocol configuration, users must disconnect the present BGP connection to make the new configuration effective.

For the detailed configuration, refer to the "BGP Configuration" section in "Routing Protocol" of this manual.

6.3 MBGP Display and Debug

Upon the above configuration, execute the **display** commands in any view to display the running information of MBGP, and to verify the effect of the configuration.

Execute the **debugging** command in user view for the debugging of MBGP.

Table 6-16 Display and debug MBGP

Operation	Command
Display an MBGP routing table	**display bgp multicast routing** *ip-address*
Display in the BGP routing table the MBGP routes that match the specified AS path list.	**display bgp multicast routing as-path-acl** *as-path-acl*
Display CIDR (classless inter-domain routing)	**display bgp multicast routing cidr**
Display the routing information about the specified MBGP community	**display bgp multicast routing community** [*community-number* | **no-export-subconfed** | **no-advertise** | **no-export** | **whole-match**]
Display the routes permitted by the specified MBGP community list	**display bgp multicast routing community-list** *community-list-number* [**whole-match**]
Display the routes with inconsistent source autonomous systems	**display bgp multicast routing different-origin-as**
Display the routing information to or from a specified multicast neighbor	**display bgp multicast routing peer** *peer-address* { **received** | **advertised** }
Display the routing information advertised by MBGP	**display bgp multicast network**

Operation	Command
Display the peer group information	**display bgp multicast group** [*group-name*]
Display information on MBGP peers.	**display bgp multicast peer** [*ip-address* | **verbose**]
Enable the debugging of MBGP UPDATE packets	**debugging bgp mp-update** [**receive| send** | **verbose**]

6.4 Typical MBGP Multicast Extension Configuration Example

I. Network requirements

This example describes how the administrator uses the MBGP attributes to manage route selection.

All routers are configured with MBGP. The IGP in AS200 uses OSPF. Router A in AS100 is the MBGP neighbor of Router B and C in AS200. Router B and C run IBGP with Router D which is also in AS200.

II. Network diagram

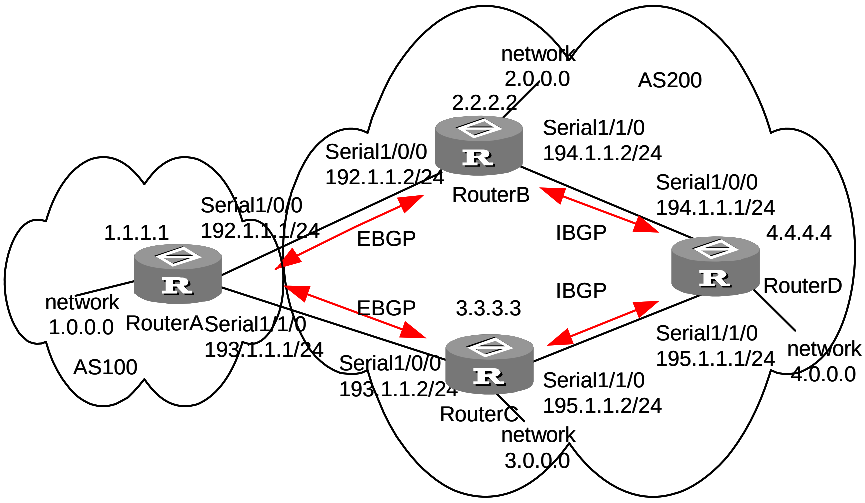


Figure 6-1 Network diagram for MBGP path selection

III. Configuration procedure

1) Configure Router A:

```
<RouterA> system-view
[RouterA] interface serial 1/0/0
[RouterA-Serial1/0/0] ip address 192.1.1.1 255.255.255.0
[RouterA-Serial1/0/0] quit
```

```
[RouterA] interface serial 1/1/0
[RouterA-Serial1/1/0] ip address 193.1.1.1 255.255.255.0
[RouterA-Serial1/1/0] quit
```

# Enable MBGP.

```
[RouterA] bgp 100
[RouterA-bgp] ipv4-family multicast
```

# Enable MBGP in a specified network segment.

```
[RouterA-bgp-af-mul] network 1.0.0.0
[RouterA-bgp-af-mul] network 2.0.0.0
[RouterA-bgp-af-mul] quit
```

# Configure the peer relationship.

```
[RouterA-bgp] bgp 100
[RouterA-bgp] group a1 external
[RouterA-bgp] peer 192.1.1.2 group a1 as-number 200
[RouterA-bgp] group a2 external
[RouterA-bgp] peer 193.1.1.2 group a2 as-number 200
[RouterA-bgp] ipv4-family multicast
[RouterA-bgp-af-mul] peer a1 enable
[RouterA-bgp-af-mul] peer 192.1.1.2 group a1
[RouterA-bgp-af-mul] peer a2 enable
[RouterA-bgp-af-mul] peer 193.1.1.2 group a2
[RouterA-bgp-af-mul] quit
```

# Configure the MED attribute of Router A.

# Add an ACL on Router A to permit network 1.0.0.0.

```
[RouterA] acl number 2001
[RouterA-acl-basic-2001] rule permit ip source 1.0.0.0 0.255.255.255
```

# Define two routing policies: set_med_50 and set_med_100, providing two MED values for network 1.0.0.0 (50 and 100).

```
[RouterA] route-policy set_med_50 permit node 10
[RouterA-route-policy] if-match acl 2001
[RouterA-route-policy] apply cost 50
[RouterA-route-policy] quit
[RouterA] route-policy set_med_100 permit node 10
[RouterA-route-policy] if-match acl 2001
[RouterA-route-policy] apply cost 100
```

# Apply the routing policy set_med_50 to the exported route updates of Router C (193.1.1.2). Apply the routing policy set_med_100 to the exported route updates of Router C (192.1.1.2).

```
[RouterA] bgp 100
```

```
[RouterA-bgp] ipv4-family multicast
[RouterA-bgp-af-mul] peer a2 route-policy set_med_50 export
[RouterA-bgp-af-mul] peer a1 route-policy set_med_100 export
```

2) Configure Router B:

```
<RouterB> system-view
[RouterB] interface serial 1/0/0
[RouterB-Serial1/0/0] ip address 192.1.1.2 255.255.255.0
[RouterB-Serial1/0/0] quit
[RouterB] interface serial 1/1/0
[RouterB-Serial1/1/0] ip address 194.1.1.2 255.255.255.0
[RouterB-Serial1/1/0] quit
[RouterB] ospf
[RouterB-ospf-1] area 0
[RouterB-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] network 192.1.1.0 0.0.0.255
[RouterB-ospf-1-area-0.0.0.0] quit
[RouterB-ospf-1] quit
[RouterB] bgp 200
[RouterB-bgp] undo synchronization
[RouterB-bgp] group b1 external
[RouterB-bgp] peer 192.1.1.1.1 group b1 as-number 100
[RouterB-bgp] group b2 internal
[RouterB-bgp] peer 194.1.1.1.1 group b1 as-number 200
[RouterB-bgp] peer 195.1.1.1.2 group b1 as-number 200
[RouterB-bgp] ipv4-family multicast
[RouterB-bgp-af-mul] peer b1 enable
[RouterB-bgp-af-mul] peer 192.1.1.1 group b1
[RouterB-bgp-af-mul] peer b2 enable
[RouterB-bgp-af-mul] peer 194.1.1.1 group b2
[RouterB-bgp-af-mul] peer 195.1.1.2 group b2
```

3) Configure Router C:

```
<RouterC> system-view
[RouterC] interface serial 1/0/0
[RouterC-Serial1/0/0] ip address 193.1.1.2 255.255.255.0
[RouterC-Serial1/0/0] quit
[RouterC] interface serial 1/1/0
[RouterC-Serial1/1/0] ip address 195.1.1.2 255.255.255.0
[RouterC-Serial1/1/0] quit
[RouterC] ospf
[RouterC-ospf-1] area 0
[RouterC-ospf-1-area-0.0.0.0] network 193.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] network 195.1.1.0 0.0.0.255
[RouterC-ospf-1-area-0.0.0.0] quit
```

```
[RouterC-ospf-1] quit
[RouterC] bgp 200
[RouterC-bgp] undo synchronization
[RouterC-bgp] group c1 external
[RouterC-bgp] peer 193.1.1.1 group c1 as-number 100
[RouterC-bgp] group c2 internal
[RouterC-bgp] peer 194.1.1.2 group c2 as-number 200
[RouterC-bgp] peer 195.1.1.1 group c2 as-number 200
[RouterC-bgp] ipv4-family multicast
[RouterC-bgp-af-mul] peer c1 enable
[RouterC-bgp-af-mul] peer 193.1.1.1 group c1
[RouterC-bgp-af-mul] peer c1  next-hop-local
[RouterC-bgp-af-mul] peer c2 enable
[RouterC-bgp-af-mul] peer 194.1.1.2 group c2
[RouterC-bgp-af-mul] peer 195.1.1.1 group c2
[RouterC-bgp-af-mul] peer c2  next-hop-local
```

# Configure the local preference attribute of Router C.

# Add ACL 2001 on Router C to permit network 1.0.0.0.

```
[RouterC] acl number 2001
[RouterC-acl-basic-2001] rule permit source 1.0.0.0 0.255.255.255
[RouterC-acl-basic-2001] quit
```

# Define the routing policy named "localpref". Set the local preference for the routes matching ACL 2001 to 200, and otherwise, to 100.

```
[RouterC] route-policy localpref permit node 10
[RouterC-route-policy] if-match acl 2001
[RouterC-route-policy] apply local-preference 200
[RouterC-route-policy] quit
[RouterC] route-policy localpref permit node 20
[RouterC-route-policy] apply local-preference 100
```

# Apply this routing policy to the inbound traffic from BGP neighbor 193.1.1.2 (Router A).

```
[RouterC] bgp 200
[RouterC-bgp] ipv4-family multicast
[RouterC-bgp-af-mul] peer c1 route-policy localpref import
```

4) Configure Router D:

```
<RouterD> system-view
[RouterD] interface serial 1/0/0
[RouterD-Serial1/0/0] ip address 194.1.1.1 255.255.255.0
[RouterD-Serial1/0/0] quit
[RouterD] interface serial 1/1/0
[RouterD-Serial1/1/0] ip address 195.1.1.1 255.255.255.0
```

```
[RouterD-Serial1/1/0] quit
[RouterD] ospf
[RouterD-ospf-1] area 0
[RouterD-ospf-1-area-0.0.0.0] network 194.1.1.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] network 195.1.1.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] network 4.0.0.0 0.0.0.255
[RouterD-ospf-1-area-0.0.0.0] quit
[RouterD-ospf-1] quit
[RouterD] bgp 200
[RouterD-bgp] undo synchronization
[RouterD-bgp] group d1 internal
[RouterD-bgp] peer 194.1.1.2 group d1
[RouterD-bgp] peer 194.1.1.2 group d1
[RouterD-bgp] ipv4-family multicast
[RouterD-bgp-af-mul] peer d1 enable
[RouterD-bgp-af-mul] peer 195.1.1.2 group d1
[RouterD-bgp-af-mul] peer 194.1.1.2 group d1
```

To make the configuration effective, the **reset bgp all** command on all MBGP neighbors.

Chapter 7 Multicast Static Route Configuration

7.1 Multicast Static Route Overview

A multicast network topology may be different from a unicast topology. Some routers in the network may only support unicast rather than multicast. Multicast static routes are helpful when you need to separate paths between unicast datagram and multicast datagram.

For example, when there are routers not supporting multicast on the path between the source and the destination, a multicast router can use a tunnel to transmit multicast packets to a neighboring multicast router. As shown in Figure 7-1, each unicast router supports unicast only. Multicast datagram transmits between multicast routers over a tunnel. If no multicast static route is configured, unicast datagram will also be sent over the tunnel. When a multicast static route is configured, the tunnel is specialized in multicast datagram transmission.

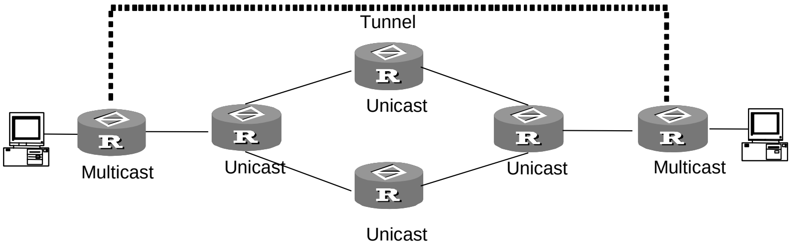


Figure 7-1 Transmit a multicast datagram over a tunnel

Multicast static routes only have effect on the related multicast routers and will not be advertised or imported to any other router in any way.

7.2 Multicast Static Route Configuration

Multicast Static Route configuration tasks include:

- Configure a multicast static route
- Change the multicast RPF route selection policy

📖 **Note:**

Multiple multicast static routes on a same network segment are matched by order of configuration. It is therefore very important to ensure the correct configuration sequence.

7.2.1 Configuring a Multicast Static Route

Perform the following configuration in system view.

Table 7-1 Configure a multicast static route

Operation	Command
Configure a multicast static route	**ip rpf-route-static** *source* { *mask* | *mask-length* } [*protocol*] [**route-policy** *policyname*] { *rpf-nbr* | *interface-type interface-number* } [**preference** *preference*]
Remove a multicast static route from the multicast static routing table	**undo ip rpf-route-static** *source* { *mask* | *mask-length* } [*protocol*] [**route-policy** *policyname*]
Remove all the multicast static routes	**delete rpf-route-static all**

source/mask, *protocol* and **route-policy** are key factors for multicast static routes. The routes are considered different if any of the three have different configurations. Check the multicast static routing tree before configuring any. If the desired already exists, modify the relevant fields as necessary (not the configuration order field); otherwise, configure to add it. Each network segment allows 8 different configurations.

Note:

The multicast static route may not become effective as soon as the **ip rpf-route-static** is configured, once outbound interfaces cannot be iterated or the specified interface goes "DOWN". Therefore, when performing this configuration, it is recommended to use the **display multicast routing-table static config** command to check whether the route has been successfully configured and the **display multicast routing-table static** command to check whether the route becomes effective.

7.2.2 Configuring the Multicast RPF Route Selection Policy

There are two kinds of multicast RPF route selection policies: longest-match rule and preference-preferred rule. The former indicates to select the routes with the longest mask from the MBGP routes, multicast static routes and unicast routes. The latter however selects those with the highest preference (with the smallest value) from the above three types of routes.

Perform the following configuration in system view.

Table 7-2 Configure the multicast RPF route selecting policy

Operation	Command
Apply the longest-match rule	**ip rpf-longest-match**
Restore the default configuration	**undo ip rpf-longest-match**

By default, routes are selected according to the preference-preferred rule.

7.3 Multicast Static Route Display and Debug

Upon the above configuration, execute the **display** commands in any view to display the running information of multicast static routes, and to verify the effect of the configuration.

Table 7-3 Display and debug multicast static routes

Operation	Command
Display the configured multicast static routes	**display multicast routing-table static config** [*source mask*]
Display the active multicast static routes	**display multicast routing-table static** [*source mask*]

7.4 Typical Multicast Static Route Configuration Example

I. Network requirements

In the following networking environment, Routers RT1 and RT2 work in the OSPF domain. RT1 supports multicast but RT2 runs a unicast routing protocol. RT0 is a router that runs a multicast routing protocol outside the domain. For RT1 to get the multicast source information outside the domain through RT0 and the multicast source information in the domain through RT2, perform the following configuration.

II. Network diagram

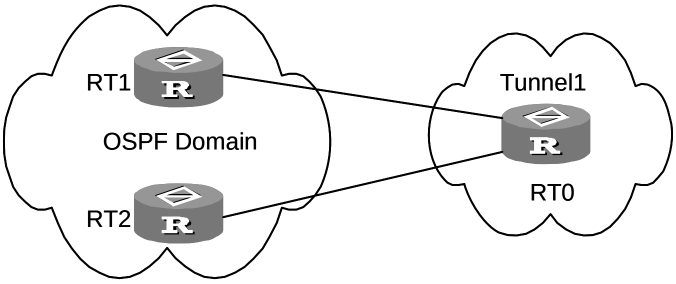


Figure 7-2 Network diagram for multicast static routing configuration

III. Configuration procedure

Configure RT1:

```
<RT1> system-view
[RT1] ip rpf-route-static 0.0.0.0 0.0.0.0 ospf null0 preference 255
[RT1] ip rpf-route-static 0.0.0.0 0.0.0.0 tunnel1
```

The first command allows the matching-rule-compliant multicast source information in the domain to pass the RPF check when it reaches RT1 through RT2. The second command allows the multicast source information outside the domain to pass the RPF check when it reaches RT1 through tunnel1.

MPLS

Table of Contents

Chapter 1 MPLS Architecture

1.1 MPLS Overview

MPLS (Multiprotocol Label Switching) encapsulates packets with labels of short and fixed length. MPLS obtains service from various link layers (such as PPP, ATM, Frame Relay, and Ethernet) and provides connection-oriented service for network layer. MPLS can obtain support from IP routing protocol and control protocol and, at the same time, it supports policy-based restraint route. It possesses powerful and flexible routing functions and is capable of satisfying the requirements for the network from various new applications. This technology was initially originated from IPV4. However, its core technology can be extended to multiple network protocols (IPV6, IPX, etc).

MPLS is a protocol initially developed for increasing forwarding speed of routers. However, it has gained wider applications in traffic engineering, VPN, and QoS and is becoming an important standard for large-scale IP networks.

1.2 MPLS Basic Concepts

1.2.1 FEC

Forwarding Equivalent Class (FEC), in fact, is a kind of classify-and-forward technology. It categorizes packets with the same forwarding strategy (same destination addresses, same forwarding routes and same QoS levels) into one group, which is called a FEC. The FEC classification is based on the network layer address. Packets in the same FEC will be processed in absolutely the same way.

1.2.2 Label

I. Label definition

Label is a locally significant and short identifier with fixed length, which is used to identify a particular FEC. When reaching at MPLS network ingress, packets are divided into different FECs, on which different labels are encapsulated. Later forwarding is based on these labels.

II. Label structure

The structure of the label is shown in Figure 1-1.

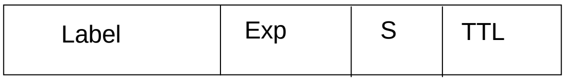


Figure 1-1 Label structure

Label is located between the link layer header and the network layer packet, with the length of 4 bytes. A label contains four fields:

Label: label value, 20bits, used as the pointer for forwarding.

Exp: 3bits, reserved for test.

S: 1bit, MPLS supports hierarchical label structure, i.e., multi-layer label. Value 1 refers to the label of bottom layer.

TTL: 8 bits, similar to TTL in IP packets.

III. Label operations

1) Label mapping

There are two types of label mapping: one is label mapping at ingress routers and the other is label mapping in MPLS domain.

The first type is also called ingress LSR, in which input packets are grouped on a certain principle into multiple FECs. The corresponding labels are mapped to these FECs and the mapping results are recorded into label information base (LIB). In simple words, it is to assign a label to a FEC.

The second type is also called incoming label mapping (ILM), that is, to map each input label to a series of next hop label forwarding entries (NHLFE). The packets are forwarded along the paths based on the mapping results.

2) Label encapsulation

Label encapsulation in different media is illustrated in Figure 1-2.

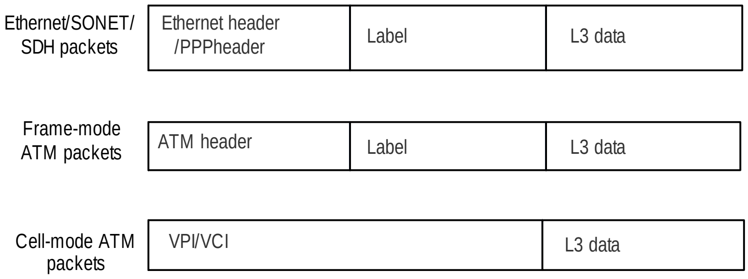


Figure 1-2 Label position in packet

3) Label assignment and distribution

Label distribution refers to the process for a FEC to create corresponding label switching path (LSP).

In the MPLS architecture, the decision to bind a particular label to a particular FEC is made by downstream LSR, and the downstream LSR notifies the upstream LSR. That is to say, the label is specified by the downstream LSR, and the label is distributed from downstream to upstream.

Two label distribution modes are available in MPLS: Downstream unsolicited (DU) mode and downstream on demand (DoD) mode.

For a specific FEC, if LSR originates label assignment and distribution even without receiving label request messages from upstream, it is in DU mode.

For a specific FEC, if LSR begins label assignment and distribution only after receiving label request messages from upstream, it is in DoD mode.

The upstream and downstream, which have adjacency relation in label distribution, should reach agreement on label distribution mode.

For the peers, LSR can use LDP messages to distribute labels or bear labels over other routing protocol messages.

🕮 **Note:**

Upstream and downstream are just on a relative basis: For a packet forwarding process, the transmit router serves as upstream LSR and receive router serves as downstream LSR.

4) Label control mode

There are two types of label control modes: independent mode and ordered mode.

In independent control mode, each LSR can notify label mapping messages anytime.

In ordered control mode, a LSR can send label mapping messages to upstream only when it receives a specific label mapping messages of the next hop of a FEC or the LSR serves as LSP (Label distribution protocol) egress node.

5) Label retention mode

There are two label-retention modes: liberal label retention mode and conservative label retention mode.

For a specific FEC, if LSR Ru has received the label binding from LSR Rd, in case Rd is not the next hop of Ru and Ru saves this binding, then it is called liberal label retention mode. If Ru discards this binding, then it is called conservative label retention mode.

In case it is required that LSR is capable of adapting route variation rapidly, liberal label retention mode can be adopted. In case it is required that a few labels are saved in LSR, then conservative label retention mode can be used.

1.2.3 LDP

Label distribution protocol (LDP) is the signaling control protocol in MPLS, which controls binding of exchange labels and FECs between LSRs and coordinates a series of procedures between LSRs.

1.3 MPLS Architecture

1.3.1 MPLS Network Structure

The basic composing unit of MPLS network is LSR (Label Switching Router). It runs MPLS control protocol and L3 routing protocol, exchanges routing messages with other LSRs and create the routing table, maps FECs with IP packet headers, binds FECs with labels, distributes label binding messages, establishes and maintains label forwarding table.

The network consisting of LSRs is called MPLS domain. The LSR that is located at the edge of the domain edge LSR (LER, Labeled Edge Router). It connects an MPLS domain with a non-MPLS domain or with another MPLS domain, classifies packets, distributes labels (as egress LER) and distracts labels. The ingress LER is termed as ingress and egress LER as egress.

The LSR located inside the domain is called core LSR. The core LSR can be either the router that supports MPLS or the ATM-LSR upgraded from ATM switch. It achieves label swapping and label distribution. The labeled packets are transmitted along the LSP (Label Switched Path) composed of a series of LSRs.

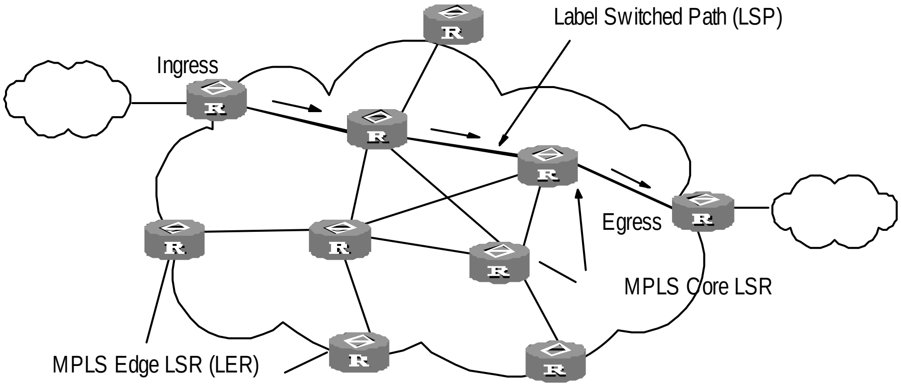


Figure 1-3 MPLS basic principle

1.3.2 LSP Establishment

Actually, LSP establishment refers to the process of binding FEC with the label, and then advertising this binding to the adjacent LSR on LSP. This process is implemented via Label Distribution Protocol (LDP). LDP regulates the message in interactive processing and message structure between LSRs as well as routing mode. Refer to the following section for the detail description of LDP

1.3.3 LSP Tunnel and Hierarchy

I. LSP tunnel

MPLS supports LSP tunnel technology. On an LSP path, LSR Ru and LSR Rd are upstream and downstream for each other. However, the path between LSR Ru and LSR Rd may not be part of the path provided by routing protocol. MPLS allows establishing a new LSP path <Ru R1...Rn Rd> between LSR Ru and LSR Rd, and LSR Ru and LSR Rd are respectively the starting point and ending point of this LSP. The LSP between LSR Ru and LSR Rd is referred to as the LSP tunnel, which avoids the traditional encapsulated tunnel on the network layer. If the route along which the tunnel passes and the route obtained hop by hop from routing protocol is in consistent, this tunnel is called hop-by-hop routing tunnel. And if the two routes are not in consistent, then the tunnel of this type is called explicit routing tunnel.

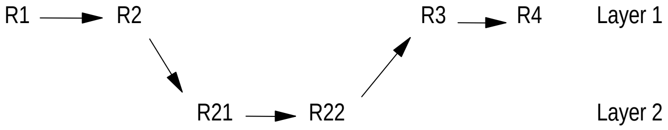


Figure 1-4 LSP tunnel

As shown in Figure 1-4, LSP <R2 R21 R22 R3> is a tunnel between R2 and R3.

II. Multi-layer label stack

When the packet is sent in LSP tunnel, there will be multiple layers for the label of the packet. Then, on the ingress and egress of each tunnel, it is necessary to implement incoming and outgoing operation for the label stack. For each incoming operation, the label will be added with one layer. And there is no depth limitation for the label stack from MPLS.

The labels are organized according to the principle “last in first out” in the label stack, and MPLS processes the labels beginning from the top of the stack.

Suppose that a packet has the label stack depth of m, then the label at the bottom of the stack is the label of first level, and the label at the top of the stack is the label of level m. The packet with no label can be regarded as the packet of blank label stack (namely, the label stack depth is zero).

1.3.4 Forwarding Labeled Packets

In Ingress, the packets entering the network are classified into Forwarding Equivalence Class (FEC) according to their characteristics. Usually, FEC is classified according to the IP address prefix or host address. The packets with the same FEC will pass through the same path (i.e., LSP) in MPLS area. LSR assigns a short label of fixed length for the incoming FEC packet, and then forwards it through the corresponding interface.

On the LSR along the LSP, the mapping table of the import/export labels has been established (the element of this table is referred to as Next Hop Label Forwarding Entry (NHLFE)). When the labeled packet arrives, LSR only needs to find the corresponding NHLFE from the table according to the label and replace the original label with the new special label, and then forwards the labeled packet. This process is called Incoming Label Map (ILM).

On the Ingress, MPLS specifies FEC of specific packet, and the following routers only need to forward it by label switching therefore this method is much simpler than the routine network layer forwarding.

Note:

TTL Processing:
For labeled packet, it is necessary to copy the TTL value in the original IP packet into the TTL field in the label. While forwarding the label type packet, LSR will perform minus one operation for the TTL field of the label on the top of the stack. When the label is out of the stack, the TTL value on the top of the stack is copied back to IP packet or the label of lower layer.
However, while LSP goes through the non-TTL LSP segment composing of ATM-LSR or FR-LSR, the LSR inside the non-TTL LSP segment is not capable of processing TTL field. In this case, it is necessary to carry out unified processing for TTL while entering non-TTL LSP segment, namely, to reduce for one time the value that reflects the length of this non-TTL LSP.

1.4 LDP Overview

The LDP is responsible for message regulation and relevant processing in the label distribution.

An LSR can directly map the routing information on the network layer to a switch path on the data link over LDP, and then establish an LSP on the network layer. The LSP can be set up between two adjacent LSRs or terminated at an Egress LSR. All the LSRs in between adopt the label switching.

1.4.1 LDP Basic Concepts

I. LDP Peers

LDP peers refer to two LSRs undergo an LDP session by exchanging label/FEC mapping information over LDP.

The LDP peers can obtain the other’s label information through an LDP session, namely, the LDP is bidirectional.

II. LDP Session

An LDP session is to exchange label and release messages between LSRs. There are two types of LDP session:

- Local LDP Session: an LDP session between two directly connecting LSRs.
- Remote LDP Session: an LDP session between two indirectly connecting LSRs.

III. LDP Message

There are four types of message involved in the LDP.

- Discovery message: used to notify or maintain the existing LSRs in the network;
- Session message: used to establish, maintain or terminate a session between LDP peers;
- Advertisement message: used to establish, modify or delete a flag, that is, an FEC binding;
- Notification message: used to provide suggestive messages or error notifications.

IV. Label Space and LDP Identifier

A label space refers to the range of labels that can be allocated to LDP peers. You can specify a label space for each interface of an LSR or for the entire LSR.

An LDP identifier is to identify a special LSR label space. It is a six-byte value in the following format:

<IP address> : <Label space number>

Here the IP address of four bytes is the LSR IP address and the remaining two bytes is the label space number.

1.4.2 LDP Working Process

Figure 1-5 illustrates the LDP label distribution.

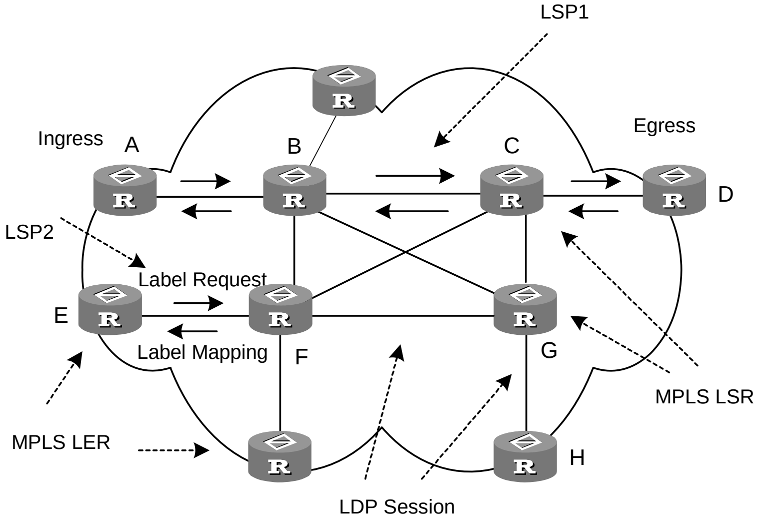


Figure 1-5 Label distribution process

On an LSP, along the data transmission direction, neighboring LSRs are respectively called as upstream LSR and downstream LSR. On LSP1 shown in Figure 1-5, LSR B is the upstream LSR of LSR C.

Labels can be distributed in two modes: downstream on demand (DoD) and downstream unsolicited (DU), depending on whether label mapping distribution is done at the downstream with solicitation or without.

1) DoD mode

In DoD mode, the label is distributed in this way: the upstream LSR sends label request message (containing FEC descriptive information) to the downstream LSR, and the downstream LSR distributes label for this FEC, and then sends the bound label back to the upstream LSR through label mapping message.

When the downstream LSR feeds back the label mapping message depends on whether this LSR uses independent label control mode or sequential label control mode. When the sequential label control mode is used by the downstream LSR, the label mapping message is sent back to its upstream LSR if only it has received the label mapping message from its downstream LSR. And when the independent label control mode is used by the downstream LSR, it will send label mapping message to its upstream LSR immediately, no matter if it has received the returned label mapping message from its downstream LSR.

Usually, the upstream LSR selects the downstream LSR according to the information in its routing table. In Figure 1-5, the sequential label control mode has been used by the LSRs on the way along LSP1, and the independent label control mode has been used by the LSRs on LSP2.

2) DU mode

In DU mode, the label is distributed in the following way: when LDP session is established successfully, the downstream LSR will actively distribute label mapping message to its upstream LSR. The upstream LSR saves the label mapping information and processes the received label mapping information according to the routing table.

1.4.3 LDP Basic Operation

The basic LDP operation includes:

- Discovery phase
- Session establishment and maintenance
- LSP setup and maintenance
- Session termination

I. Discovery Phase

The originating LSR periodically sends a Hello message to its adjacent LSRs, notifying them its peer information, so that the LSR can automatically find its LDP peer.

There are two types of LDP discovery mechanisms.

- Basic discovery mechanism

The basic discovery mechanism is to discover the local LDP peer, that is, to establish a local LDP session between directly connecting LSRs.

In this case, the LSR periodically sends a Hello message of the LDP link to a specific port, carrying the LDP identifier of the label space where the specific port belongs as well as other relevant information. If the LSR receives the Hello message over the specific port, it knows that there is a potential reachable peer on the link layer and learns the label space of the port.

- Extended discovery mechanism

The extended discovery mechanism is to discover a remote LDP peer, that is, to establish a remote LDP session between non-directly connecting LSRs.

In this case, the LSR periodically sends an LDP Targeted Hello message to a specific IP address.

The LDP Targeted Hello message is sent in a UDP packet to the Well-known LDP discovery port of the specific address. The message contains the desired label space of the LSR as well as all relevant information.

II. Session Establishment and Maintenance

After the peer is set up, the LSR begins to establish a session by the following two steps:

- Establishing a connection on the transport layer, that is, establishing TCP connection between the LSR peers;
- Initializing the session and negotiating the parameters involved in the session, such as the LDP version, label distribution mode, timer timeout and label space.

III. LSP Setup and Maintenance

Actually, LSP establishment refers to the process of binding FEC with the label, and then advertising this binding to the adjacent LSR on LSP. This process is implemented through LDP in the following steps:

1) When the routing of the network changes and an LER finds a new destination address in its routing table not belonging to any existing FEC, the LER needs to create an FEC for the address and determine routes for the FEC, and then sends a label request message to the downstream LSR, indicating the FEC to be allocated;
2) After the downstream LSR receives the label request message and records it, it relays the message to the next hop LSR according to its routing table;
3) When the label request message reaches the destination LSR or the Egress LSR in the MPLS network and either can allocate the requested label, it will allocate the label to the FEC after the label request message passes its authentication. Then it

sends a label mapping message to the upstream LSR with the allocated label information included;

4) The upstream LSR compares the received label mapping message with its label database, allocates the matched label to the FEC, adds the map to its label forwarding table, and then sends the label mapping message to its upstream LSR;
5) When the Ingress ISR receives the label mapping message, it adds the map to its label forwarding table. In this way, an LSP is set up and the corresponding FEC data packet can be forwarded based on its label.

IV. Session Termination

The LDP checks the session integrity depending on the LDP PDU transmitted in the session connection.

The LSR sets up a living timer for each session and refreshes the timer after receiving an LDP PDU. If the timer expires before the reception of an LDP PDU, the LSR considers the session interrupted and tears down the corresponding connection on the transport layer to terminate the session.

1.4.4 LDP Loop Detection

It is necessary to prevent path loop from happening while establishing LSP in the MPLS domain. The LSP loop detection mechanism can detect such path loop and avoid message loop occurring such as the label request message.

To avoid the LSP path loop, two methods can be used:

I. Maximum Hop Count

The maximum hop count method is to contain the hop-count information in the message bound with the forwarding label. This value is added by one for each hop. When the value exceeds the specified maximum value, it is considered that a loop happens, and the process for establishing LSP is terminated.

II. Path Vector

The path vector method is to record the path information in the message bound with the forwarding label. For every hop, the corresponding router checks if its ID is contained in this record. If not, the router adds its ID into the record; and if so, it indicates that a loop happens and the process for establishing LSP is terminated.

1.4.5 Constrain-based Routing LDP

MPLS also supports Constrain-based Routing LDP mechanism (CR-LDP). The so-called CR-LDP refers to that, while originating the establishment of LSP, the ingress node adds some constrain information for LSP routing in label request message. Two routing approaches are available: strict explicit routing, where the constraint information is the exact designation of all the LSRs along the path; and loose explicit routing where only some of the LSRs along the path are specified.

1.5 MPLS and Other Protocols

1.5.1 MPLS and Routing Protocols

When LDP establishes LSP in hop-by-hop mode, the next hop will be determined by using the information that is usually collected via such routing protocols as IGP, BGP in each LSR route forwarding table on the way. However, LDP just uses the routing information indirectly, rather than being associated with various routing protocols directly.

On the other hand, although LDP is the special protocol for implementing label distribution, but it is not the sole protocol for label distribution. The existing protocols such as BGP, RSVP, after being extended, can also support MPLS label distribution. For some MPLS applications, it is also necessary to extend some routing protocols. For example, MPLS-based VPN application needs the extension of BGP so that the BGP is capable of supporting the sending of VPN routing information. In addition, MPLS-based Traffic Engineering (TE) needs the extension of OSPF or IS-IS protocol to carry link status information.

1.5.2 MPLS Extension by RSVP

Resource Reservation Protocol (RSVP), after being extended, can support MPLS label distribution. At the same time, while transmitting label-binding message, it is also capable of carrying resource reservation information. The LSP established in this way is of resource reservation function, namely, the LSRs on the way can distribute some resources for this LSP to ensure the service transmitted on it.

The extension of RSVP mainly refers to adding new objects in its Path message and Resv message. Besides carrying label binding information, these new objects are also capable of carrying the constrain information for searching path for the LSRs on the way, thus supporting LSP constraining function on routing. The extended RSVP also supports fast rerouting, namely, when it is necessary to change LSP under some condition, the original service flow can be rerouted to the newly established LSP without interrupting the customer service.

1.6 MPLS Application

1.6.1 MPLS-Based VPN

For traditional VPN, the transmission of the data flow between private networks on the public network is usually realized via such tunneling protocols as GRE, L2TP and PPTP, and LSP itself is the tunnel on the public network. The implementation of VPN using MPLS is of natural advantages. MPLS-based VPN connects the geographically different branches of private network by using LSP, forming a united network. MPLS-based VPN also supports the interconnection between different VPNs.

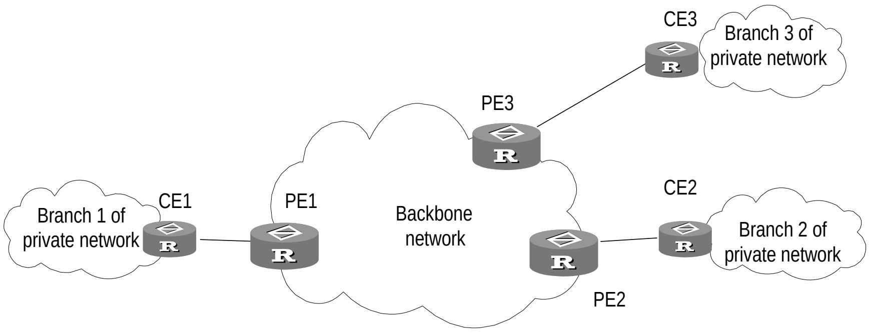

CE3
Branch 3 of private network
PE3
Branch 1 of private network
CE1
PE1
Backbone network
CE2
Branch 2 of private network
PE2
R

Figure 1-6 MPLS-based VPN

The basic structure of MPLS-based VPN is shown in Figure 1-6. CE is the customer edge device, and it may be a router, a switch, or perhaps a host. PE is a service provider edge router, which is located on the backbone network. PE is responsible for the management of VPN customers, establishing LSP connection between various PEs, route allocation among different branches of the same VPN customer.

Usually the route allocation between PEs is realized by using extended BGP. MPLS-based VPN supports the IP address multiplexing between different branches and the interconnection between different VPNs. Compared with traditional route, it is necessary to add branch and VPN distinguisher information in VPN route. Therefore, it is necessary to extend BGP to carry VPN routing information.

1.6.2 MPLS-Based QoS

QoS is indispensable to the implementation of voice, video, and some other real-time services over an IP network in the sense that it can differentiate the data streams so that those crucial, sensitive, and delay-sensitive data streams over the network can be processed first. As Huawei Technologies devices support MPLS-based Diff-serv features, they can provide differentiated services for the data streams assigned with different precedence levels while maintaining high network efficiency. Thus, they can provide the services featuring guaranteed bandwidth, low delay, and low loss rate for voice and video traffic. As it is difficult to deploy TE over the entire network, the Diff-ser model is always preferred for implementing QoS in actual networking solutions.

The basic mechanism of Diff-serv goes like this: A service is mapped to a service category, which can be uniquely identified by the DS bits in the TOS field of the IP packets, according to the required service quality at the network edge. Then, the nodes on the backbone network adopt the proper service policy to process the packets according to the service category defined by the DS bits (derived from the TOS field), ensuring the proper service quality. The service quality classification and the label mechanism in Diff-serv are very similar to the label distribution in MPLS. In fact, MPLS-based Diff-serv is fulfilled by integrating DS assignment into the label distribution process of MPLS.

Diff-serv defines the same processing method, which includes queue selection, queuing, and the drop operation, for each service category. The combination of these processing operations is called Per Hop Behavior (PHB). In addition, the packets that belong to the same PHB may be assigned with different drop preference. The information of PHB and drop preference is indicated by the DS code assigned to the packets. The DS codes are also known as Diff-serv Code Point (DSCP). For more information about Diff-serv, refer to the Section QoS Configuration in this manual.

The following methods are available for supporting end-to-end QoS based on the Diff-serv model:

- IP Precedence for Traffic Classification

IP precedence classification is implemented at the network edge. It makes use of the 3-bit Type-of-Service field in the IPv4 header to sort precedence of the IP packets according to their addresses. At the core, different queuing technologies are used to make different processing on the streams of different precedence, thus to discriminate the services at different levels. To implement Diff-serv for the voice, image, and data streams, when PE labels the packets, that is, makes label switching for different traffic, it will map the TOS value carried in the IP packets to the COS field of the label. Thus, the type information previously carried by IP will be carried by the label. Depending on the CoS field of the label, PE routers will implement differentiated scheduling on the packets using PQ, CQ, WFQ or CBQ.

- TP for implementing committed and constraint bandwidth

This function can be implemented by configuring Traffic Policing (TP) on the link that connects PE to CE. In addition, TP also provides the functions of committed bandwidth and constraint bandwidth.

- WRED for congestion avoidance

WRED can be used to monitor and alleviate network congestion at the bottleneck of the network. Usually, congestion is more likely caused at the access layer. At the onset of congestion, WRED, which is monitoring the network load, begins to select packets and discard them for decreasing the traffic size. The packet drop policy of WRED is to discard the packets of low preference to ensure the smooth transmission of high preference packets. Running WRED on a port prone to congestion is a good choice for congestion avoidance.

In actual deployment, the tasks should be distributed in order to achieve the optimal efficiency. As QoS is such an application that will consume enormous resources of the processor, the tasks of QoS are shared by the edge and core routers so as to alleviate the load imposed on a single router.

To sum up, four steps should be followed in order to implement CoS-based Diff-serv:

- Impose the incoming bandwidth constraint on the MPLS edge router to classify the incoming traffic.
- Adopt CAR on the edge devices so that they can share the work of bandwidth management.
- The MPLS core router accomplishes CoS management to implement Diff-serv QoS.
- The egress device, like the ingress device, implements bandwidth restriction. The bandwidth restriction implemented by the ingress and egress devices protects the network from congestion and hence significantly improves the network scalability.

For more details, see QoS section.

Chapter 2 MPLS Basic Capability Configuration

2.1 Introduction to MPLS Basic Capability

The following MPLS basic capabilities are available:

- Basic MPLS forwarding

Each router interface supports the basic MPLS forwarding function, including label packet forwarding and TTL processing.

- LDP session establishment and LSP maintenance

Each interface supports LDP session and supports the loop detection in both maximum hop count mode and path vector mode. It can create and delete LSPs.

It also supports loose routing and strict explicit routing: You can also specify LSPs.

Besides MPLS basic functions, V 2.41 also provide performance monitoring and fault diagnostic tools.

To enable basic MPLS functions at a router, you should complete the following configuration tasks:

1) Configure LSR ID
2) Enable MPLS
3) Enable LDP protocol
4) Enter interface view and enable interface LDP function

Then the router can provides MPLS forwarding and LDP signaling functions.

If you want to modify the default parameters or enable some special functions, for example, creating LSP, creating explicit route, you just configure according to the method in configuration list. For some complicated functions, configuration combination may be required.

Currently, MPLS is not available on the following interfaces:

- Serial interface encapsulated with X.25 or MP
- ATM interface
- Dialer interface
- Virtual template interface

2.2 MPLS Basic Capability Configuration

MPLS basic capability configuration (compulsory) includes:

- Define MPLS LSR ID
- Disable/enable LDP and enter LDP view

MPLS basic capability configuration (optional) includes:

- Enable LDP on interface
- Control LDP loop detection
- Set LDP session keepalive parameters on interface

2.2.1 Defining MPLS LSR ID

Before configuring any other MPLS command, it is necessary to configure LSR ID firstly. The ID is usually in IP address format and must be unique in the domain.

Perform the following configurations in the system view.

Table 2-1 Define MPLS LSR ID

Operation	Command
Define LSR ID	**mpls lsr-id** *ip-address*
Delete LSR ID	**undo mpls lsr-id**

By default, LSR ID is not specified.

2.2.2 Entering MPLS View

To make the MPLS configurations, you must enter the MPLS view first.

Perform the following configuration in the system view, routing protocol view, interface view or virtual interface view.

Table 2-2 Enter MPLS view

Operation	Command
Enter MPLS view	**mpls**
Disable MPLS globally.	**undo mpls**

Executing the **mpls** command in the system view will enter the MPLS view.

Executing the **mpls** command in the interface view will enable the MPLS capability on the corresponding interface.

For those link layer protocols that do not support broadcast, such as X.25, Frame Relay, ATM, you must use the **protocol ip** { *ip-address* [*ip-mask*] **| default | inarp** [*minutes*] } [**broadcast**] command to configure the **broadcast** attribute to support the transmission of broadcast and multicast packets.

2.2.3 Configuring the Topology-Driven LSP Setup Policy

It refers to specifying filtering policy as all or ip-prefix.

Perform the following configuration in MPLS view.

Table 2-3 Configure a topology-driven LSP setup policy

Operation	Command
Configure a topology-driven LSP setup policy	**lsp-trigger** { **all | ip-prefix** *ip-prefix* }
Disable the filtering condition specified by the arguments and no routes of any type can trigger the LSP setup	**undo lsp-trigger** { **all** | **ip-prefix** [*ip-prefix*] }

2.2.4 Configuring Static LSP

You can manually set an LSR to be a node along an LSP, and place a limit on the traffic over the LSP. Depending on the position in an MPLS domain, LSR can be ingress, transit node, or an egress. Note that the correct operation of this LSP can be ensured only after the LSRs along the specified LSP have been properly configured.

The **undo static-lsp** command is used to delete a specified LSP established manually.

Perform the following configuration in MPLS view.

Table 2-4 Set this LSR to be a node on a specified LSP

Operation	Command
Set the current LSR to be the ingress of a specified LSP	**static-lsp ingress** *lsp-name* **destination** *dest-addr* { *addr-mask* | *mask-length* } **| l2vpn** } { **nexthop** *next-hop-addr* **| outgoing-interface** *interface-type interface-num* } **out-label** *out-label-value*
	undo static-lsp ingress *lsp-name* [**l2vpn**]
Set the current LSR to be a transit node along the specified LSP	**static-lsp transit** *lsp-name* [**l2vpn**] **incoming-interface** *interface-type interface-num* } **in-label** *in-label-value* { **nexthop** *next-hop-addr* **| outgoing-interface** *interface-type interface-num* } **out-label** *out-label-value*
	undo static-lsp transit *lsp-name* [**l2vpn**]
Set the current LSR to be the egress of the specified LSP	**static-lsp egress** *lsp-name* [**l2vpn**] **incoming-interface** *interface-type interface-num* **in-label** *in-label-value*
	undo static-lsp egress *lsp-name* [**l2vpn**]

2.2.5 Configuring IP TTL Duplication of MPLS

The MPLS label contains an eight-bit TTL field same as the one used in an IP header. It can be used for supporting the **tracert** command in addition to suppressing routing loops.

As described in RFC3031, when an LSR labels a packet, it needs to copy the TTL value in the IP packet or the upper layer label into the TTL field in the added label. When it forwards a labeled packet, it decrements the TTL value in the top label by one. When the LSR pops the stack, it copies the TTL value in the top label back to the IP packet or the lower label.

If an LSP has a non-TTL LSP segment which comprises a sequence of ATM-LSRs or FR-LSRs unable to handle the TTL field, the TTL value must be decremented by the value that reflects the length of the non-TTL LSP segment before a packet is forwarded into this segment.

In MPLS VPN networking, you may hide the MPLS backbone topology for security sake. You cannot however, apply on the ingress TTL duplication to VPN packets.

Perform the following configuration in MPLS view.

Table 2-5 Configure IP TTL duplication of MPLS

Operation	Command
Enable IP TTL duplication of MPLS.	**ttl propagate** { **public** | **vpn** }
Disable IP TTL duplication of MPLS.	**undo ttl propagate** { **public** | **vpn** }

By default, IP TTL duplication is enabled for public-network packets and disabled for VPN packets.

If IP TTL duplication is enabled at the ingress, the TTL value of packets is decremented at each LSR hop that it passes. This allows the tracert to reflect the path that a packet travels.

If IP TTL duplication is disabled at the ingress, the TTL value is not decremented at the LSR hops that packets travel and as such, those hops in the MPLS backbone are excluded from the path shown after you run a tracert, just as if the ingress and the egress are directly connected.

Note that:

- Inside an MPLS domain, if an MPLS packet has a label stack, the TTL value in a label is always copied from other labels in the stack.
- The TTL value of the transmitted local packets is copied regardless whether IP TTL duplication is enabled or not. This ensures that the local administrator can execute the tracert command to test the network.
- At the egress, if IP TTL duplication is enabled, the TTL value in the MPLS label is copied to the TTL field in the IP header and decremented by one.
- Configure IP duplication for VPN packets in the same way at the ingress and the egress: if the **ttl propagate vpn** command is enabled at the ingress, enable it at the egress; if the command is disabled at the ingress, disable it also at the egress. This ensures that the results of traceroutes can reflect the real network conditions. You are recommended to enable this function on the involved PEs to ensure consistency of the results gotten by tracerting on different PEs.
- You need not to configure the **ttl propagate** command on any P routers.

2.2.6 Configuring MPLS to Return ICMP Responses by IP routing

In an MPLS VPN network, a P router cannot route the IP packets encapsulated in MPLS. When the TTL value of an MPLS packet expires, the ICMP response continues to travel the LSP until reaching the egress, where it is forwarded by IP routing. This approach increases network traffic while decreasing reliability of packet forwarding.

For a one-tier MPLS packet with TTL expired, you can configure to have its ICMP response forwarded by local IP routing, that is, the default.

Perform the following configuration in MPLS view.

Table 2-6 Configure MPLS to return ICMP responses by IP routing

Operation	Command
Return ICMP responses by IP routing.	**ttl expiration pop**
Return ICMP responses along the LSP.	**undo ttl expiration pop**

On an ASBR or SPE (it can be an SPE in a nesting application) on an HoVPN network, the MPLS packets that carry VPN packets may have only one-tier labels. In this circumstance, to tracert to a VPN to view the forwarding path of the routers on the public network, you need to perform the following tasks:

1) Configure the **ttl propagate vpn** command on all the involved PEs.
2) Configure the **undo ttl expiration pop** command on the ASBR and SPE to guarantee ICMP responses to be forwarded along the original LSP.

2.3 LDP Configuration

Perform the following compulsory tasks in configuring LDP:

- Enable LDP
- Enable LDP on Interface

Perform the following optional tasks in configuring LDP:

- Configure LDP extended discovery mode
- Configure the label of the penultimate hop at the egress
- Configure session parameters
- Configure LDP loop detection control
- Configuring LDP authentication mode

2.3.1 Enabling/Disabling LDP

To configure LDP, first enable LDP.

Perform the following configurations in the system view.

Table 2-7 Enable/disable LDP view

Operation	Command
Enable LDP	**mpls ldp**
Disable LDP	**undo mpls ldp**

By default, LDP is disabled.

2.3.2 Enabling/Disabling LDP on Interface

To make the interface be of MPLS function, it is necessary to enable the LDP of interface in the interface view. Then the interface is capable of establishing LDP session and forwarding labeled packet.

Disabling LDP function will delete LDP peer, delete LSP tunnel, close TCP connection, interrupt peer LDP session, stop sending HELLO packets, and stop labeled packet forwarding.

Perform the following configurations in the interface view.

Table 2-8 Enable/disable LDP on interface

Operation	Command
Enable LDP function on interface	**mpls ldp enable**
Disable LDP function on interface	**mpls ldp disable**

By default, the interface MPLS function is disabled.

2.3.3 Configure LDP extended discovery mode

It is to create extended discovery mode, to set up sessions with peers not directly connected to the link.

I. Entering remote-peer mode

Perform the following configurations in the system view.

Table 2-9 Enter the extended discovery mode

Operation	Command
Enter the extended discovery mode	**mpls ldp remote-peer** *index*
Delete the corresponding remote-peer	**undo mpls ldp remote-peer** *index*

There is no default remote-peer.

II. Configuring a remote-peer address

You can specify the address of any LDP-enabled interface on the remote-peer or the address of the loopback interface on the LSR that has advertised the route as the address of the remote-peer.

Perform the following configurations in the remote-peer view.

Table 2-10 Configure a remote-peer address

Operation	Command
Configure the remote-peer address	**remote-ip** *ip-address*

There is no default remote-peer.

2.3.4 Configuring Session Parameters

I. Configuring session hold-time

The LDP entity on the interface sends Hello packets periodically to find out LDP peer, and the established sessions must also maintain their existence by periodic message (if there is no LDP message, then Keepalive message must be sent).

⚠ **Caution:**

Modifying the *holdtime* parameter may re-establish the original session, as well as the LSP over this session. Here the session refers to link session, but not remote session.

Perform the following configurations in the interface view.

Table 2-11 Set interface LDP session parameters

Operation	Command
Set interface LDP session keepalive parameters	**mpls ldp timer** { **session-hold** *session-holdtime* **|** **hello** *hello-holdtime* }
Restore the default interface LDP session parameters	**undo mpls ldp timer** { **session-hold | hello** }

The *session-holdtime* argument defaults to 60 seconds and the *hello-holdtime* argument defaults to 15 seconds.

Note:

For ATM, interface configuration commands are only available for the ATM subinterfaces in point-to-point mode.

For those link layer protocols that do not support broadcast packets, for example, frame relay and ATM, you must configure broadcast attributes, for transmission of broadcast and multi-cast packets.

II. Configuring hello transport-address

The transport-address discussed here refers to the address carried in the transport address field TLV in hello messages. Generally, transport-address is the MPLS LSR ID of the current LSR, but other configurations may be required in some applications.

Perform the following configurations in the interface view.

Table 2-12 Configure hello transport-address

Operation	Command
Configure a hello transport-address	**mpls ldp transport-ip** { **interface** | *ip-address* }
Restore the default hello transport-address	**undo mpls ldp transport-ip**

Transport-address defaults to the MPLS LSR ID of the current LSR.

When MPLS LDP is enabled on multiple directly connected links, these links must be configured with the same transport address. It is recommended that you take the default LSR-ID as the transport address; otherwise, the LDP session may not be well established.

2.3.5 LDP Loop Detection Control

I. Enabling loop detection

It is used to enable or disable the loop detection function during LDP signaling process. The loop detection includes maximum hop count mode and path vector mode.

In maximum hop count mode, hop count information is included in label binding information and is added by 1 when the packet passes through another hop. When the value exceeds the maximum, it is reckoned that loop appears, so LSP setup process terminates.

In path vector mode, path information is included in the label binding information. Each time the packet passes through a hop, the corresponding router will check whether its

ID is recorded in the path information. If not, the router just adds its ID. If yes, it means loop appears, so LSP setup process terminates.

Perform the following configurations in the system view.

Table 2-13 Enable loop detection

Operation	Command
Enable loop detection	**mpls ldp loop-detect**
Disable loop detection	**undo mpls ldp loop-detect**

By default, the loop detection is disabled.

II. Setting the maximum hop count for loop detection

When maximum hop count mode is adopted for loop detection, the maximum hop-count value can be defined. And if the maximum value is exceeded, it is considered that a loop happens and the LSP establishment fails.

Perform the following configurations in the system view.

Table 2-14 Set the maximum hop count for loop detection

Operation	Command
Set maximum hop count for loop detection	**mpls ldp hops-count** *hop-number*
Restore default maximum hop count	**undo mpls ldp hops-count**

The maximum hop count defaults to 32.

III. Setting the maximum value of the path vector

When path vector mode is adopted for loop detection, it is also necessary to specify the maximum value of LSP path. In this way, when one of the following conditions is met, it is considered that a loop happens and the LSP establishment fails.

1) The record of this LSR already exists in the path vector recording table.
2) The path hop count exceeds the maximum value set here.

Perform the following configurations in the system view.

Table 2-15 Set the maximum value of the path vector

Operation	Command
Set maximum value of the path vector	**mpls ldp path-vectors** *pv-number*
Remove maximum value setting for path vector	**undo mpls ldp path-vectors**

The maximum hop count defaults to 32.

2.3.6 Configuring LDP Authentication Mode

Perform the following configurations in the interface view or remote-peer view.

Table 2-16 Configure LDP authentication mode

Operation	Command
Configure LDP authentication mode	**mpls ldp password** { **cipher** | **simple** } *password*
Remove LDP authentication	**undo mpls ldp password**

2.3.7 Configuring the Type of Label to Be Distributed to the Penultimate Hop

This command is used at the egress to specify the type of the label to be distributed to the penultimate hop.

Perform the following configurations in MPLS view.

Table 2-17 Configure the type of the label to be distributed to the penultimate hop

Operation	Command
Specify at the egress the type of the label to be distributed to the penultimate hop	**mpls label advertise** { **implicit-null** | **explicit-null** | **non-null** }
Restore the default setting	**undo mpls label advertise** { **implicit-null** | **explicit-null** | **non-null** }

explicit-null: Specifies at egress to distribute an explicit null label to the penultimate hop.

implicit-null: Specifies at egress to distribute an implicit null label to the penultimate hop.

non-null: Specifies at egress to distribute a normal label to the penultimate hop.

If the explicit null label is assigned to the penultimate hop, it can only reside at the bottom of the label stack.

The label type defaults to implicit null label.

2.4 MPLS Display and Debug

2.4.1 Displaying and Debugging MPLS

MPLS provides abundant display and debugging commands for monitoring LDP session state, tunnel, all the LSPs and their states, and so on. These commands are the powerful debugging and diagnosing tools.

I. Displaying static LSPs

After accomplishing the configuration tasks mentioned earlier, you can execute the **display** command in any view to view the running state of a single or all the static LSPs and thus to evaluate the effect of the configurations.

Table 2-18 Display the static LSP information

Operation	Command
Display the static LSP information	**display mpls static-lsp** [**verbose**] [**include** *text*]

II. Displaying the MPLS statistics

Execute the **display** command in any view or the reset command in user view to view or clear statistics about the specified or all static LSPs.

Table 2-19 Display/clear the MPLS statistics

Operation	Command
Display the MPLS statistics	**display mpls statistics** { **interface** { **all** | *interface-type interface-number* } } | { **lsp** [*lsp-Index* | **all** | **name** *lsp-name*] } }
Clear the MPLS statistics	**reset mpls statistics** { { **interface** { **all** | *interface-type interface-num* } } | { **lsp** *lsp-name* } }

III. Displaying MPLS-enabled interfaces

After accomplishing the configuration tasks mentioned earlier, you can execute the **display** command in any view to view the information related to the MPLS-enabled interfaces and thus to evaluate the effect of the configurations.

Table 2-20 Display information of the MPLS-enabled interfaces

Operation	Command
Display information of the MPLS-enabled interfaces	**display mpls interface**

IV. Display LSP

Please execute the following commands in any view to display the information related to MPLS LSP.

Table 2-21 Display MPLS LSP

Operation	Command
Display the information related to MPLS LS	**display mpls lsp** [**verbose**] [**include** *text*]

V. Debugging MPLS

You may execute the **debugging** command in user view to debug the information concerning all interfaces with MPLS function enabled.

As enabling debugging may affect the router performance, you are recommended to use this command unless necessary. Execute the **undo** form of this command to disable the corresponding debugging.

Table 2-22 Debug MPLS

Operation	Command
Enable debugging on various MPLS LSP information.	**debugging mpls lspm** { **all** | **packet** | **event** | **process** | **agent** | **interface** | **policy** | **vpn** }
Disable MPLS LSP debugging.	**undo debugging mpls lspm** { **all** | **packet** | **event** | **process** | **agent** | **interface** | **policy** | **vpn** }

VI. Trapping MPLS

This command is used to enable the trap function of MPLS during an LSP/LDP setup process.

Perform the following configuration in system view.

Table 2-23 Enable the trap function of MPLS

Operation	Command
Enable the ldp trap function of MPLS	**snmp-agent trap enable ldp**
Disable the ldp trap function of MPLS	**undo snmp-agent trap enable ldp**
Enable the lsp trap function of MPLS	**snmp-agent trap enable lsp**
Disable the lsp trap function of MPLS	**undo snmp-agent trap enable lsp**

2.4.2 Displaying and Debugging LDP

I. LDP display commands

V 2.41 provides abundant MPLS monitoring commands for monitoring states of LSRs, LDP sessions, interfaces and peers. These commands are the powerful debugging and diagnosing tools.

After accomplishing the configuration tasks described earlier, you can execute the **display** command in any view to view the running state of LDP and thus to evaluate the effect of the configurations.

Table 2-24 LDP monitoring commands

Operation	Command
Display LDP information	**display mpls ldp**
Display buffer information for LDP	**display mpls ldp buffer-info**
Display LDP interface information	**display mpls ldp interface**
Display LDP label information	**display mpls ldp lsp**
Display LDP session peer information	**display mpls ldp peer**
Display information of the remote-peers in the LDP sessions	**display mpls ldp remote**
Display states and parameters of LDP sessions	**display mpls ldp session**

II. Debugging commands

Execute **debugging** command in user view for the debugging of various messages related to LDP

Table 2-25 Debug MPLS

Operation	Command
Enable MPLS debugging	**debugging mpls ldp** { { **all** | **main** | **advertisement** | **session** | **pdu** | **notification** } [**interface** *interface-type interface-number*] | **remote** }
Disable MPLS debugging.	**undo debugging mpls ldp** { { **all** | **main** | **advertisement** | **session** | **pdu** | **notification** | **remote** } [**interface** *interface-type interface-number*] | **remote** }

all: Displays all LDP-related debugging information

main: Displays debugging information about LDP main tasks

advertisement: Displays debugging information in processing LDP advertisements

session: Displays debugging information in processing LDP session

pdu: Displays debugging information in processing PDU packets

notification: Displays debugging information in processing notifications

remote: Displays debugging information about all remote peers

2.5 MPLS Configuration Example

I. Network requirements

As shown in Figure 2-1, there is a network consisting of four 3Com router routers, among which Router B and Router C are connected via SDH, and Router B, Router A and Router D are interconnected via Ethernet.

The four routers all support MPLS, and LSP can be established between any two routers with the routing protocol OSPF.

II. Network diagram

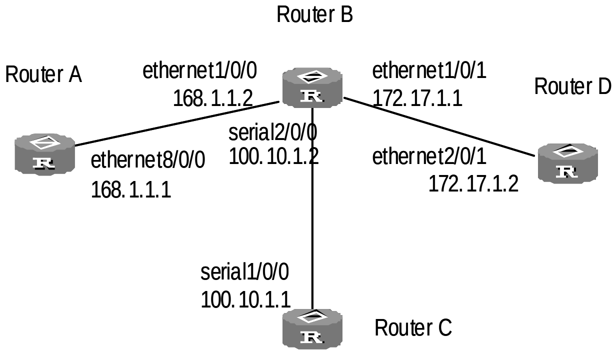


Figure 2-1 Network diagram

III. Configuration procedure

1) Configuration on Router A:

# Configure LSR ID and enable MPLS and LDP.

```
[3Com] mpls lsr-id 168.1.1.1
[3Com] mpls
[3Com] mpls ldp
```

# Configure IP address and enable LDP for Ethernet interface.

```
[3Com] interface ethernet 8/0/0
[3Com-Ethernet8/0/0] ip address 168.1.1.1 255.255.0.0
[3Com-Ethernet8/0/0] mpls ldp enable
```

# Enable OSPF on the interfaces connecting Router A and Router B

```
[3Com] route id 168.1.1.1
[3Com] ospf
```

```
[3Com-ospf] area 0
[3Com-ospf-area-0.0.0.0] network 168.1.0.0 0.0.255.255
```

2) Configuration on Router B:

# Configure LSR ID and enable MPLS and LDP.

```
[3Com] mpls lsr-id 172.17.1.1
[3Com] mpls
[3Com] mpls ldp
```

# Configure IP address and enable LDP for Ethernet interface 1/0/0.

```
[3Com] interface ethernet 1/0/0
[3Com-Ethernet1/0/0] mpls ldp enable
[3Com-Ethernet1/0/0] exit
```

# Configure Ethernet interface 1/0/1 and enable LDP on it.

```
[3Com] interface ethernet 1/0/1
[3Com-Ethernet1/0/1] ip address 172.17.1.1 255.255.0.0
[3Com-Ethernet1/0/1] mpls ldp enable
```

# Configure SERIAL interface 2/0/2 and enable LDP on it.

```
[3Com] interface serial 2/0/0
[3Com-Serial2/0/2] ip address 100.10.1.2 255.255.255.0
[3Com-Serial2/0/2] mpls ldp enable
[3Com-Serial2/0/2] quit
```

# Enable OSPF on the interfaces connecting Router B to Router A, Router D and Router C.

```
[3Com] route id 172.17.1.1
[3Com] ospf
[3Com-ospf] area 0
[3Com-ospf-area-0.0.0.0] network 168.1.0.0 0.0.255.255
[3Com-ospf-area-0.0.0.0] network 172.17.0.0 0.0.255.255
[3Com-ospf-area-0.0.0.0] network 100.10.1.0 0.0.0.255
[3Com-ospf-1-area-0.0.0.0] quit
```

3) Configuration on Router C:

# Configure a loopback interface.

```
[3Com] interface LoopBack0
[3Com-LoopBack0] ip address 172.16.1.2 255.255.255.255
[3Com-LoopBack0] quit
```

# Configure OSPF.

```
[3Com] ospf
[3Com-ospf-1] area 0
[3Com-ospf-1-area-0.0.0.0] network 172.16.1.2  0.0.0.0
```

# Configure LSR ID and enable MPLS and LDP.

```
[3Com] mpls lsr-id 172.16.1.2
[3Com] mpls
[3Com] mpls ldp
```

# Configure IP address and enable LDP on SERIAL interface 1/0/0.

```
[3Com] interface serial 1/0/0
[3Com-Serial1/0/0] ip address 100.10.1.1 255.255.255.0
[3Com-Serial1/0/0] mpls ldp enable
[3Com-Serial1/0/0] quit
```

# Configure OSPF on the interfaces connecting Router C and Router B.

```
[3Com] route id 172.16.1.2
[3Com] ospf
[3Com-ospf] area 0
[3Com-ospf-area-0.0.0.0] network 100.10.1.0 0.0.0.255
```

4) Configuration on Router D:

```
[3Com] interface ethernet 2/0/1
[3Com-Ethernet2/0/1] ip address 172.17.1.2 255.255.0.0
```

# Configure LSR ID and enable MPLS and LDP.

```
[3Com] mpls lsr-id 172.17.1.2
[3Com] mpls
[3Com] mpls ldp
```

# Configure IP address and enable LDP on Ethernet interface 2/0/1.

```
[3Com] interface ethernet 2/0/1
[3Com-Ethernet2/0/1] ip address 172.17.1.2 255.255.0.0
[3Com-Ethernet2/0/1] mpls ldp enable
```

# Configure OSPF on the interfaces connecting Router D and Router B.

```
[3Com] route id 172.17.1.2
[3Com] ospf
[3Com-ospf] area 0
[3Com-ospf-area-0.0.0.0] network 172.17.0.0 0.0.255.255
```

2.6 Troubleshooting MPLS Configuration

Symptom: Session links cannot be setup with the peer after LDP is enabled on the interface.

Troubleshooting:

Cause 1: Loop detection configuration is different at both ends.

Measure: Check loop detection configuration at both end to see if one end is configured while the other end is not.

Cause 2: Local machine cannot get the route to peer LSR ID, so TCP connection cannot be set up.

Measure: The default address for session transfer is MPLS LSR ID. The local machine should issue the LSR ID route (often the loopback address) and learn the peer LSR ID route.

Chapter 3 BGP/MPLS VPN Configuration

3.1 BGP/MPLS VPN Overview

Traditional VPN, for which layer 2 tunneling protocol (L2TP, L2F and PPTP, etc.) or layer 3 tunnel technology (IPSec, GRE and etc.) is adopted, is a great success in such aspects as solving network security and flexibility and is widely used. However, as the connecting domain extends, the deficiency of traditional VPN on such aspects as expansibility and manageability becomes more and more obvious. In addition, QoS (Quality of Service) and security are also the difficult problem for traditional VPN.

MPLS (Multiprotocol Label Switching) technology is fit for VPN networking. With MPLS network, the IP-based VPN service can be realized easily, thus the requirements for the expansibility and manageability of VPN are satisfied. In addition, security precautions can be adopted on MPLS VPN to ensure that no IP connection can be established between different VPNs and thus VPN security is guaranteed. The VPN constructed by using MPLS also provides the possibility for the implementation of value-added service. Multiple VPNs can be formed from a single access point, and each VPN represents a different service, making the network able to transmit services of different types in a flexible way.

V 2.41 provides comparatively complete BGP/MPLS VPN networking capabilities:

- Address separation. Allow the address overlapping of the different VPN or between VPN and public network.
- Supporting MP-BGP advertising VPN routing message, establishing BGP/MPLS VPN.
- Forwarding VPN data stream over MPLS LSP.
- 3Com router provides MPLS VPN performance monitoring and fault detecting tools.

3.1.1 BGP/MPLS VPN Model

I. BGP/MPLS VPN model

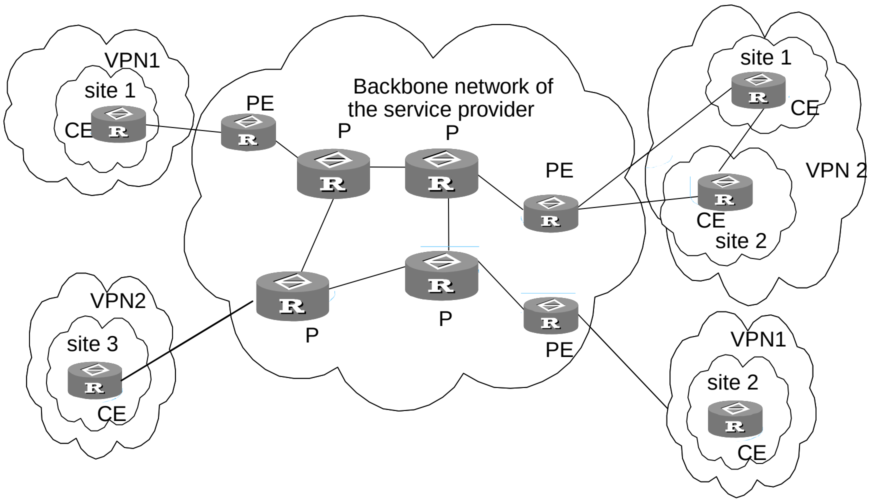


Figure 3-1 MPLS VPN model

As shown in Figure 3-1, MPLS VPN model contains three parts: CE, PE and P.

- CE (Customer Edge) device: It is a composing part of the customer network, which is usually connected with the service provider directly via an interface. It is commonly a router. CE cannot “sense” the existence of VPN.
- PE (Provider Edge) router: It is the Provider Edge router, namely the edge device of the provider network, which is connected with the customer’s CE directly. In MPLS network, PE router disposes all the processing for VPN.
- P (Provider) router: It is the backbone router in the provider network, which is not connected with CE directly. P router needs to possess MPLS basic forwarding capability.

The classification of CE and PE mainly depends on the range for the management of the provider and the customer, and CE and PE are the edges of the management domains.

II. Basic concepts in BGP/MPLS VPN

1) vpn-instance

vpn-instance is an important concept in VPN routing in MPLS. In actual network, each site on PE corresponds to a single vpn-instance (their association is implemented via interface binding). If subscribers on one site belong to multiple VPNs, then the corresponding vpn-instance should include information about all these VPNs.

Specifically, such information should be included in vpn-instance: label forwarding table, IP routing table, the interfaces bound with vpn-instance, and the management information (RD, route filtering policy, member interface list, etc). It includes the VPN membership and routing rules of this site.

PE is responsible for updating and maintaining the correlation between vpn-instance and VPN. To avoid data leakage from the VPN and illegal data entering into the VPN, each vpn-instance on the PE has an independent set of routing table and label forwarding table, in which the forwarding information of the message is saved

2) MP-BGP

MP-BGP (multiprotocol extensions for BGP-4, see RFC2283) propagates VPN membership information and routes between PE routers. It features backward compatibility: It not only supports conventional IPv4 address family, but also supports other address families, for example, VPN-IPv4 address family. MP-BGP ensures that VPN private routes are only advertised within VPNs, as well as implementing communication between MPLS VPN members.

3) VPN-IPv4 address family

VPN is just a private network, so it can use the same IP address to indicate different sites. But the IP address is supposed as unique when MP-BGP advertises CE routes between PE routers, so routing errors may occur for the different meaning in two systems. The solution is to switch IPv4 addresses to VPN-IPv4 address family to generate a globally unique address before advertising them, so PE routers is required to support MP-BGP.

A VPN-IPv4 address consists of 12 bytes, and the first eight bytes represent the RD (Route Distinguisher), which are followed by a 4-byte IPv4 address. The service providers can distribute RD independently. However, their special AS (Autonomous System) number must be taken as a part of the RD to ensure that each RD is globally unique. The VPN-IPv4 address with the RD of zero is synonymous with the IPv4 address that is globally unique. After being processed in this way, even if the 4-byte IPv4 address contained in VPN-IPv4 address has been overlapped, the VPN-IPv4 address can still maintain globally unique. RD is only used within the carrier network to differentiate routes. When the RD is 0, a VPN-IPv4 address is just a IPv4 address in general sense.

The route received by PE from CE is the IPv4 route that needs to be redistributed into vpn-instance routing table, and in this case a RD needs to be added. It is recommended that the same RD be configured for the same VPN.

III. VPN Target attribute

VPN Target attribute is one of the MP-BGP extension community attributes and is used to limit VPN routing information advertisement. It identifies the set of sites that can use some route, namely by which Sites this route can be received, and the PE router can receive the route transmitted by which Sites. The PE routers connected with the Site specified in VPN Target can all receive the routes with this attribute. After PE router has received the route with this attribute, it will add the route into the corresponding routing table.

For PE routers, there are two sets of VPN Target attributes: one of them, referred to as Export Targets, is added to the route received from a directly connected Site in advertising local routes to remote PE routers. And the other one, known as Import Targets, is used to decide which routes can be redistributed into the routing table of this Site in receiving routings from remote PE routers.

In matching the VPN Target attribute carried by the route, if there are identical items in the export VPN target set and import VPN target set, the route is redistributed into the VPN routing table and then advertised to the CE connected. Otherwise, the route is rejected.

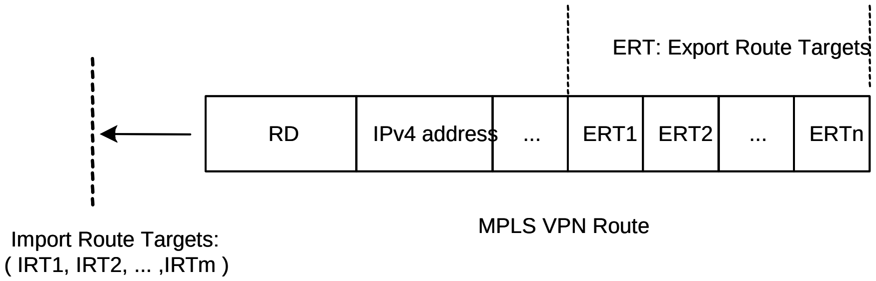


Figure 3-2 Route filtering via matching VPN Target attribute

📖 **Note:**

The routes for other VPNs will not appear in the routing table of the VPN in question using VPN Target attribute to filter routing information received at PE router, so the CE-transmitted data will only be forwarded within the VPN.

3.1.2 BGP/MPLS VPN Implementation

BGP/MPLS VPN works on this principle: It uses BGP to propagate VPN private routing information on carrier backbone network and MPLS to forward VPN service traffic.

I. Advertising VPN routing information via BGP

1) Routing information exchange between CE and PE

A PE router can learn routing information about the CE connected to it through static route, RIP (supporting multi-instance), OSPF (supporting multi-instance) or EBGP, and redistributes it into a vpn-instance.

2) Routing information exchange between ingress PE and egress PE

The ingress PE router uses MP-BGP to advertise routing information learned from CE to the egress PE router (with MPLS label) and learn the CE routing information learned at the egress PE router.

The internal connectivity among all the PEs is ensured via IGP (for example, RIP and OSPF), so IGP should run at all interconnection interfaces and loopback interfaces.

3) LSP setup between PEs

LSPs should be set up between PEs for VPN data traffic forwarding with MPLS LSP. The PE router that receives packets from CE and create label protocol stack is called ingress LSR, while the BGP next hop (egress PE router) is egress LSR.

4) Routing information exchange between PE and CE

A CE can learn remote VPN routes from the PE connected through static routes, RIP, OSPF or EBGP.

With above-mentioned steps, reachable routes can be established between CEs, for transmission of VPN private routing information over public network.

II. Forwarding VPN packets

VPN packets are forwarded by adopting two-layer label mode:

Interior-layer label, also called MPLS label, is at the bottom in label stack and distributed when the egress PE advertises routing information (in VPN forwarding table) to ingress GE. When VPN packets from public network reach the CE, they can be forwarded from the designated interface to the designated CE or site by searching for the target MPLS forwarding table according to the labels contained.

Exterior-layer label, known as LSP initialization label, is at the top in label stack and indicates an LSP from the ingress PE to egress PE. By switching exterior-layer label, VPN packets can be forwarded along the LSP to the peer PE.

Figure 3-3 illustrates the details:

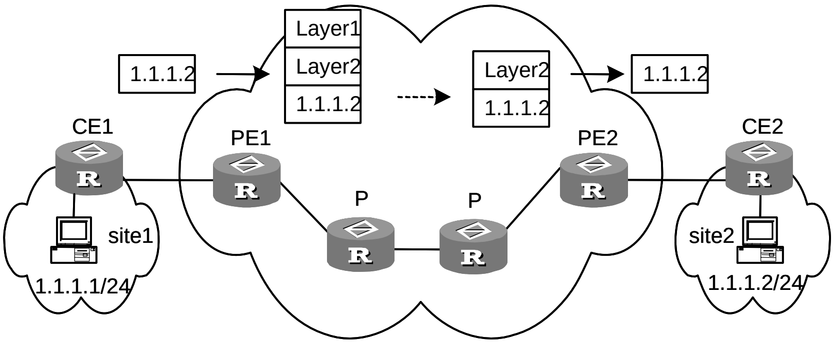


Figure 3-3 VPN packet forwarding

1) Site 1 sends an IPv4 packet with destination address 1.1.1.2 to CE1. CE1 looks routing information up in the IP routing table and sends the packet to PE1.
2) PE1 looks up in the VPN-instance table according to the destination interface and destination address to get MPLS label (or interior-layer label), LSP initialization label (or exterior-layer label), BGP next hop (PE2), egress interface etc. When the label stack is established, PE1 forwards via the egress interface the MPLS packet to the first P on the LSP.
3) Every P router on the LSP forwards the MPLS packet according to the exterior-layer label until the packet reaches the penultimate router, i.e. the P router right before the PE2, which extracts the exterior-layer label and forwards the packet to PE2.
4) PE2 looks up in the MPLS forwarding table according to the interior-layer label and destination address to determine the egress interface for labeling operation and the packet. It then extracts the interior-layer label and forwards through the egress interface the IPv4 packet to CE2.
5) CE2 looks up in the routing table and sends the packet in normal IPv4 packet forwarding mode to the site2.

3.1.3 HoVPN

I. HoVPN Introduction

1) Hierarchical model and plane model

In BGP/MPLS VPN solutions the key devices, PEs, function in two aspects:

- Providing access functions for users. PEs need a large number of interfaces.
- Managing and advertising VPN routes, and processing user packets. PEs need large-capacity memory and high forwarding capability.

Hierarchical architectures are mostly used in the current network schemes. For example, the WAN architecture model contains three layers, namely, core layer, convergence layer and access layer. The core layer requires the devices with the highest performance among the three layers, while its network scale is the least.

However, BGP/MPLS VPN is a plane model, which requires the same performance on all the PEs. If some PEs are limited in extending performance, all the network will be influenced.

Because the plane model of BGP/MPLS VPN does not accord with the typical hierarchical model, the scalability problem occurs in PE deployment at each layer. So the plane model is not applicable to the large-scale VPN deployment.

2) HoVPN

To solve this problem, BGP/MPLS VPN needs to become the hierarchical model from the plane model.

In MPLS L3VPN area, Huawei Technologies proposed the solution of hierarchy of VPN (HoVPN). In HoVPN, functions of PE are distributed to multiple devices. Acting as different roles in a hierarchical architecture, the devices fulfill functions of a centralized PE together.

It is required that the devices in the upper hierarchy possess higher routing and forwarding performance, while those in the lower hierarchy with lower performance, which is similar to the typical network model.

II. HoVPN Implementation

1) Basic architecture of HoVPN

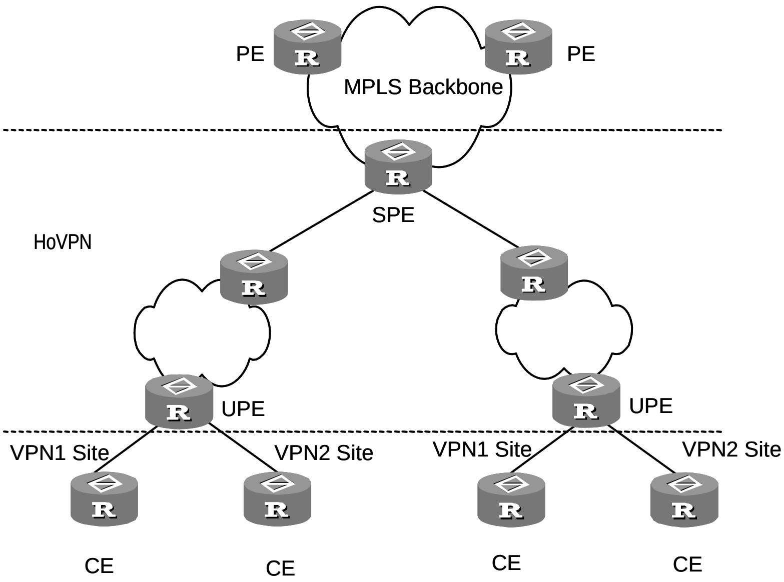


Figure 3-4 Basic architecture of HoVPN

As shown in Figure 3-4, the device directly connected with users is called underlayer PE or User-end PE, shortened as UPE. The device connected with UPE in the internal network is called superstratum PE or Service Provider-end PE, shortened as SPE.

Multiple UPEs and SPEs compose the hierarchical PE, functioning together as a traditional PE.

Note:

In the networking of HoVPN, functions of PE are implemented hierarchically. So the solution is also called hiberarchy of VPN or HoPE.

The UPE and SPE play different roles:

- The UPE implements the user access. It maintains the routes of VPN Site directly connected with it. It does not maintain the routes of other remote Sites in VPN, or only maintains their summary routes. The UPE assigns interior layer label to the routes in its directly connected Site, and advertises the label to the SPE with VPN routes through MP-BGP.
- The SPE manages and advertises VPN routes. It maintains all the routes in the VPN where its connected Site locates, including the routes in local and remote Sites. The SPE does not advertise routes in remote Sites to UPE. It only advertises the default route of VPN-instance or summary route to UPE with the label.

Different roles result in different requirements for the SPE and UPE:

- SPE: large capacity of routing table, high forwarding performance, few interface resources
- UPE: small capacity of routing table, low forwarding performance, high access capability

The HoVPN takes advantage of the performance of SPEs and access capability of UPEs.

It should be noted that the SPE and UPE are relative. In the hierarchical architecture, the superstratum PE is SPE for the underlayer, and the Underlayer PE is UPE for the superstratum.

The HoPE is the same as the traditional PE in appearance. It can exist together with common PEs in an MPLS network.

2) SPE–UPE

The MP-BGP running between SPE and UPE can be either MP-IBGP or MP-EBGP. This depends on whether UPE and SPE belong to the same AS.

When MP-IBGP is used, SPE acts as the route reflector in order to advertise routes between IBGP peers. It advertises the VPN routes from the IBGP peer UPE to the peer SPE, but it does not act as the route reflector of other PEs.

3) Embedment and extension of HoVPN

HoVPN supports the embedment of HoPE:

- An HoPE can act as a UPE, and compose a new HoPE with another SPE.
- An HoPE can act as the SPE, and compose a new HoPE with multiple UPEs.
- Multiple embedment processes can be supported.

The embedment of HoPE can infinitely extend a VPN network in theory.

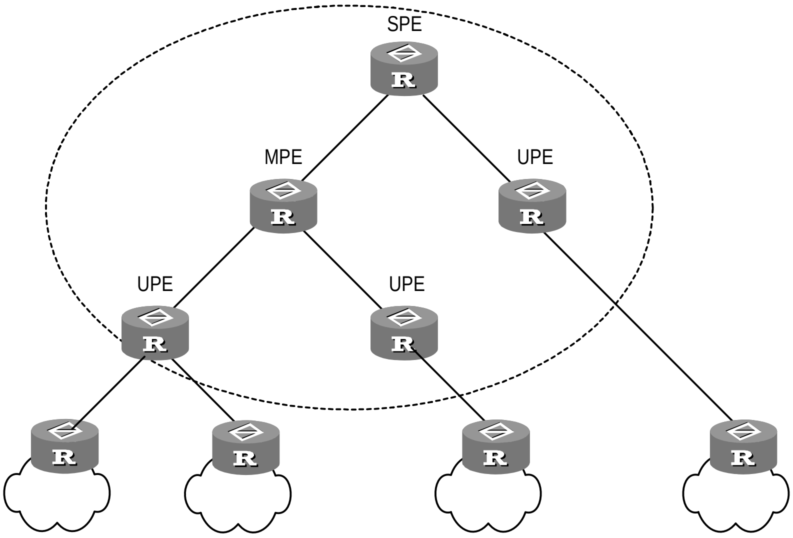


Figure 3-5 Embedment of HoVPN

As shown in Figure 3-5, the PE in the middle is called Middle-level PE (MPE) in a three-level HoPE. MP-BGP runs between SPE, MPE, and UPE.

Note:

The MPE does not really exit in an HoVPN model. It is used here just for the convenience of description.

MP-BGP advertises all the VPN routes of Underlayer PEs for Superstratum PEs, but only advertises the default routes of VPN-instance of Superstratum PEs for Underlayer PEs.

The SPE maintains VPN routes of all Sites in the HoVPN, while UPE only maintains VPN routes of its directly connected Sites. The number of routes maintained by the MPE is between the above two.

3.1.4 Introduction to Multi-Role Host Features

As the VPN attribute of a packet that enters PE from CE is determined by the VPN bound with the incoming interface, it in essence determines that all the CEs that obtain the forwarding service of PE via the same incoming interface must belong to the same VPN. In the actual networking environments, however, there is the need for a CE to access multiple VPNs via the same physical interface. Such a requirement can be satisfied by setting different logical interfaces, but such a stopgap solution will increase the extra configuration works and have great limit in application. In the process of solving this problem, the concept of multi-role host was introduced. It distinguishes the VPNs that the packets will access by configuring policy routing based on IP address. As for the PE-CE downstream traffic, this function is implemented via static routing. The static routing in a multi-role host application is different from the regular static routes in the sense that it enables a logical interface to access multiple VPNs by making use of the static route on a VPN to specify an interface in some other VPN as the outgoing interface.

3.1.5 OSPF VPN Extension

I. OSPF multi-instance

As one of the most popular IGP routing protocols, OSPF is used as internal routing protocol in many VPNs. If OSPF is also used on PE-CE links, then CE routers only need to support OSPF protocol. If you want to transform conventional OSPF backbone into BGP/MPLS VPN, the OSPF can simplify this process.

When OSPF is used as PE-CE routing protocol in BGP/MPLS VPN application,, PE must support OSPF multi-instance, one OSPF instance corresponds to one VPN instance. It owns its own interface, routing table and sends VPN routing information over MPLS network using BGP/OSPF interaction.

The following involves details about the OSPF configuration between PE and CE.

1) OSPF domain configuration between PE and CE

The OSPF domain between PE and CE can be a non-backbone area or a backbone area.

In the application of OSPF VPN extension, the MPLS VPN backbone network is considered as the backbone area (area 0). All the areas should be connected with the backbone area in OSPF, so area 0 of all the VPN nodes must be connected with the MPLS VPN backbone network.

That is, if a VPN node involves OSPF domain 0, the PE connected to CE must connect with the backbone area of the VPN node through area 0 (The virtual link can be used for logical connection).

2) BGP/OSPF interaction

After OSPF runs between PE and CE, PE advertises VPN routes to other PEs through BGP and to CEs through OSPF.

As shown in Figure 3-6, PE1 connects to PE2 through the MPLS backbone network. CE11, CE21, and CE22 belong to VPN1. Suppose all the routers in the figure belong to the same AS, that is, CE11, CE21, and CE22 belong to the same OSPF area.

The advertisement procedure of VPN1 routes is as follows:

- BGP redistributes OSPF routes of CE11 on PE1.
- BGP advertises the VPN routes to PE2.
- OSPF redistributes BGP VPN routes on PE2, and advertises them to CE21 and CE22.

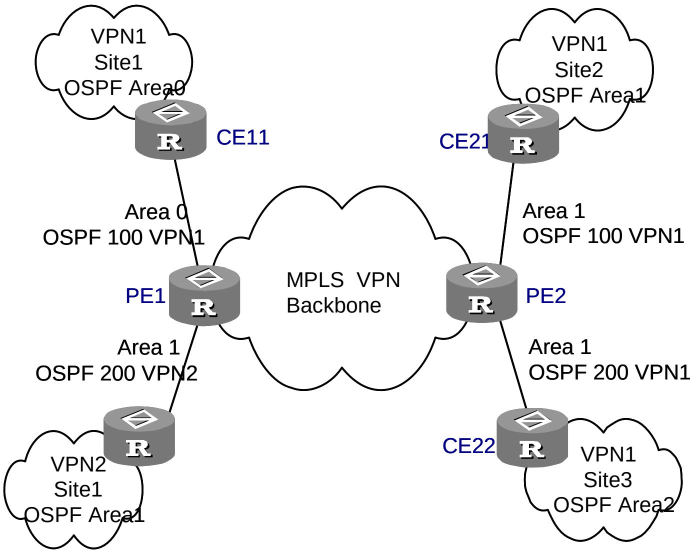


Figure 3-6 Application of OSPF in VPN

The standard BGP/OSPF interaction enables PE2 to advertise the BGP VPN routes to CE21 and CE22 through Type5 LSAs (ASE LSAs). However, CE11, CE21, and CE22 belong to the same OSPF area, and the route advertisement between them depends on Type3 LSAs (inter-domain routes).

To avoid the above cases, the PE applies a modified BGP/OSPF interaction process (shorted as BGP/OSPF interoperability). It can advertise the routes from a Site to another, and differentiate the routes from real AS-External routes. The process requires the extension community attribute of BGP and the information identifying OSPF attributes.

The V 2.41 requires that each OSPF domain have a Domain ID. It is recommended to configure a same Domain ID for all OSPF instances in the network related to each VPN instance, or adopt the default ID 0. In this case, all the VPN routes with the same Domain ID come from the same VPN instance.

3) Routing loop detection

Suppose PE connects to CE through the OSPF backbone area, and a VPN Site connects to multiple PEs. When a PE advertises BGP VPN routes learnt from MPLS/BGP to a VPN Site through LSAs, the LSAs may possibly be received by another PE, thus resulting in the routing loop.

To avoid the routing loop, the PE sets the flag bit DN for BGP VPN routes learnt from MPLS/BGP when originating Type3 LSAs, regardless of whether PE connects to CE through the OSPF backbone area. The PE ignores the Type3 LSAs for DN settings during the route calculation of OSPF process.

To advertise a route from another OSPF domain to CE, the PE should claim an ASBR and advertise the route as Type5 LSA. The VPN Route Tag configured for an OSPF instance is contained in Type5 or Type7 LSAs. The PE ignores the Type5 or Type7 LSA if the contained tag value is the same as that configured on PE during the route calculation of OSPF process.

II. Multi-VPN-Instance CE

If supporting OSPF multi-instance, one router can run multiple OSPF procedures, which can be bound to different VPN instances. In practice, you can create one OSPF instance for each service type. OSPF multi-instance can fully isolate different services in transmission, which can solve security problems with low cost. OSPF multi-instance runs on PE router, which is called multi-VPN-instance CE. Currently, different services in a LAN are often isolated with the VLAN function of a switch, but OSPF multi-instance provides a solution for service isolation on routers.

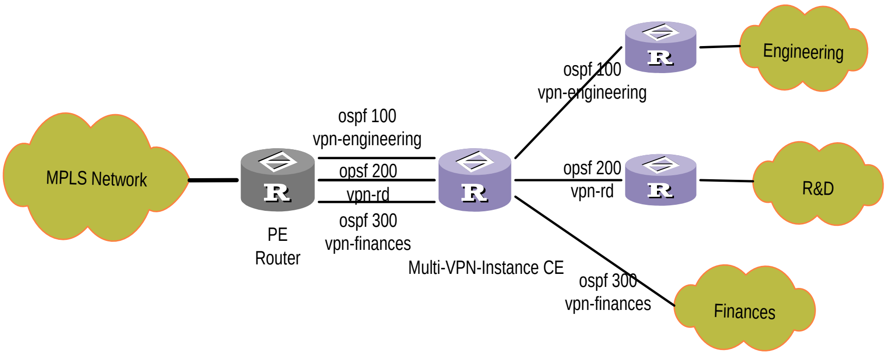


Figure 3-7 Multi-VPN-instance CE application in conventional LAN

III. Sham Link

As shown in Figure 3-8,, two Sites in a same OSPF domain connect to PE1 and PE2. There is an OSPF link inside the area (called backdoor link) between the two Sites. The two Sides belong to a same VPN. In this case, the route connecting the two Sites through PEs is called the Inter-Area Route. It is not selected as the optimal route by OSPF because its preference is lower than that of the Intra-Area Route across the backdoor link.

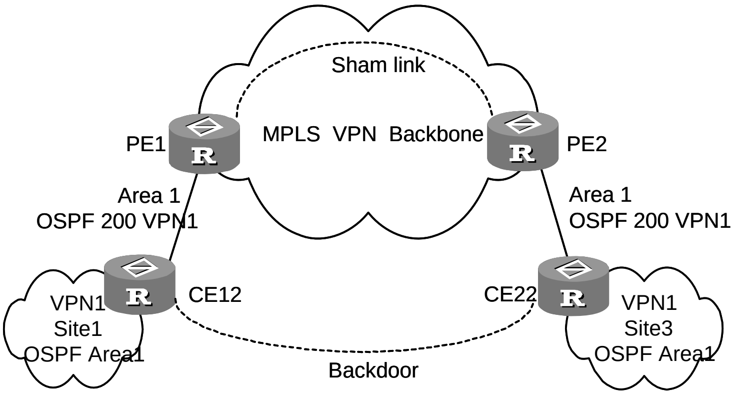


Figure 3-8 Sham link application

In some cases, the routes across the MPLS VPN backbone network need to be firstly selected. You can establish a sham link between PEs to make the routes become the Intra-Area Routes.

The sham link acts as an unnumbered point-to-point link inside the area and is advertised using Type1 LSA. You can select a route between the sham link and backdoor link by adjusting the metric.

The sham link is considered the link between two VPN instances with one endpoint address in each VPN instance. The address is a Loopback interface address with a 32-bit mask in the VPN address space on the PE. The same OSPF process can share endpoint addresses between sham links, while different OSPF processes cannot.

The BGP advertises the endpoint addresses of sham links as VPN-IPv4 addresses. A route across the sham link cannot be redistributed into BGP as a VPN-IPv4 route.

The sham link can be configured in any area. You need to configure it manually in V 2.41. In addition, the local VPN instance must contain a route to the destination of sham link.

3.1.6 Multi-AS BGP/MPLS VPN

In some networking scenarios, a user’s multiple sites belong to the same VPN may connect to multiple ISPs that use different ASs or connect to multiple ASs of an ISP. Such application is called Multi-AS BGP/MPLS VPN.

RFC 2547bis presents three multi-AS VPN solutions, which are:

- VPN-INSTANCE-to-VPN-INSTANCE: ASBRs manage VPN routes in between by using subinterfaces, which is also called Inter-Provider Backbones Option A.
- EBGP Redistribution of labeled VPN-IPv4 routes: ASBRs advertise labeled VPN-IPv4 routes to each other through MP-EBGP, which is also called Inter-Provider Backbones Option B.
- Multihop EBGP redistribution of labeled VPN-IPv4 routes: PEs advertise labeled VPN-IPv4 routes to each other through Multihop MP-EBGP, which is also called Inter-Provider Backbones Option C.

The V 2.41 supports the above three solutions.

I. Managing VPN Routes Between ASBRs by Using Subinterfaces

PEs, acting as ASBRs in two ASs, are directly connected.

ASBR PEs connect to each other through multiple subinterfaces. Considering each other as their CE, the ASBR PEs advertise IPv4 routes to the peer using traditional EBGP. Each subinterface is associated with a VPN. You need to bind the subinterfaces on the ASBR to their corresponding VPN-instances but do not need to enable MPLS on them. Within an AS, packets are forwarded as VPN packets using two-tier labels; between ASBRs, they are forwarded using IP routing.

Ideally, each multi-AS VPN has a pair of subinterfaces for exchanging VPN routing information.

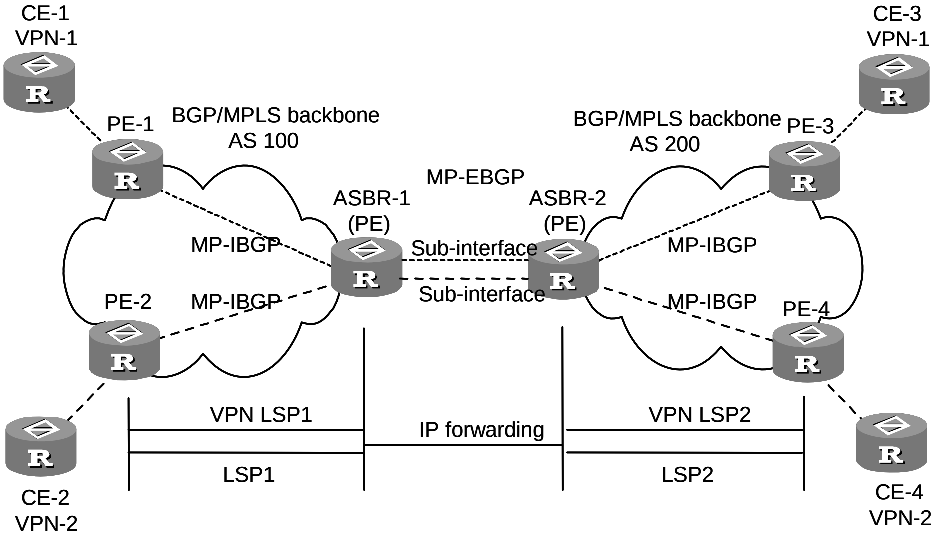


Figure 3-9 Network diagram for managing VPN routes between ASBRs by using subinterfaces

This method is easily to implement. No special configuration is required on the ASBRs.

However, it has weak extensibility. Because ASBR PEs need to manage all VPN routes and create VPN instances on a per-VPN basis. This will lead to excessive VPN-IPv4 routes on PEs, and poses high performance requirements for the PEs.

II. Advertising Labeled VPN-IPv4 Routes Through MP-EBGP Between ASBRs

Two ASBRs, through MP-EBGP, exchange labeled VPN-IPv4 routes that they obtain from respective AS PEs.

The routes are advertised following the procedures below:

1) PEs in AS 100 advertise labeled VPN-IPv4 routes to ASBR PE of AS 100 or the Route Reflector (RR) of ASBR PE through MP-IBGP.
2) ASBR PE advertises labeled VPN-IPv4 routes to ASBR PE of AS 200 through MP-EBGP.
3) ASBR PE of AS 200 advertises labeled VPN-IPv4 routes to PEs in AS 200 or the RR of ASBR PE through MP-IBGP.

In this way, special processing is needed for labeled VPN-IPv4 routes on ASBRs. So it is also called ASBR extension method.

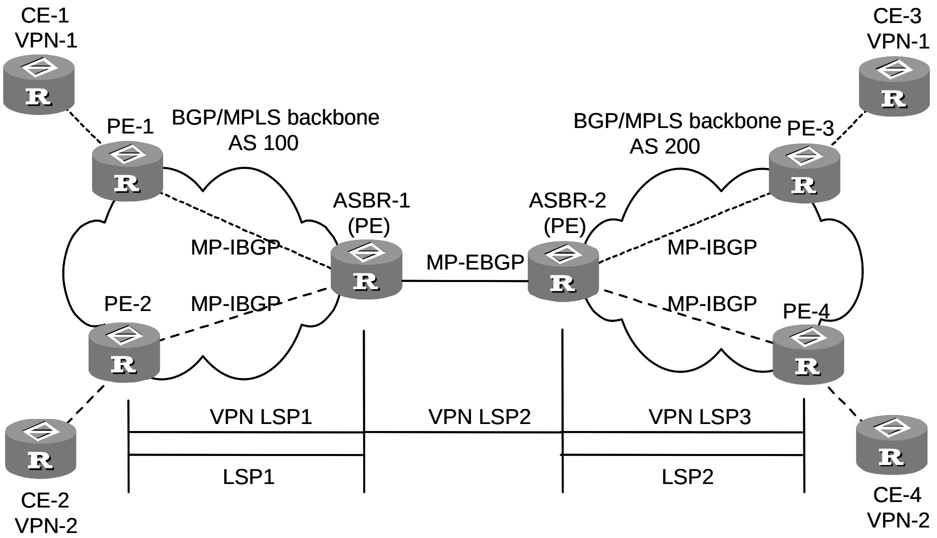


Figure 3-10 Network diagram for advertising labeled VPN-IPv4 routes through MP-EBGP between ASBRs

In terms of extensibility, advertising labeled VPN-IPv4 routes through MP-EBGP is prior to managing VPN between ASBRs through subinterfaces.

When adopting MP-EBGP method, note that:

- ASBRs perform no VPN-Target filtering on VPN-IPv4 routes that they receive from each other. So the ISPs in different ASs that exchange VPN-IPv4 routes need to reach a trust agreement on the route exchange.
- VPN-IPv4 routes are exchanged only between VPN peers. A VPN user cannot exchange VPN-IPv4 routes with the public network or with MP-EBGP peers with whom it has not signed a trust agreement.

III. Advertising Labeled VPN-IPv4 Routes Through Multihop MP-EBGP Between PEs

The two methods above require ASBRs to participate in maintaining and distributing VPN-IPv4 routes. When all ASs need to exchange a great amount of VPN routes, ASBRs may become the bottleneck that prevents the extension of network.

One solution is to make PEs exchange VPN-IPv4 routes directly with each other, without the participation of ASBRs.

Two ASBRs advertise labeled IPv4 routes to PEs in their respective ASs through MP-IBGP.

ASBRs neither keep VPN-IPv4 routes nor advertise VPN-IPv4 routes in between.

ASBRs keep the labeled IPv4 routes of PEs in the AS and advertise them to the peers in other ASs. The ASBR in the transit AS also advertises labeled IPv4 routes. Therefore, an LSP is established between ingress PE and egress PE.

PEs in different ASs establish Multihop EBGP connections with each other and exchange VPN-IPv4 routes.

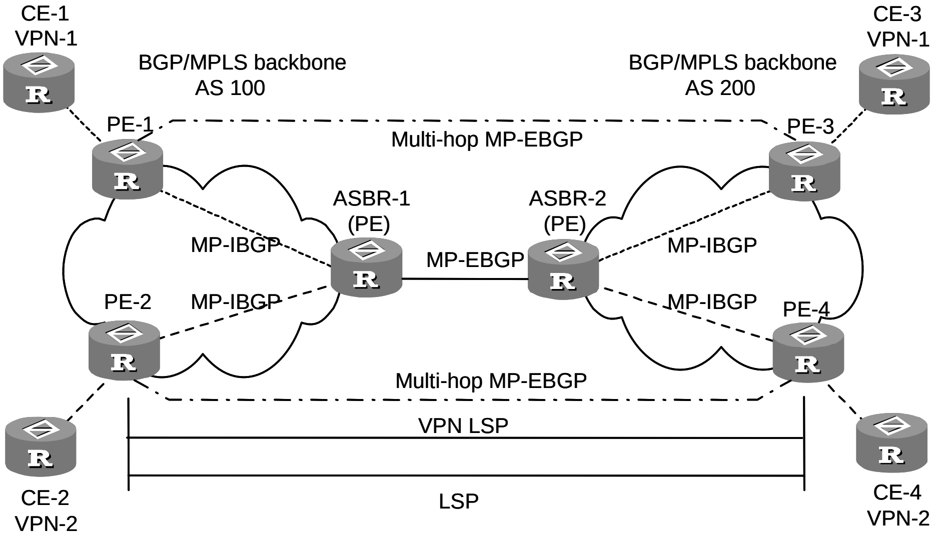


Figure 3-11 Network diagram for advertising labeled VPN-IPv4 routes through Multihop MP-EBGP between PEs

To improve the extensibility, you can specify an RR in each AS to keep all VPN-IPv4 routes and exchange VPN-IPv4 routes with PEs in the AS. The RRs in two ASs establish multi-AS VPNv4 connection with each other and advertise VPN-IPv4 routes, as shown in the following figure.

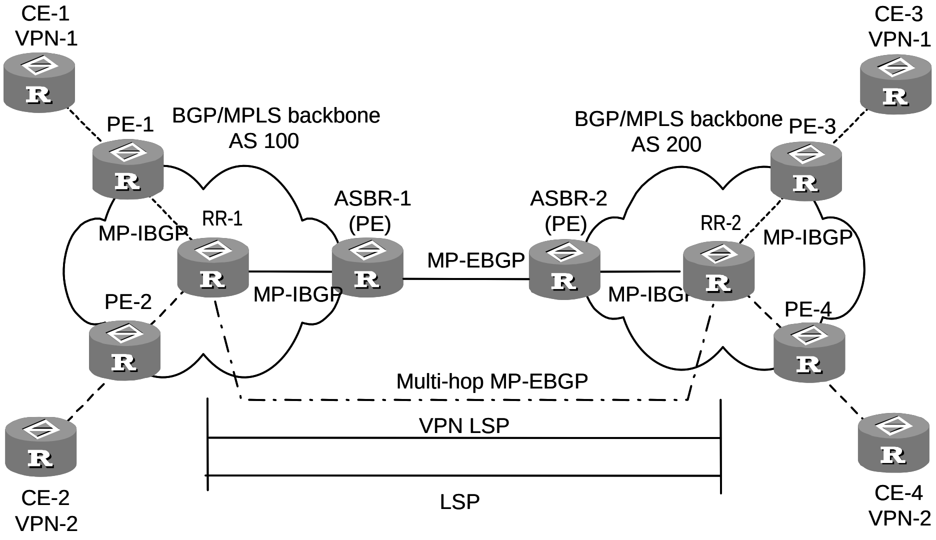


Figure 3-12 Network diagram for multi-AS VPN Option C adopting RR

3.2 BGP/MPLS VPN Configuration

📖 **Note:**

If you have configured both L2VPN and L3VPN services, L3VPN service must comply with L2VPN service. If you remove L2VPN service, you can go on using L3VPN service.

To configure MPLS VPN it is required to complete the following procedures in general:

- Configure basic information on PE, CE and P.
- Establish the logical or physical link with IP capabilities from PE to PE.
- Advertise and update VPN network information.

I. CE router

Only static route, RIP, OSPF or EBGP is configured for VPN routing information exchange with the PE connected, without MPLS.

II. PE router

It implements MPLS/BGP VPN core functions, so its configuration is a bit complicated, including:

- Configure MPLS basic capacity, joint maintenance of LSP with P router or other PE router
- Configure BGP/MPLS VPN site, i.e. VPN instance
- Configure static route, RIP, OSPF or MP-EBGP, for VPN routing information exchange with CE.
- Configure IGP, for intra-PE interconnection.
- Configure MP-IBGP, for VPN routing information exchange between PEs.

III. P router

MPLS basic capacity is configured, to support LDP and MPLS forwarding.

The following are detailed configurations.

3.2.1 Configuring CE Router

Only basic configuration is required on CE router, for routing information exchange with PE router. Currently route switching modes available include static route, RIP, OSPF, EBGP, VLAN subinterface etc.

I. Configuring static route

If you select static route mode for CE-PE route switching, you should then configure a private static route pointing to PE on CE.

Perform the following configurations in system view.

Table 3-1 Configure/delete static routes in the VPN-instance routing table

Operation	Command
Create a specific vpn-instance static route	**ip route-static** *ip-address* { *mask* | *mask-length* } { *interface-type interface-number* | *gateway-address* } [**preference** *preference-value*] [**reject** | **blackhole**]
Delete a specific vpn-instance static route	**undo ip route-static** *ip-address* { *mask* | *mask-length* } [*interface-type interface-number* | *gateway-address*] [**preference** *preference-value*]

You can also specify preference for a static route. By default, the preference value for a static route is 60.

II. Configuring RIP

If you select RIP mode for CE-PE route switching, you should then configure RIP on CE. For details about RIP configuration, see RIP configuration section in Routing Protocol of this manual.

III. Configuring OSPF

If you select OSPF mode for CE-PE route switching, you should then configure OSPF on CE. For details about OSPF configuration, see *V 2.41 Operation Manual* – *Routing Protocol*.

IV. Configuring EBGP

If you select BGP mode for CE-PE route switching, you should then configure EBGP peer, redistribute directly connected route, static route and other IGP routes, for BGP to advertise VPN routes to PE.

3.2.2 Configuring PE Router

I. Configuring MPLS basic capacity

It includes configuring MPLS LSR ID, enable global MPLS and enable MPLS in the interface view.

See MPLS Basic Capacity Configure for details.

II. Defining VPN-instance

1) Establish and enter vpn-instance view

The VPN instance is associated with the site. The VPN membership and routing rules of a site is configured in the corresponding VPN instance.

This command is used to establish a new vpn-instance or enter the existing vpn-instance view. To delete a certain vpn-instance, use the **no** form of this command.

If this vpn-instance already exists, then directly enter the view of this vpn-instance to perform the corresponding configurations.

Perform the following configurations in the system view.

Table 3-2 Create and enter vpn-instance view

Operation	Command
Establish and enter vpn-instance view	**ip vpn-instance** *vpn-instance_name*
Delete vpn-instance	**undo ip vpn-instance** *vpn-instance_name*

By default, no vpn-instance is defined.

2) Configure RD for VPN instance

After PE router is configured with RD, MP-BGP attaches the RD behind IPv4 when BGP is redistributed at a VPN route learned at the CE. Then the general IPv4 address is turned into a globally unique VPN IPv4 address.

Perform the following configuration in the vpn-instance view.

Table 3-3 Configure RD for VPN instance

Operation	Command
Configure RD for VPN instance	**route-distinguisher** *route-distinguisher*

Here the parameter is required and no default value is set.

Other parameters for VPN instance cannot be configured before configuring RD for it.

3) Configure vpn-instance description

Perform the following configuration in vpn-instance view to configure vpn-instance description.

Table 3-4 Configure vpn-instance description

Operation	Command
Configure vpn-instance description	**description** *vpn-instance-description*
Delete vpn-instance description	**undo description**

4) Configure vpn-target attribute for vpn-instance

VPN-target attribute, a BGP extension community attribute, controls advertisement of VPN routing information.

It works on such principle:

- When BGP redistributes a VPN route learned at CE, it associates a VPN-target extension community attribute list with the route. Usually the list is the VPN-instance output routing attribute list associated with CE.
- VPN instance defines input routing attribute list according the **import-extcommunity** in VPN-target, defining the range of routes that are acceptable and can be redistributed.
- VPN instance modifies VPN-target attributes for the routes to be advertised, according to the **export-extcommunity** in VPN-target.

Like RD, an extension community includes an ASN plus an arbitrary number or an IP address plus an arbitrary number. There are two types of formats:

16-bit ASN: 32-bit user-defined number, for example, 101:3.

32-bit IP address: 16-bit user-defined number, for example, 192.168.122.15:1.

Perform the following configurations in the vpn-instance view.

Table 3-5 Configure vpn-target attribute for vpn-instance

Operation	Command
Establish vpn-target extension community for vpn-instance	**vpn-target** *vpn-target-extcommunity* [**import-extcommunity** | **export-extcommunity** | **both**]
Delete the specified vpn-target attribute from the vpn-target attribute list	**undo vpn-target** *vpn-target-extcommunity* [**import-extcommunity** | **export-extcommunity** | **both**]

By default, the value is **both**. In general all sites in a VPN can be interconnected, and the import-extcommunity and export-extcommunity attributes are the same.

Up to 16 vpn-targets can be configured with a command, and up to 256 vpn-targets can be configured for a VPN-INSTANCE.

5) Limit the maximum route number in a vpn-instance

This command is used to limit the maximum route number for a vpn-instance to avoid too many routes at the import of PE router.

Perform the following configurations in the vpn-instance sub-mode.

Table 3-6 Limit the maximum route number for a vpn-instance

Operation	Command
Limit the maximum route number for a vpn-instance	**routing-table limit** *threshold-value* { *warn-threshold* **| syslog-alert** }

Operation	Command
Remove maximum route number limitation	**undo routing-table limit**

🕮 **Note:**

Changing maximum route count for VPN-instance will not affect the existing routing table. To make the new configuration take effect immediately, you should rebuild the corresponding routing protocol or perform **shutdown**/**undo shutdown** operation on the corresponding interface.

6) Associate interface with vpn-instance

VPN instance is associated with the directly connected site through interface binding. When the packets from the site reach the PE router though the interface bound, then the PE can look routing information (including next hop, label, egress interface etc.) up in the corresponding VPN instance.

This command can associate a vpn-instance with an interface.

Perform the following configurations in the interface view.

Table 3-7 Associate the interface with vpn-instance

Operation	Command
Associate the interface with vpn-instance	**ip binding vpn-instance** *vpn-instance-name*
Remove the association of the interface with vpn-instance	**undo ip binding vpn-instance** *vpn-instance-name*

⚠ **Caution:**

As executing the **ip binding vpn-instance** command on an interface will delete the IP address of the interface, you must configure the IP address of the interface after executing that command when you bind the interface with a vpn-instance.

III. Configuring PE-CE Routing Switch

These routing switch modes are available between PE and CE: static route, RIP, OSPF, EBGP and VLAN subinterface.

1) Configure static route on PE

You can configure a static route pointing to CE on PE for it to learn VPN routing information from CE.

Perform the following configuration in the system view.

Table 3-8 Create/delete the static route in vpn-instance routing table

Operation	Command
Create a specific vpn-instance static route	**ip route-static vpn-instance** *vpn-instance-name1 vpn-instance-name2 …destination-address* { *mask* | *mask-length* } { *interface-type interface-number* [*nexthop-address*] | **vpn-instance** *vpn-nexthop-name vpn-nexthop-address* | *nexthop-address* [**public**] } [**preference** *preference-value*] [**reject** | **blackhole**]
Delete a specific vpn-instance static route	**undo ip route-static vpn-instance** *vpn-instance-name1 vpn-instance-name2 … destination-address* { *mask* | *mask-length* } { *interface-type interface-number* [**vpn-instance** *vpn-nexthop-name vpn-nexthop-address* | *nexthop-address* [**public**] } [**preference** *preference-value*]

You can also specify preference for a static route. By default, the preference value for a static route is 60.

2) Configure RIP multi-instance

If you select RIP mode for CE-PE route switching, you should then specify running environment for RIP instance on PE. With this command, you can enter RIP view and redistribute and advertise RIP instance in the view.

Perform the following configuration in the RIP view.

Table 3-9 Configure PE-CE RIP instance

Operation	Command
Create PE-CE RIP instance	**ipv4-family** [**unicast**] **vpn-instance** *vpn-instance-name*
Delete PE-CE RIP instance	**undo ipv4-family** [**unicast**] **vpn-instance** *vpn-instance-name*

Then configure the RIP multi-instance to induct IBGP routing.

For details about RIP configuration, see Routing Protocol of this manual.

3) Configure EBGP on PE

If EBGP runs between PE and CE, you should then configure neighbor for each VPN and redistribute IGP route into CE in the VPN-instance view of MP-BGP.

Step 1: Configure peer group

Perform the following configurations in the VPN-instance view of MP-BGP.

Table 3-10 Configure peer group

Operation	Command
Configure a peer group	**group** *group-name* [**internal** | **external**]
Delete the specified peer group	**undo group** *group-name*

By default, the peer group is configured as internal. When BGP mode is used for PE-CE route switching, they often belong to different ASs, so you should configure EBGP peer as external.

Step 2: Configure AS number for a specific neighbor

When EBGP mode is used for PE-CE route switching, you should configure AS number for a specific neighbor for every CE VPN-instance.

Perform the following configurations in the VPN-instance view of MP-BGP.

Table 3-11 Configure AS number for a specific neighbor

Operation	Command
Configure AS number for a specific neighbor	**peer** { *group-name* | *peer-address* **group** *group-name* } **as-number** *as-number*
Delete the AS number of a specific neighbor	**undo peer** { *group-name* | [*peer-address* **group** *group-name*] } **as-number** *as-number*

Step3: Redistribute IGP route

To advertise correctly VPN routing information over public network to other PEs with which BGP adjacency has been created, a PE must redistribute the VPN routing information of the directly connected CE into its MBGP routing table.

For example, if a static route is used between PE and CE, PE must redistribute a static route in VPN-instance view of MBGP (import-route static). If RIP is run between PE and CE, PE must redistribute an RIP route in VPN-instance view of MBGP (import-route rip). If BGP is run between PE and CE, MBGP redistributes a directly connected route.

Perform the following configurations in the VPN-instance view of MBGP.

Table 3-12 Redistribute IGP routes

Operation	Command
Redistribute IGP routes.	**import-route** *protocol* [*process-id*] [**med** *med*]
Remove IGP route distribution.	**undo import-route** *protocol*

Step 4: Configure BGP in asynchronous mode

Perform the following configuration in the VPN-instance view of MBGP.

Table 3-13 Configure BGP asynchronous with IGP

Operation	Command
Configure BGP asynchronous with IGP	**undo synchronization**

By default, asynchronous mode is selected.

Step 5: Permit route loop configuration in Hub&Spoke networking (optional)

Normally, PE-CE configuration can be performed by specifying the AS number of the peer; other configurations can be performed by keeping the system default value.

In the case of standard BGP, BGP tests routing loop via AS number to avoid generating routing loop. In the case of Hub&Spoke networking, however, PE carries the AS number of the local autonomous system when advertising the routing information to CE, if EBGP is run between PE and CE. Accordingly, the updated routing information will carry the AS number of the local autonomous system when route update is received from CE. In this case, PE cannot receive the route update information.

This phenomenon can be avoided by configuring the **peer allowas-loop** command, which permits the routing loop to pass through and makes PE still receive the route update information containing the local AS number from CE.

Perform the following configuration in IPv4 address-family sub-view.

Table 3-14 Allow/disable routing loop

Operation	Command
Allow routing loop.	**peer** { *group-name* **|** *peer-address* } **allow-as-loop** [*number*]
Disable routing loop	**undo peer** { *group-name* **|** *peer-address* } **allow-as-loop**

By default, the received route update information is not allowed to generate loop information.

Step 6: Configure BGP attribute.

IV. Configuring PE-PE route switching

To exchange VPN-IPv4 routing information between PEs, you should configure MP-IBGP on PEs.

Perform the following configurations in BGP view or PVN instance view.

1) Configure IBGP

These steps are often required.

Step 1: Configure BGP as asynchronous.

Step 2: Configure BGP neighbor.

Note that BGP adjacency is established through loopback interface and the sub-net mask must be 32 bits.

Step 3: Permit BGP session over any operable TCP interface.

In general, BGP uses the best local address in TCP connection. To keep TCP connection available even when the interface involved fails, you can permit BGP session over any interface through which TCP connection can be set up.

Table 3-15 Permit BGP session over any operable TCP interface

Operation	Command
Permit BGP session over any operable TCP interface	**peer** { *peer-address* | *group-name* } **connect-interface** *interface-type interface-number*
Use the best local address for TCP connection	**undo peer** { *peer-address* | *group-name* } **connect-interface** *interface-type interface-number*

BGP often uses the specified loopback interface to set up BGP adjacency with the peer. This can reduce the impact of network flap, because loopback interfaces are always up.

2) Configure MP-IBGP

Step: Enter MP-IBGP address family view.

Perform the following configurations in BGP view.

Table 3-16 Configure VPNv4 address family view

Operation	Command
Enter MBGP VPNv4 view	**ipv4-family vpnv4** [**unicast**]
Exit MBGP VPNv4 view	**undo ipv4-family vpnv4** [**unicast**]

Step 2: Configure MBGP neighbor

Configure MBGP internal neighbor in MBGP VPNv4 view.

Step 3: Activate peer (group)

By default, BGP neighbor is active while MBGP neighbor is inactive. You should activate MBGP neighbor in VPNv4 view.

Step 4: Configure local address as next hop in route advertisement (optional)

It is not configured by default. When configuring in multi-AS VPN Option B mode, you must configure the IBGP peers in each involved domain with this command.

Table 3-17 Configure its address as next hop in route advertisement

Operation	Command
Configure its address as next hop in route advertisement	**peer** { *peer-address* | *group-name* } **next-hop-local**
Remove the configuration	**undo peer** { *peer-address* | *group-name* } **next-hop-local**

Step 5: Transfer BGP update packet without AS number (optional)

Table 3-18 Transfer BGP update packet without AS number

Operation	Command
Transfer BGP update packet without AS number	**peer** { *peer-address* | *group-name* } **public-as-only**
Transfer BGP update packet with AS number	**undo peer** { *peer-address* | *group-name* } **public-as-only**

V. Configuring OSPF VPN Extension

Configuration of OSPF VPN extension includes:

- Running OSPF between PE and CE
- Configuring Multi-VPN-Instance CE
- Configuring sham link

1) Configure OSPF multi-instance on PE

If you select OSPF mode for CE-PE route switching, you should then configure OSPF multi-instance on PE. It should be noted that when OSPF routes and directly connected routes are redistributed into VPN instance, BGP routes should also be redistributed into OSPF. Here only OSPF multi-instance configuration is detailed.

First step: Configure OSPF procedure.

Perform the following configurations in the system view.

Table 3-19 Configure OSPF procedure

Operation	Command
Configure an OSPF procedure	**ospf** *process-id* [**router-id** *router-id-number*] [**vpn-instance** *vpn-instance-name*]
Delete an OSPF procedure	**undo ospf** *process-id*

By default, the procedure index is 1.

⚠ **Caution:**

An OSPF procedure can only belong to one VPN instance, while one VPN instance may contain multiple OSPF procedures. By default, an OSPF procedure belongs to public network.

Step 2: Configure domain ID

Domain ID identifies an OSPF autonomous system (AS). Each procedure is configured with one domain ID, but different procedures may have the same domain ID.

Table 3-20 Configure domain ID

Operation	Command
Configure domain ID	**domain-id** { *id-number* | *id-addr* }
Restore the default value	**undo domain-id**

By default, *id-number* is 0 and *id-addr* is 0.0.0.0.

It is recommended that all OSPF instances in VPN be configured with the same domain ID or the default value 0.

⚠ **Caution:**

The configured value will not take effect unit the command **reset ospf** is executed.

Step 3: Configure tag for redistributed VPN route (optional)

If a VPN site is linked to multiple PEs, routing ring may be caused when the routes learned by MPLS/BGP are received by another PE router in being advertised by category-5/-7 LSA of a PE to the VPN site. To solve this problem, you should configure route-tag. It is recommended to configure identical route-tag for the PEs in the same VPN.

Perform the following configurations in OSPF view.

⚠ **Caution:**

The configured value will not take effect unit the command **reset ospf** is executed.

Table 3-21 Configure tag for redistributed VPN route

Operation	Command
Configure tag for an redistributed VPN route	**route-tag** *tag-number*
Restore the default value	**undo route-tag**

By default, the first two characters of tag-number are fixed to 0xD000 and the last two ones are the AS number of the local BGP. For example, if the local BGP AS number is 100, the tag value in decimal is 3489661028. Tag-number is in range of 0~4294967295.

2) Configuring Multi-VPN-Instance CE

You may configure OSPF multi-instance to isolate the services of different VPNs.

After binding an OSPF process with a VPN instance on a CE router, you must configure the following command in OSPF view.

Table 3-22 Configure a router as multi-VPN-instance CE

Operation	Command
Configure a router as multi-VPN-instance CE	**vpn-instance-capability simple**
Remove the configuration	**undo vpn-instance-capability**

3) Configuring a Sham-Link

Sham links are required between two CEs when backdoor links are set up between the two PEs and service data is expected to be transmitted over MPLS backbone. A sham link between two PEs is considered as a link in OSPF domain. Its source and destination addresses are both the loopback interface address with 32-bit mask, but this loopback interface should be bound to a VPN instance and directly connected routes must be redistributed to BGP.

Perform the following configuration in OSPF domain view.

Table 3-23 Configure a sham-link

Operation	Command
Configure a sham-link	**sham-link** *source-addr destination-addr* [**cost** *cost-value*] [**simple** *password* **|** **md5** *keyid key*] [**dead** *seconds*] [**hello** *seconds*] [**retransmit** *seconds*] [**trans-delay** *seconds*]

Operation	Command
Remove the sham-link	**undo sham-link** *source-addr destination-addr*

By default, the value of **cost** is 1, and the values of **dead**, **hello**, **retransmit** and **trans-delay** are respectively 40, 10, 5 and 1 second.

VI. Configuring HoVPN

The difference between HoVPN configuration and common BGP/MPLS VPN configuration lies in the SPE-UPE connection.

You need to perform the following configuration:

- Specifying a BGP peer/peer group on SPE as the UPE
- Sending the default routes of specified VPN instances to UPE

No special configuration is needed for HoVPN on UPE.

Step 1: Advertise default route to the peer (group)

This command adds a default route which uses local address as next hop on the PE SPE.

Perform the following configuration in BGP or MBGP IPv4-family view.

Table 3-24 Advertise default route to the peer (group)

Operation	Command
Configure to advertise default route to the peer (group)	**peer** *group-name* **default-route-advertise**
Remove to advertise default route to the peer (group)	**undo peer** *group-name* **default-route-advertise**

After executing the **peer default-route-advertise** command, SPE advertises a default route to UPE with its address being the next hop, regardless of the existence of default routes in the local routing table.

Note:

Before sending the default routes of specified VPN instances to a BGP peer/peer group, make sure that the BGP peer/peer group is UPE.

Step 2: Configure BGP neighbor as the UPE of BGP/MPLS VPN

Perform the following configurations in VPNv4 view.

Table 3-25 Configure BGP neighbor as the UPE of BGP/MPLS VPN

Operation	Command
Configure BGP neighbor as the UPE of BGP/MPLS VPN	**peer** *peer-address* **upe**
Disable the configuration	**undo peer** *peer-address* **upe**

VII. Configuring multi-role host attribute

After the configuration of the routing switch between PEs,, configure these items on PE to achieve multi-role application with the site connected.

Step 1: Configure VPN-instance.

In multi-role application, a site is connected to a PE through physical port, but it can access multiple VPNs. So you need to configure multiple VPN-instances on the PE and bind the site port with the desired VPNs. For details about VPN-instance configuration, see the section “Defining VPN-instance”.

Step 2: Configure policy routing

If policy routing has been enabled and the route-policy conditions have been met, the command in the following table can be used to specify the system to forward the packets along the route found by looking up the configured *vpn-name1*, *vpn-name2*, *vpn-name3*, *vpn-name4*, *vpn-name5*, and *vpn-name6*.

Perform the following configuration in route-policy view.

Table 3-26 Look up private forwarding route and make the forwarding

Operation	Command
Look up private forwarding route and make the forwarding	**apply access-vpn vpn-instance** [*vpn-name1 vpn-name2 …*]
Remove the lookup in the specified VPN instances	**undo apply access-vpn vpn-instance** [*vpn-name1 vpn-name2 …*]

Step 3: Configure a private static route

Configure a static route to specify an interface in another VPN as egress interface, so that the packets from PE to CE can be returned directly to the site.

Perform the following configurations in system view.

Table 3-27 Configure static route

Operation	Command
Configure a private static route	**ip route-static vpn-instance** *vpn-instance-name1 vpn-instance-name2* … *ip-address* { *mask* | *mask-length* } { *interface-type interface-number* | [**vpn-instance** *vpn-nexthop-name vpn-nexthop-address*] } [**preference** *preference-value*] [**reject** | **blackhole**]
Remove the static route	**undo ip route-static vpn-instance** *vpn-instance-name1 vpn-instance-name2* … *ip-address* { *mask* | *mask-length* } { *interface-type interface-number* [**vpn-instance** *vpn-nexthop-name vpn-nexthop-address*] } [**preference** *preference-value*] [**reject** | **blackhole**]

VIII. Configuring Multi-AS BGP/MPLS VPN

Do following configuration to achieve the Multi-AS BGP/MPLS VPN after the configuration of the routing switch between PEs.

1) Configuring VPN-Target Filtering

By default, PE performs VPN-Target filtering for the received VPNv4 routes. The routes passing the filtering are added into the routing table, while the rest are discarded.

If PE acts as an ASBR, it needs to collect all the VPNv4 routing information and advertise it to other ASBRs. In this case, PE accepts all the VPNv4 routing information from its peers without filtering based on VPN-target.

Perform the following configuration in BGP-VPNv4 sub-address family view.

Table 3-28 Configure VPN-Target filtering

Operation	Command
Enable VPN-Target filtering for the VPNv4 routing information	**policy vpn-target**
Disable VPN-Target filtering for the VPNv4 routing information	**undo policy vpn-target**

The **undo policy vpn-target** command is only applied to ABSR PEs in multi-AS VPN Option B.

2) Configuring Label Processing on Public Network Routes

In the Multihop MP-EBGP multi-AS VPN solution, you need to establish a multi-AS VPN LSP. PEs and ASBRs exchange public network routes through carried MPLS label information.

Through the route-policy, MPLS labels are assigned to those public network routes that match certain conditions. Other routes are still common IPv4 routes.

Perform the following configuration in route-policy view.

Table 3-29 Configure label processing on public network routes

Operation	Command
Assign MPLS labels to the public network routes that match route-policy conditions	**apply mpls-label**
Remove the assigned MPLS labels	**undo apply mpls-label**
Configure to only receive/transmit the public network routes with MPLS labels	**if-match mpls-label**
Remove the configuration of only receiving/sending public network routes with MPLS labels	**undo if-match mpls-label**

By default, public network routes do not carry MPLS labels and no route-policy is defined.

The public network routes with MPLS labels are advertised by MP-BGP. According to RFC 3107 (Carrying Label Information in BGP-4), the label mapping information of a route can be piggybacked by advertising BGP Update messages of the route. This capability is implemented through BGP extension attributes and requires BGP peers processing labeled IPv4 routes.

Perform the following configuration in BGP view.

Table 3-30 Configure the capability for processing labeled IPv4 routes

Operation	Command
Enable the capability for processing labeled IPv4 routes	**peer** *group-name* **label-route-capability**
Disable the capability for processing labeled IPv4 routes	**undo peer** *group-name* **label-route-capability**

By default, BGP peers cannot process labeled IPv4 routes.

3) Configuring Invariable Next Hop when Advertising Routes

Generally, BGP Speaker changes the next hop to itself when advertising routes to EBGP peers. In the networking application that adopts Multihop MP-EBGP multi-AS VPN mode and uses RR to advertise VPNv4 routes, BGP Speaker cannot vary the next hop when advertising VPNv4 routes between RRs.

Perform the following configuration in BGP view, BGP-VPNv4 sub-address family view, BGP VPN instance view, or BGP-IPv4 multicast sub-address family view.

Table 3-31 Configure invariable next hop when advertising routes

Operation	Command
Configure invariable next hop when advertising routes to EBGP peers	**peer** *group-name* **next-hop-invariable**
Restore the default configuration	**undo peer** *group-name* **next-hop-invariable**

By default, the next hop changes to BGP Speaker when sending routes to EBGP peers.

3.2.3 Configuring P Router

P router does not maintain VPN routes, but do keep connection with public network and coordinate with PE in creating LSPs. These configurations are required on P router:

Step 1: Configure MPLS basic capacity and enable LDP on the interfaces connecting P router to PE router, for forwarding MPLS packets. See Chapter 2 "MPLS Basic Capability Configuration" for details.

Step 2: Enable OSPF on the interfaces that connect P router to PE router and redistribute directly connected routes. See Routing Protocol for details.

3.3 BGP/MPLS VPN Display and Debug

I. Displaying VPN address information from BGP table

After the above configuration, execute **display** command in any view to display the running of the VPNv4 information in BGP database configuration, and to verify the effect of the configuration.

Table 3-32 Display VPN address information from BGP table

Operation	Command
Display VPN address information from BGP table	**display bgp vpnv4** { **all** | **route-distinguisher** *rd-value* | **vpn-instance** *vpn-instance-name* } { **group** [*group-name*] | **network** | **peer** [*ip-address1* | **verbose**] | **routing** [*ip-address2* | **statistic**] [**label**] [**as-path-acl** *as-path-acl* | **cidr** | **community** [*community-number* | **no-advertise** | **no-export** | **no-export-subconfed** | **whole-match**] | **community-list** *community-list* [**whole-match**] | **different-origin-as** | **peer** *ip-address1* [**advertised** | **received**] | **regular-expression** *text*] }

II. Displaying IP routing table associated with vpn-instance

After the above configuration, you can execute **display** command in any view to display the corresponding information in the IP routing tables related to vpn-instance, and to verify the effect of the configuration.

Table 3-33 Display the IP routing table associated with vpn-instance

Operation	Command
Display the IP routing table associated with vpn-instance	**display ip routing-table vpn-instance** *vpn-instance-name* [**statistics** | [*ip-address*] [**verbose**]]

III. Displaying vpn-instance related information

After finishing the above configuration, executing the **display** command in any view can display the vpn-instance related information, including its RD, description, the interfaces associated with it, and so on. You can view the information to verify the configuration effect.

Table 3-34 Display the vpn-instance related information

Operation	Command
Display the vpn-instance related information, including its RD, description, the interfaces associated with it, and so on.	**display ip vpn-instance** [*vpn-instance-name* **|** **verbose**]

IV. Debugging information concerning processing BGP

Execute **debugging** command in user view for the debugging of the related vpn-instance information.

Table 3-35 Debugging information concerning processing BGP

Operation	Command
Debug information concerning processing BGP	**debugging bgp** { { **keepalive** | **mp-update** | **open** | **packet** | **update** | **route-refresh** } [**receive** | **send** | **verbose**] } { **all** | **event** | **normal** }
Disable the debug information	**undo debugging bgp** { { **keepalive** | **mp-update** | **open** | **packet** | **update** | **route-refresh** } [**receive** | **send** | **verbose**] } { **all** | **event** | **normal** }

V. Displaying MPLS l3vpn-lsp information

Table 3-36 Display MPLS l3vpn-lsp information

Operation	Command
Display information on MPLS L3VPN LSPs.	**display mpls l3vpn-lsp** [**verbose**] [**include** *text*]

Operation	Command
Display information on the VPN-instances of MPLS L3VPN LSPs.	**display mpls l3vpn-lsp** [**vpn-instance** *vpn-instance-name*] [**transit | egress | ingress**] [**include** *text* | **verbose**]

VI. Displaying sham link

Table 3-37 Display sham link

Operation	Command
Display sham link	**display ospf** [*process-id*] **sham-link**

3.4 BGP/MPLS VPN Configuration Example

3.4.1 Configuring Integrated BGP/MPLS VPN

I. Network requirements

- VPN-A includes CE1 and CE3; VPN-B includes CE2 and CE4
- Subscribers in different VPNs cannot access each other. The VPN-target attribute for VPN-A is 111:1 and that for VPN-B is 222:2.
- 3Com routers serve as PE, 3Com routers running MPLS serve as P, and CEs are common middle or lower end routers.

Note:

The configuration in this case is focused on:

- Configure EBGP to exchange VPN routing information between CE and PE.
- Configure OSPF for intra-PE communication between PEs.
- Configure MP-IBGP to exchange VPN routing information between PEs.

II. Network diagram

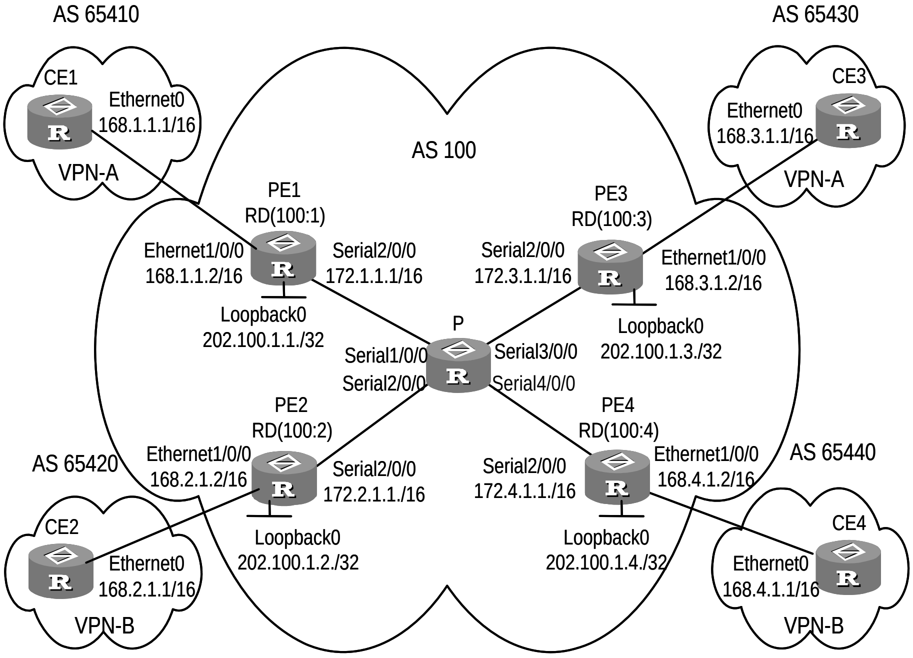


Figure 3-13 Integrated BGP/MPLS VPN network diagram

III. Configuration procedure

1) Configure CE1

# Configure CE1 and PE1 as neighbors, redistribute directly connected routes and static routes to redistribute intra-CE1 VPN routes into BGP and advertise to PE1. CE1 connects PE1 through Ethernet0.

```
[CE1] interface ethernet 0/0/0
[CE1-Ethernet0/0/0] ip address 168.1.1.1 255.255.0.0
[CE1-Ethernet0/0/0] quit
[CE1] bgp 65410
[CE1-bgp] group 168 external
[CE1-bgp] peer 168.1.1.2 group 168 as-number 100
[CE1-bgp] import-route direct
[CE1-bgp] import-route static
```

Note:

The configuration of other three CEs (CE2~CE4) is similar, so it is not mentioned here.

2) Configure PE1.

# Configure vpn-instance for VPN-A on PE1, as well as other associated attributes to control advertisement of VPN routing information.

```
[PE1] ip vpn-instance vpna
[PE1-vpn-vpna] route-distinguisher 100:1
[PE1-vpn- vpna] vpn-target 111:1 both
[PE1-vpn- vpna] quit
```

# Configure PE1 and CE1 as EBGP neighbors, redistribute CE1 VPN routes learned into MBGP VPN-instance address family.

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpna
[PE1-bgp-af-vpn-instance] group 168 external
[PE1-bgp-af-vpn-instance] peer 168.1.1.1 group 168 as-number 65410
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-instance] quit
```

# Bind the interface Ethernet1/0/0 connecting PE1 and CE1 to the VPN-A. Note that you should first configure association between the interface and VPN-instance, and then the IP address.

```
[PE1] interface ethernet 1/0/0
[PE1-Ethernet1/0/0] ip binding vpn-instance vpna
[PE1-Ethernet1/0/0] ip address 168.1.1.2 255.255.0.0
[PE1-Ethernet1/0/0] quit
```

# Configure loopback interface. (For PE, the IP address for loopback interface must be a host address with 32-bit mask, to prevent the route is aggregated and then LSP cannot process correctly interior-layer labels.)

```
[PE1] interface loopback0
[PE1-LoopBack 0] ip address 202.100.1.1 255.255.255.255
[PE1-LoopBack 0] quit
```

# Configure MPLS basic capacity and enable LDP on the interface connecting PE1 and P, create LSP for MPLS packet forwarding.

```
[PE1] mpls lsr-id 172.1.1.1
[PE1-mpls] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface Serial2/0/0
[PE1-Serial2/0/0] ip address 172.1.1.1 255.255.0.0
[PE1-Serial2/0/0] mpls ldp enable
[PE1-Serial2/0/0] quit
```

# Enable OSPF on the interface connecting PE1 and P and on the loopback interface, and allow it to redistribute directly connected routes for intra-PE communication.

```
[PE1] ospf
[PE1-ospf] area 0
```

```
[PE1-ospf-area-0.0.0.0] network 172.1.0.0 0.0.255.255
[PE1-ospf-area-0.0.0.0] network 202.100.1.1 0.0.0.0
[PE1-ospf-area-0.0.0.0] quit
[PE1-ospf] import-route direct
[PE1-ospf] quit
```

# Set up MP-IBGP adjacency between PEs, for intra-PE VPN routing information exchange, activate MP-IBGP peer in VPNv4 address family view.

```
[PE1] bgp 100
[PE1-bgp] group 202 internal
[PE1-bgp] peer 202.100.1.3 group 202
[PE1-bgp] peer 202.100.1.3 connect-interface loopback0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer 202 enable
[PE1-bgp-af-vpn] peer 202.100.1.3 group 202
[PE1-bgp-af-vpn] quit
[PE1-bgp] quit
```

3) Configure P router

# Configure MPLS basic capacity, enable LDP on the interfaces connecting P and PE for MPLS packet forwarding.

```
[P] mpls lsr-id 172.1.1.2
[P] mpls ldp
[P-mpls-ldp] quit
[P] interface Serial1/0/0
[P-Serial1/0/0] ip address 172.1.1.2 255.255.0.0
[P-Serial1/0/0] mpls ldp enable
[P-Serial1/0/0] interface Serial2/0/0
[P-Serial2/0/0] ip address 172.2.1.2 255.255.0.0
[P-Serial2/0/0] mpls ldp enable
[P-Serial2/0/0] interface Serial3/0/0
[P-Serial3/0/0] ip address 172.3.1.2 255.255.0.0
[P-Serial3/0/0] mpls ldp enable
[P-Serial3/0/0] interface Serial4/0/0
[P-Serial4/0/0] ip address 172.4.1.2 255.255.0.0
[P-Serial4/0/0] mpls ldp enable
[P-Serial4/0/0] quit
```

# Enable OSPF on the interfaces connecting P and PE, and allow it to redistribute directly connected route for intra-PE communication.

```
[P] ospf
[P-ospf] area 0
[P-ospf-area-0.0.0.0] network 172.1.1.0 0.0.255.255
[P-ospf-area-0.0.0.0] network 172.2.1.0 0.0.255.255
```

```
[P-ospf-area-0.0.0.0] network 172.3.1.0 0.0.255.255
[P-ospf-area-0.0.0.0] network 172.4.1.0 0.0.255.255
[P-ospf-area-0.0.0.0] quit
[P-ospf] import-route direct
```

4) Configure PE3

Note:

The configuration on PE3 is similar to that on PE1, you should pay more attention to VPN routing attribute setting on PE3 to get information about how to control advertisement of a same VPN routing information (with same VPN-target) over MPLS network.

# Create VPN-instance for VPN-A on PE3, configure correlative attributes to control advertisement of VPN routing information.

```
[PE3] ip vpn-instance vpna
[PE3-vpn- vpna] route-distinguisher 100:3
[PE3-vpn- vpna] vpn-target 111:1 both
[PE3-vpn- vpna ] quit
```

# Set up EBGP adjacency between PE3 and CE3, redistribute intra-CE3 VPN routes learned to MBGP VPN-instance address family.

```
[PE3] bgp 100
[PE3-bgp] ipv4-family vpn-instance vpna
[PE3-bgp-af-vpn-instance] group 168 external
[PE3-bgp-af-vpn-instance] peer 168.3.1.1 group 168 as-number 65430
[PE3-bgp-af-vpn-instance] import-route direct
[PE3-bgp-af-instance] quit
```

# Bind the interface Ethernet1/0/0 connecting PE3 and CE3 to VPN-A.

```
[PE3] interface ethernet 1/0/0
[PE3-Ethernet1/0/0] ip binding vpn-instance vpna
[PE3-Ethernet1/0/0] ip address 168.3.1.2 255.255.0.0
[PE3-Ethernet1/0/0] quit
```

# Configure loopback interface

```
[PE3] interface loopback0
[PE3-LoopBack 0] ip address 202.100.1.3 255.255.255.255
[PE3-LoopBack 0] quit
```

# Configure MPLS basic capacity, enable LDP on the interface connecting PE3 and P, and create LSP to achieve MPLS packet forwarding.

```
[PE3] mpls lsr-id 172.3.1.1
```

```
[PE3-mpls] mpls ldp
[PE3-mpls-ldp] quit
[PE3] interface Serial 2/0/0
[PE3-Serial2/0/0] ip address 172.3.1.1 255.255.0.0
[PE3-Serial2/0/0] mpls ldp enable
[PE3-Serial2/0/0] quit
```

# Enable OSPF on the interface connecting PE3 and P and on the loopback interface, and allow it to redistribute directly connected routes.

```
[PE3] ospf
[PE3] area 0
[PE3-ospf-area-0.0.0.0] network 172.3.0.0 0.0.255.255
[PE3-ospf-area-0.0.0.0] network 202.100.1.3 0.0.0.0
[PE3-ospf-area-0.0.0.0] import-route direct
```

# Set up MP-IBGP adjacency between PEs to exchange intra-PE VPN routing information.

```
[PE1] bgp 100
[PE1-bgp] group 202 internal
[PE3-bgp] peer 202.100.1.1 group 202
[PE3-bgp] peer 202.100.1.1 connect-interface loopback0
[PE3-bgp] ipv4-family vpnv4
[PE3-bgp-af-vpn] peer 202 enable
[PE3-bgp-af-vpn] peer 202.100.1.1 group 202
[PE3-bgp-af-vpn] quit
```

5) Configure PE2 and PE4

The configuration of PE2 and PE4 is similar to that of PE1 and PE3. The details are omitted here.

3.4.2 Configuring GRE Tunnel BGP/MPLS VPN

I. Network requirements

- VPN-A includes CE-1 and CE3; VPN-B includes , CE-2 and , CE-3, and CE-4
- 3Com routers serve as PE, 3Com routers running MPLS serve as P, and CEs are common middle or lower end routers.

II. Network diagram

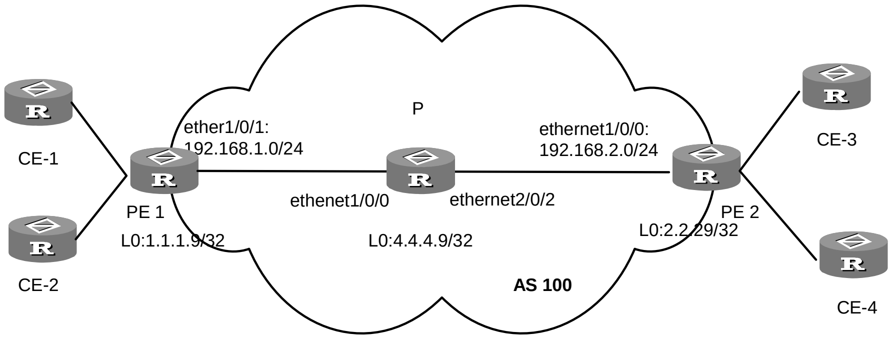


Figure 3-14 GRE tunnel BGP/MPLS VPN network diagram

III. Configuration procedure

1) Configure CE1

# Configure CE1 and PE1 as neighbors, redistribute directly connected routes and static routes to redistribute intra-CE1 VPN routes to BGP and advertise to PE1. CE1 connects PE1 through Ethernet0/0/0.

```
[CE1] interface ethernet 0/0/0
[CE1-Ethernet0/0/0] ip address 20.1.1.1 255.255.0.0
[CE1-Ethernet0/0/0] quit
[CE1] bgp 65410
[CE1-bgp] group 20 external
[CE1-bgp] peer 20.1.1.2 group 20 as-number 100
[CE1-bgp] import-route direct
[CE1-bgp] import-route static
```

Note:

The configuration of other three CEs (CE2~CE4) is similar, so it is not mentioned here.

2) Configure PE1.

# Configure vpn-instance.

```
[PE1] ip vpn-instance vpna
[PE1-vpn-vpna] route-distinguisher 100:1
[PE1-vpn-vpna] vpn-target 100:1 both
[PE1-vpn-vpna] VPN-target 100:2 import-extcommunity
[PE1-vpn-vpna] VPN-target 100:3 export-extcommunity
[PE1-vpn-vpna] quit
```

# Bind the interface Ethernet1/0/0 connecting PE1 and CE1 to the VPN-A.

```
[PE1] interface loopback0
```

```
[PE1-LoopBack0] ip address 1.1.1.9 255.255.255.255
[PE1-LoopBack0] quit
[PE1] interface ethernet 1/0/0
[PE1-Ethernet1/0/0] ip binding vpn-instance vpna
[PE1-Ethernet1/0/0] ip address 20.1.1.2 255.255.0.0
[PE1-Ethernet1/0/0] quit
[PE1] interface ethernet1/0/1
[PE1-Ethernet1/0/1] ip address 192.168.1.1 255.255.255.0
[PE1-Ethernet1/0/1] quit
```

# Configure PE1 and CE1 as EBGP neighbors, redistribute VPN-instance interface routes.

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpna
[PE1-bgp-af-vpn-instance] group 20 external
[PE1-bgp-af-vpn-instance] peer 20.1.1.1 group 20 as-number 65410
[PE1-bgp-af-vpn-instance] peer 20 next-hop-local
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] quit
[PE1-bgp] quit
```

# Set up MP-IBGP adjacency between PEs, for intra-PE VPN routing information exchange, activate MP-IBGP peer in VPNv4 address family view.

```
[PE1] bgp 100
[PE1-bgp] group 2
[PE1-bgp] peer 2.2.2.9 group 2
[PE1-bgp] peer 2.2.2.9 connect-interface loopback0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer 2 enable
[PE1-bgp-af-vpn] peer 2.2.2.9 group 2
```

# Enable OSPF on the interface connecting PE1 and P and the loopback interface, redistribute directly connected routes to achieve intra-AS communication.

```
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 192.168.1.0 0.255.255.255
[PE1-ospf-1-area-0.0.0.0] network 1.1.1.9 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] import-route direct
```

# Configure MPLS.

```
[PE1] mpls lsr-id 1.1.1.9
[PE1] mpls
[PE1-mpls] mpls ldp
```

# Configure GRE tunnel

```
[PE1] interface tunnel 1
[PE1-Tunnel1] tunnel-protocol gre
[PE1-Tunnel1] source loopback 0
[PE1-Tunnel1] destination 2.2.2.9
[PE1-Tunnel1] mpls
[PE1-Tunnel1] mpls ldp enable
```

# Configure static routing.

```
[PE1] ip route-static 2.2.2.9 32 tunnel 1
```

Note:

The configuration of PE2 is similar to PE1, so the details are omitted here.

3) Configure P router

# Configure interface.

```
[P] interface ethernet1/0/0
[P-ethernet1/0/0] ip address 192.168.1.2 255.255.255.0
[P] interface ethernet2/0/1
[P-ethernet2/0/1] ip address 192.168.2.2 255.255.0.0
```

# Enable OSPF.

```
[P] ospf
[P-ospf-1] area 0
[P-ospf-1-area-0.0.0.0] network 192.168.1.0 0.255.255.255
[P-ospf-1-area-0.0.0.0] network 192.168.2.0 0.255.255.255
[P-ospf-1-area-0.0.0.0] import-route direct
```

3.4.3 Configuring Extranet

I. Network requirements

Both Company A and Company B locate their headquarters in City C. They are interconnected with VPNs and own VPN1 and VPN2 respectively.

MPLS provides VPN function. There are some shared resources at the City C for two VPNs. All VPN subscribers can access the shared resources, but VPN subscribers in City A and City B cannot access each other.

The two companies cannot use identical IP addresses, for they share the same VPN-instance at PE2.

Note:

In the case the configuration is focused on controlling access authority of VPN subscribers at different cities by configuring different VPN-target attributes at different PEs.

II. Network diagram

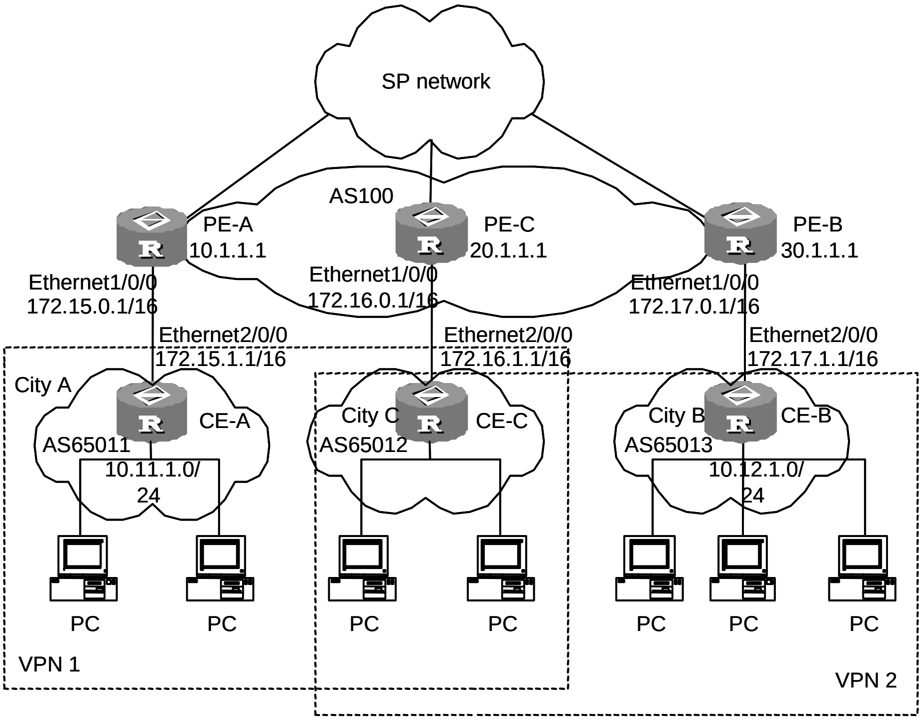


Figure 3-15 Extranet diagram

III. Configuration procedure

Note:

The following contents are omitted in this case: MPLS basic capacity configuration between PEs, configuration between PE and P, configuration between CEs. For these details refer to the former case.

1) Configure PE-A

# Configure VPN-instance for VPN1 on PE-A, so that it can receive VPN routing information of VPN-target 111:1.

```
[PE-A] ip vpn-instance 1
[PE-A-vpn-1] route-distinguisher 100:1
[PE-A-vpn-1] vpn-target 111:1 both
[PE-A-vpn-1] quit
```

# Set up EBGP adjacency between PE-A and CE-A, redistribute intra-CE-A VPN routes learned into MBGP VPN-instance address family.

```
[PE-A] bgp 100
[PE-A-bgp] ipv4-family vpn-instance vpn-instance1
[PE-A-bgp-af-vpn-instance] group 172 external
[PE-A-bgp-af-vpn-instance] peer 172.15.1.1 group 172 as-number 65011
[PE-A-bgp-af-vpn-instance] import-route direct
[PE-A-bgp-af-vpn-instance] import-route static
[PE-A-bgp-af-vpn-instance] quit
[PE-A-bgp] quit
```

# Bind the interface Ethernet1/0/0 connecting CE-A with VPN-instance 1.

```
[PE-A] interface ethernet 1/0/0
[PE-A-Ethernet1/0/0] ip binding vpn-instance vpn-instance1
[PE-A-Ethernet1/0/0] ip address 172.15.0.1 255.255.0.0
[PE-A-Ethernet1/0/0] quit
```

# Configure loopback interface.

```
[PE-A] interface loopback 0
[PE-A-LoopBack0] ip address 10.1.1.1 255.255.255.255
[PE-A-LoopBack0] quit
```

# Configure MPLS basic capacity.

```
[PE-A] mpls lsr-id 10.1.1.1
[PE-A] mpls ldp enable
[PE-A-mpls-ldp] quit
```

# Set up MP-IBGP adjacency between PEs to exchange intra-PE VPN routing information, activate MP-IBGP peer in VPNv4 address family view.

```
[PE-A] bgp 100
[PE-A-bgp] group 20
[PE-A-bgp] peer 20.1.1.1 group 20
[PE-A-bgp] peer 20.1.1.1 connect-interface loopback 0
[PE-A-bgp] group 30
[PE-A-bgp] peer 30.1.1.1 group 30
[PE-A-bgp] peer 30.1.1.1 connect-interface loopback 0
[PE-A-bgp] ipv4-family vpnv4
[PE-A-bgp-af-vpn] peer 20 enable
[PE-A-bgp-af-vpn] peer 20.1.1.1 group 20
[PE-A-bgp-af-vpn] peer 30 enable
```

```
[PE-A-bgp-af-vpn] peer 30.1.1.1 group 30
[PE-A-bgp-af-vpn] quit
```

2) Configure PE-C.

# Create a VPN-instance on PE-C, so that it can transceive VPN routing information of VPN-target 111:1 and 222:2.

```
[PE-C] ip vpn-instance 2
[PE-C-vpn-2] route-distinguisher 100:2
[PE-C-vpn-2] vpn-target 111:1
[PE-C-vpn-2] vpn-target 222:2
[PE-C-vpn-2] quit
```

# Set up EBGP adjacency between PE-C and CE-E, redistribute intra-CE-C VPN routes learned into MBGP VPN-instance address family.

```
[PE-C] bgp 100
[PE-C-bgp] ipv4-family vpn-instance vpn-instance2
[PE-C-bgp-af-vpn-instance] group 172
[PE-C-bgp-af-vpn-instance] peer 172.16.1.1 group 172 as-number 65012
[PE-C-bgp-af-vpn-instance] import-route direct
[PE-C-bgp-af-vpn-instance] import-route static
[PE-C-bgp-af-vpn-instance] quit
[PE-C-bgp] quit
```

# Bind the interface Ethernet1/0/0 connecting CE-C with VPN-instance 2.

```
[PE-C] interface ethernet 1/0/0
[PE-C-Ethernet1/0/0] ip binding vpn-instance vpn-instance2
[PE-C-Ethernet1/0/0] ip address 172.16.0.1 255.255.0.0
```

# Configure loopback interface.

```
[PE-C] interface loopback 0
[PE-C-LoopBack0] ip address 20.1.1.1 255.255.255.255
[PE-C-LoopBack0] quit
```

# Configure MPLS basic capacity.

```
[PE-C] mpls lsr-id 20.1.1.1
[PE-C] mpls ldp enable
[PE-C-mpls-ldp] quit
```

# Set up MP-IBGP adjacency between PEs to exchange intra-PE VPN routing information, activate MP-IBGP peer in VPNv4 address family view.

```
[PE-C] bgp 100
[PE-C-bgp] group 10
[PE-C-bgp] peer 10.1.1.1 group 10
[PE-C-bgp] peer 10.1.1.1 connect-interface loopback 0
[PE-C-bgp] group 30
```

```
[PE-C-bgp] peer 30.1.1.1 group 30
[PE-C-bgp] peer 30.1.1.1 connect-interface loopback 0
[PE-C-bgp] ipv4-family vpnv4
[PE-C-bgp-af-vpn] peer 10 enable
[PE-C-bgp-af-vpn] peer 10.1.1.1 group 10
[PE-C-bgp-af-vpn] peer 30 enable
[PE-C-bgp-af-vpn] peer 30.1.1.1 group 30
[PE-C-bgp-af-vpn] quit
```

3) Configure PE-B.

# Create VPN-instance for VPN2 on PE-B, so that it can transceive VPN routing information of VPN-target 222:2.

```
[PE-B] ip vpn-instance 3
[PE-B-vpn-3] route-distinguisher 100:3
[PE-B-vpn-3] vpn-target 222:2
[PE-B-vpn-3] quit
```

# Set up EBGP adjacency between PE-B and CE-B, redistribute intra-CE-B VPN routes learned into MBGP VPN-instance address family.

```
[PE-B] bgp 100
[PE-B-bgp] ipv4-family vpn-instance vpn-instance3
[PE-B-bgp-af-vpn-instance] group 172 external
[PE-B-bgp-af-vpn-instance] peer 172.17.1.1 group 172 as-number 65013
[PE-B-bgp-af-vpn-instance] import-route direct
[PE-B-bgp-af-vpn-instance] import-route static
[PE-B-bgp-af-vpn-instance] quit
[PE-B-bgp] quit
```

# Bind the interface Ethernet1/0/0 connecting CE-B with VPN-instance 3.

```
[PE-B] interface ethernet 1/0/0
[PE-B-Ethernet1/0/0] ip binding vpn-instance vpn-instance3
[PE-B-Ethernet1/0/0] ip address 172.17.0.1 255.255.0.0
[PE-B-Ethernet1/0/0] quit
```

# Configure loopback interface.

```
[PE-B] interface loopback 0
[PE-B-LoopBack0] ip address 30.1.1.1 255.255.255.255
[PE-B-LoopBack0] quit
```

# Configure MPLS basic capacity.

```
[PE-B] mpls lsr-id 30.1.1.1
[PE-B] mpls ldp enable
[PE-B-mpls-ldp] quit
```

# Set up MP-IBGP adjacency between PEs to exchange intra-PE VPN routing information, activate MP-IBGP peer in VPNv4 address family view.

```
[PE-B] bgp 100
[PE-B-bgp] group 10
[PE-B-bgp] peer 10.1.1.1 group 10
[PE-B-bgp] peer 10.1.1.1 connect-interface loopback 0
[PE-B-bgp] group 20
[PE-B-bgp] peer 20.1.1.1 group 20
[PE-B-bgp] peer 20.1.1.1 connect-interface loopback 0
[PE-B-bgp] ipv4-family vpnv4
[PE-B-bgp-af-vpn] peer 10 enable
[PE-B-bgp-af-vpn] peer 10.1.1.1 group 10
[PE-B-bgp-af-vpn] peer 20 enable
[PE-B-bgp-af-vpn] peer 20.1.1.1 group 20
[PE-B-bgp-af-vpn] quit
```

3.4.4 Configuring Hub&Spoke

I. Network requirements

Hub&Spoke networking is also called central server networking. The site in the center is called hub-site, while the one not in the center is called spoke-site. The hub-site knows the routes to all other sites in the same VPN, and the spoke-site must send its traffic first to hub-site and then to the destination.

A bank has its headquarters network and subsidiary networks, and it requires that subsidiaries cannot exchange data with each other, but through the headquarters network. Hub&Spoke networking topology is used here: CE2 and CE3 are as spoke-sites, while CE1 is as the hub-site of the bank data center. CE1 controls communication between CE1 and CE3.

- Set up IBGP adjacency between PE1 and PE2, between PE1 and PE3, but not between PE2 and PE3, that is, VPN routing information cannot be exchanged between PE2 and PE3.
- Create two VPN-instances on PE1, redistribute VPN routes of VPN-target 100:1, and set VPN-target for VPN routes advertised as 100:2.
- Create one VPN-instance on PE2, redistribute VPN routes of VPN-target 100:2, set VPN-target for VPN routes advertised as 100:1.
- Create one VPN-instance on PE3, redistribute VPN routes of VPN-target 100:2, set VPN-target for VPN routes advertised as 100:1.

Then PE2 and PE3 can only learn their neighbor’s routes through PE1.

Note:

In the case the configuration is focused on two points:

- Route advertisement can be controlled by VPN-target settings on different PEs.
- One routing loop is permitted, so that PE can receive route update messages with AS number included from CE.
- In the HUB&SPOKE networking on the PE1, Vpn-target of VPN-instance (VPN-instance3) for releasing routings cannot be the same with any Vpn-target of VPN-instance (VPN-instance2) for redistributing routings.
- In the HUB&SPOKE networking on the PE1, route-distinguisher rd2 (100:2) of VPN-instance for releasing routings cannot be the same with any one of corresponding route-distinguisher rd1(100:1) , rd4 (100:4) on each PE2, PE3. Rd1 and rd4 can be same or not.

II. Network diagram

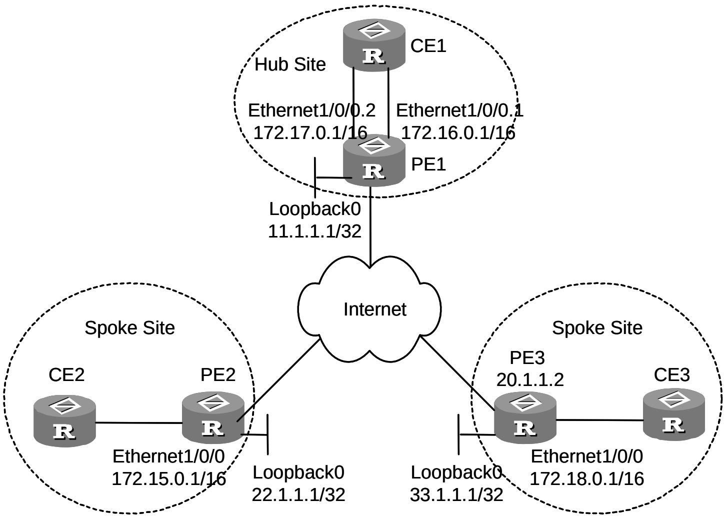


Figure 3-16 Hub&Spoke network diagram

III. Configuration procedure

Note:

The following contents are omitted in this case: MPLS basic capacity configuration between PEs, configuration between PE and P, configuration between CEs. For these details refer to the former case.

1) Configure PE1

# Configure two VPN-instances on PE1, add the specified VPN-target attribute to the routes received from PE2 and PE3.

```
[PE1] ip vpn-instance vpn-instance2
[PE1-vpn- vpn-instance2] route-distinguisher 100:2
[PE1-vpn- vpn-instance2] vpn-target 100:1 import-extcommunity
[PE1-vpn- vpn-instance2] quit
[PE1] ip vpn-instance vpn-instance3
[PE1-vpn- vpn-instance3] route-distinguisher 100:3
[PE1-vpn- vpn-instance3] vpn-target 100:2 export-extcommunity
[PE1-vpn- vpn-instance3] quit
```

# Set up EBGP adjacency between PE1 and CE1, redistribute intra-CE1 VPN routes learned into MBGP VPN-instance address family, with one routing loop permitted.

```
[PE1] bgp 100
[PE1-bgp] group 17216 external
[PE1-bgp] ipv4-family vpn-instance vpn-instance2
[PE1-bgp-af-vpn-instance] peer 172.16.1.1 group 17216 as-number 65002
[PE1-bgp-af-vpn-instance] peer 172.16.1.1 allow-as-loop 1
[PE1-bgp-af-vpn-instance] import-route static
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] quit
[PE1-bgp] group 17217 external
[PE1-bgp] ipv4-family vpn-instance vpn-instance3
[PE1-bgp-af-vpn-instance] peer 172.17.1.1 group 17217 as-number 65002
[PE1-bgp-af-vpn-instance] peer 172.17.1.1 allow-as-loop 1
[PE1-bgp-af-vpn-instance] import-route static
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] quit
[PE1-bgp] quit
```

# Bind Ethernet1/0/0.1 with VPN-instance 2 and Ethernet1/0/0.2 with VPN-instance 3.

```
[PE1] interface ethernet 1/0/0.1
[PE1-Ethernet1/0/0.1] ip binding vpn-instance vpn-instance2
[PE1-Ethernet1/0/0.1] ip address 172.16.0.1 255.255.0.0
[PE1-Ethernet1/0/0.1] quit
[PE1] interface ethernet 1/0/0.2
[PE1-Ethernet1/0/0.2] ip binding vpn-instance vpn-instance3
[PE1-Ethernet1/0/0.2] ip address 172.17.0.1 255.255.0.0
[PE1-Ethernet1/0/0.2] quit
```

# Configure loopback interface.

```
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 11.1.1.1 255.255.255.255
[PE1-LoopBack0] quit
```

# Set up MP-IBGP adjacency between PEs to exchange intra-PE VPN routing information, and activate MP-IBGP peer in VPNv4 address family view.

```
[PE1] bgp 100
[PE1-bgp] group 22
[PE1-bgp] peer 22.1.1.1 connect-interface loopback 0
[PE1-bgp] group 33
[PE1-bgp] peer 33.1.1.1 connect-interface loopback 0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer 22 enable
[PE1-bgp-af-vpn] peer 22.1.1.1 group 22
[PE1-bgp-af-vpn] peer 33 enable
[PE1-bgp-af-vpn] peer 33.1.1.1 group 33
[PE1-bgp-af-vpn] quit
```

2) Configure PE2

# Create a VPN-instance on PE2, redistribute VPN routing information of VPN-target 100:2 and advertise VPN routing information of VPN-target 100:1.

```
[PE2] ip vpn-instance vpn-instance1
[PE2-vpn- vpn-instance1] route-distinguisher 100:1
[PE2-vpn- vpn-instance1] vpn-target 100:1 export-extcommunity
[PE2-vpn- vpn-instance1] vpn-target 100:2 import-extcommunity
[PE2-vpn- vpn-instance1] quit
```

# Set up EBGP adjacency between PE2 and CE2, redistribute intra-CE2 VPN routes learned into MBGP VPN-instance address family.

```
[PE2] bgp 100
[PE2-bgp] group 172 external
[PE2-bgp] ipv4-family vpn-instance vpn-instance1
[PE2-bgp-af-vpn-instance] peer 172.15.1.1 group 172 as-number 65001
[PE2-bgp-af-vpn-instance] import-route static
[PE2-bgp-af-vpn-instance] import-route direct
[PE2-bgp-af-vpn-instance] quit
[PE2-bgp] quit
```

# Bind the interface connecting PE2 and CE2 with VPN-instance 1.

```
[PE2] interface ethernet 1/0/0
[PE2-Ethernet1/0/0] ip binding vpn-instance vpn-instance1
[PE2-Ethernet1/0/0] ip address 172.15.0.1 255.255.0.0
[PE2-Ethernet1/0/0] quit
```

# Configure loopback interface.

```
[PE2] interface loopback 0
[PE2-LoopBack0] ip address 22.1.1.1 255.255.255.255
[PE2-LoopBack0] quit
```

# Set up MP-IBGP adjacency between PE2 and PE1 to exchange intra-PE VPN routing information, and activate MP-IBGP peer in VPNv4 address family view.

```
[PE2] bgp 100
[PE2] group 11
[PE2-bgp] peer 11.1.1.1 connect-interface loopback 0
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpn] peer 11 enable
[PE2-bgp-af-vpn] peer 11.1.1.1 group 11
[PE2-bgp-af-vpn] quit
[PE2-bgp] quit
```

3) Configure PE3

# Create a VPN-instance on PE3, redistribute VPN routing information of VPN-target 100:2 and advertise VPN routing information of VPN-target 100:1.

```
[PE3] ip vpn-instance vpn-instance2
[PE3-vpn- vpn-instance2] route-distinguisher 100:1
[PE3-vpn- vpn-instance2] vpn-target 100:1 export-extcommunity
[PE3-vpn- vpn-instance2] vpn-target 100:2 import-extcommunity
[PE3-vpn- vpn-instance2] quit
```

# Set up MP-EBGP adjacency between PE3 and CE3 to redistribute intra-CE3 VPN routes learned into MBGP VPN-instance address family.

```
[PE3] bgp 100
[PE3-bgp] group 172 external
[PE3-bgp] ipv4-family vpn-instance vpn-instance1
[PE3-bgp-af-vpn-instance] peer 172.18.1.1 group 172 as-number 65001
[PE3-bgp-af-vpn-instance] import-route static
[PE3-bgp-af-vpn-instance] import-route direct
[PE3-bgp-af-vpn-instance] quit
[PE3-bgp] quit
```

# Bind the interface connecting PE3 and CE3 with VPN-instance 2.

```
[PE3] interface ethernet 1/0/0
[PE3-Ethernet1/0/0] ip binding vpn-instance vpn-instance2
[PE3-Ethernet1/0/0] ip address 172.18.0.1 255.255.0.0
[PE3-Ethernet1/0/0] quit
```

# Configure loopback interface.

```
[PE3] interface loopback 0
[PE3-LoopBack0] ip address 33.1.1.1 255.255.255.255
[PE3-LoopBack0] quit
```

# Set up MP-IBGP adjacency between PE3 and PE1 to exchange intra-PE VPN routing information, and activate MP-IBGP peer in VPNv4 address family view.

```
[PE3] bgp 100
```

```
[PE3-bgp] group 11
[PE3-bgp] peer 11.1.1.1 connect-interface loopback 0
[PE3-bgp] ipv4-family vpnv4
[PE3-bgp-af-vpn] peer 11 enable
[PE3-bgp-af-vpn] peer 11.1.1.1 group 11
[PE3-bgp-af-vpn] quit
[PE3-bgp] quit
```

3.4.5 Configuring CE Dual-Home

I. Network requirements

For the applications that require high robustness of network, you may use CE dual-home networking mode.

CE1 and CE2 are respectively connected to PE1 and PE2 to achieve dual-homing. Three PEs are also connected to each other as back links. CE2 and CE4 are not in dual-home mode, and only connected to one PE.

CE1 and CE3 are in one VPN, and CE2 and CE4 are in another VPN. Two VPNs cannot access each other.

II. Network diagram

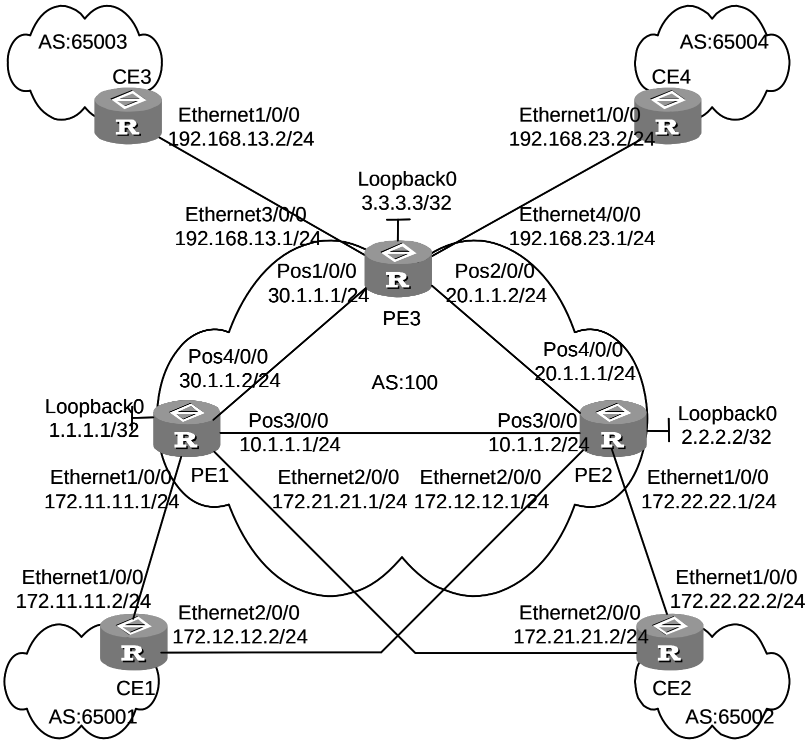


Figure 3-17 CE dual-home network diagram

III. Configuration procedure

Note:

The configuration of CE router is omitted in this case and you can refer to 3.4.1 Configuring Integrated BGP/MPLS VPN.

1) Configure PE1

# Configure two VPN-instances 1.1 and 1.2 respectively for CE1 and CE2 on PE1, set different VPN-targets for them.

```
[PE1] ip vpn-instance vpn-instance1.1
[PE1-vpn- vpn-instance1.1] route-distinguisher 1.1.1.1:1
[PE1-vpn- vpn-instance1.1] vpn-target 1.1.1.1:1
[PE1-vpn- vpn-instance1.1] vpn-target 2.2.2.2:1 import-extcommunity
[PE1-vpn- vpn-instance1.1] vpn-target 3.3.3.3:1 import-extcommunity
[PE1-vpn- vpn-instance1.1] quit
[PE1] ip vpn-instance vpn-instance1.2
[PE1-vpn- vpn-instance1.2] route-distinguisher 1.1.1.1:2
[PE1-vpn- vpn-instance1.2] vpn-target 1.1.1.1:2
[PE1-vpn- vpn-instance1.2] vpn-target 2.2.2.2:2 import-extcommunity
[PE1-vpn- vpn-instance1.2] vpn-target 3.3.3.3:2 import-extcommunity
[PE1-vpn- vpn-instance1.2] quit
```

# Set up EBGP adjacency between PE1 and CE1, redistribute intra-CE1 VPN routes learned into VPN-instance 1.1.

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpn-instance1.1
[PE1-bgp-af-vpn-instance] group 17211 external
[PE1-bgp-af-vpn-instance] peer 172.11.11.2 group 17211 as-number 65001
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] import-route static
[PE1-bgp-af-vpn-instance] quit
[PE1-bgp] quit
```

# Set up EBGP adjacency between PE1 and CE2, redistribute intra-CE2 VPN routes learned into VPN-instance 1.2.

```
[PE1-bgp] group 17221
[PE1-bgp] ipv4-family vpn-instance vpn-instance1.2
[PE1-bgp-af-vpn-instance] peer 172.21.21.2 group 17221 as-number 65002
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] import-route static
```

```
[PE1-bgp-af-vpn-instance] quit
[PE1-bgp] quit
```

# Bind the interface connecting PE1 and CE1 with VPN-instance 1.1 and interface connecting PE1 and CE2 with VPN-instance 1.2.

```
[PE1] interface ethernet 1/0/0
[PE1-Ethernet1/0/0] ip binding vpn-instance vpn-instance1.1
[PE1-Ethernet1/0/0] ip address 172.11.11.1 255.255.255.0
[PE1-Ethernet1/0/0] quit
[PE1] interface ethernet 2/0/0
[PE1-Ethernet2/0/0] ip binding vpn-instance vpn-instance1.2
[PE1-Ethernet2/0/0] ip address 172.21.21.1 255.255.255.0
[PE1-Ethernet2/0/0] quit
```

# Configure loopback interface.

```
[PE1] interface loopback 0
[PE1-LoopBack0] ip address 1.1.1.1 255.255.255.255
[PE1-LoopBack0] quit
```

# Configure MPLS basic capacity, enable LDP on the interface connecting PE1 and PE2 and the interface connecting PE1 and PE3.

```
[PE1] mpls lsr-id 1.1.1.1
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface Serial 3/0/0
[PE1-Serial3/0/0] mpls ldp enable
[PE1-Serial3/0/0] ip address 10.1.1.1 255.255.255.0
[PE1-Serial3/0/0] interface Serial 4/0/0
[PE1-Serial4/0/0] mpls ldp enable
[PE1-Serial4/0/0] ip address 30.1.1.2 255.255.255.0
[PE1-Serial4/0/0] quit
```

# Enable OSPF on the interface connecting PE1 and PE2 and the interface connecting PE1 and PE3 and the loopback interface, to achieve intra-PE communication.

```
[PE1] router id 1.1.1.1
[PE1] ospf
[PE1-ospf] area 0
[PE1-ospf-area-0.0.0.0] network 1.1.1.1 0.0.0.0
[PE1-ospf-area-0.0.0.0] network 30.1.1.2 0.0.0.255
[PE1-ospf-area-0.0.0.0] network 10.1.1.1 0.0.0.255
[PE1-ospf-area-0.0.0.0] quit
[PE1-ospf] quit
```

# Set up MP-IBGP adjacency between PEs to exchange intra-PE VPN routing information, activate MP-IBGP peer in VPNv4 address family view.

```
[PE1] bgp 100
[PE1-bgp] group 2
[PE1-bgp] peer 2.2.2.2 group 2
[PE1-bgp] peer 2.2.2.2 connect-interface loopback 0
[PE1-bgp] group 3
[PE1-bgp] peer 3.3.3.3 group 3
[PE1-bgp] peer 3.3.3.3 connect-interface loopback 0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer 2 enable
[PE1-bgp-af-vpn] peer 2.2.2.2 group 2
[PE1-bgp-af-vpn] peer 3 enable
[PE1-bgp-af-vpn] peer 3.3.3.3 group 3
[PE1-bgp-af-vpn] quit
```

2) Configure PE2

Note:

The configuration of PE2 is similar to that of PE1, so only VPN-instance configuration is detailed here.

# Create two VPN-instances 2.1 and 2.2 respectively for CE1 and CE2 on PE2, configure different VPN-targets for them.

```
[PE2] ip vpn-instance vpn-instance2.1
[PE2-vpn- vpn-instance2.1] route-distinguisher 2.2.2.2:1
[PE2-vpn- vpn-instance2.1] vpn-target 2.2.2.2:1
[PE2-vpn- vpn-instance2.1] vpn-target 1.1.1.1:1 import-extcommunity
[PE2-vpn- vpn-instance2.1] vpn-target 3.3.3.3:1 import-extcommunity
[PE2-vpn- vpn-instance2.1] quit
[PE2] ip vpn-instance vpn-instance2.2
[PE2-vpn- vpn-instance2.2] route-distinguisher 2.2.2.2:2
[PE2-vpn- vpn-instance2.2] vpn-target 2.2.2.2:2
[PE2-vpn- vpn-instance2.2] vpn-target 1.1.1.1:2 import-extcommunity
[PE2-vpn- vpn-instance2.2] vpn-target 3.3.3.3:2 import-extcommunity
[PE2-vpn- vpn-instance2.2] quit
```

# Set up EBGP adjacency between PE2 and CE1, redistribute intra-CE1 VPN routes learned into VPN-instance2.1.

```
[PE2] bgp 100
[PE2-bgp] ipv4-family vpn-instance vpn-instance2.1
[PE2-bgp-af-vpn-instance] group 17212 external
[PE2-bgp-af-vpn-instance] peer 172.12.12.2 group 17212 as-number 65001
```

```
[PE2-bgp-af-vpn-instance] import-route direct
[PE2-bgp-af-vpn-instance] import-route static
[PE2-bgp-af-vpn-instance] quit
```

# Set up EBGP adjacency between PE2 and CE2, redistribute intra-CE2 VPN routes learned into VPN-instance2.2.

```
[PE2-bgp] ipv4-family vpn-instance vpn-instance2.2
[PE2-bgp-af-vpn-instance] group 17222 external
[PE2-bgp-af-vpn-instance] peer 172.22.22.2 group 17222 as-number 65002
[PE2-bgp-af-vpn-instance] import-route direct
[PE2-bgp-af-vpn-instance] import-route static
[PE2-bgp-af-vpn-instance] quit
[PE2-bgp] quit
```

# Bind the interface connecting PE2 and CE1 with VPN-instance 2.1 and the interface connecting PE2 and CE2 with VPN-instance 2.2.

```
[PE2] interface ethernet 2/0/0
[PE2-Ethernet2/0/0] ip binding vpn-instance vpn-instance2.1
[PE2-Ethernet2/0/0] ip address 172.12.12.1 255.255.255.0
[PE2-Ethernet2/0/0] quit
[PE2] interface ethernet 1/0/0
[PE2-Ethernet1/0/0] ip binding vpn-instance vpn-instance2.2
[PE2-Ethernet1/0/0] ip address 172.22.22.1 255.255.255.0
[PE2-Ethernet1/0/0] quit
```

3) Configure PE3

Note:

The configuration of PE3 is similar to that of PE1, so only VPN-instance configuration is detailed here.

# Create two VPN-instances 3.1 and 3.2 respectively for CE3 and CE4 on PE3, configure different VPN-targets for them.

```
[PE3] ip vpn-instance vpn-instance3.1
[PE3-vpn- vpn-instance3.1] route-distinguisher 3.3.3.3:1
[PE3-vpn- vpn-instance3.1] vpn-target 3.3.3.3:1
[PE3-vpn- vpn-instance3.1] vpn-target 1.1.1.1:1 import-extcommunity
[PE3-vpn- vpn-instance3.1] vpn-target 2.2.2.2:1 import-extcommunity
[PE3-vpn- vpn-instance3.1] quit
[PE3] ip vpn-instance vpn-instance3.2
[PE3-vpn- vpn-instance3.2] route-distinguisher 3.3.3.3:2
[PE3-vpn- vpn-instance3.2] vpn-target 3.3.3.3:2
```

```
[PE3-vpn- vpn-instance3.2] vpn-target 1.1.1.1:2 import-extcommunity
[PE3-vpn- vpn-instance3.2] vpn-target 2.2.2.2:2 import-extcommunity
[PE3-vpn- vpn-instance3.2] quit
```

# Set up EBGP adjacency between PE3 and CE3, redistribute intra-CE3 VPN routes learned into VPN-instance3.1.

```
[PE3] bgp 100
[PE3-bgp] ipv4-family vpn-instance vpn-instance3.1
[PE3-bgp-af-vpn-instance] group 192 external
[PE3-bgp-af-vpn-instance] peer 192.168.13.2 group 192 as-number 65003
[PE3-bgp-af-vpn-instance] import-route direct
[PE3-bgp-af-vpn-instance] import-route static
[PE3-bgp-af-vpn-instance] quit
[PE3-bgp] quit
```

# Set up EBGP adjacency between PE3 and CE4, redistribute intra-CE4 VPN routes learned into VPN-instance3.2.

```
[PE3-bgp] ipv4-family vpn-instance vpn-instance3.2
[PE3-bgp-af-vpn-instance] group 232 external
[PE3-bgp-af-vpn-instance] peer 192.168.23.2 group 232 as-number 65004
[PE3-bgp-af-vpn-instance] import-route direct
[PE3-bgp-af-vpn-instance] import-route static
[PE3-bgp-af-vpn-instance] quit
[PE3-bgp] quit
```

# Bind the interface connecting PE3 and CE3 with VPN-instance3.1 and the interface connecting PE3 and CE4 with VPN-instance 3.2.

```
[PE3] interface ethernet 3/0/0
[PE3-Ethernet3/0/0] ip binding vpn-instance vpn-instance3.1
[PE3-Ethernet3/0/0] ip address 192.168.13.1 255.255.255.0
[PE3-Ethernet3/0/0] quit
[PE3] interface ethernet 4/0/0
[PE3-Ethernet4/0/0] ip binding vpn-instance vpn-instance3.2
[PE3-Ethernet4/0/0] ip address 192.168.23.1 255.255.255.0
[PE3-Ethernet4/0/0] quit
```

3.4.6 Configuring Multi-Role Hosts

I. Network requirements

A company provides VPN service with BGP/MPLS VPN.

The interface Serial1/0/0 connecting PE1 and CE1 is bound with VPN1 and the interface Serial0/0/0 connecting PE2 and CE2 is bound with VPN2.

PC1 is accessed into the VPN1 and VPN2 through CE1. The IP address for PC1 is 100.1.1.2.

Note:

In the case the configuration is focused on this point:

With proper configuration of static route and routing policy, PC1 can access packets in different VPNs and search routes in different VPN-instances.

II. Network diagram

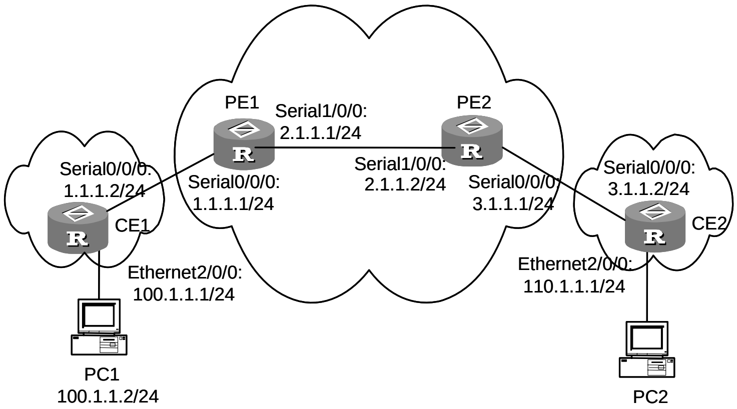


Figure 3-18 Multi-role host network diagram

III. Configuration procedure

1) Configure CE1.

# Configure a default route to PE1 on CE1.

```
[CE1] ip route-static 0.0.0.0 0 1.1.1.1
```

2) Configure PE1

# Configure two VPN-instances respectively for VPN1 and VPN2 on PE1, set different VPN-targets for them.

```
[PE1] ip vpn-instance vpn1
[PE1-vpn- vpn1] route-distinguisher 100:1
[PE1-vpn- vpn1] vpn-target 100:1 both
[PE1-vpn- vpn1] quit
[PE1] ip vpn-instance vpn2
[PE1-vpn- vpn2] route-distinguisher 100:2
[PE1-vpn- vpn2] vpn-target 100:2 both
[PE1-vpn- vpn2] quit
```

# Bind the interface connecting PE1 and CE1 with VPN 1.

```
[PE1] interface serial0/0/0
[PE1-Serial0/0/0] ip binding vpn-instance vpn1
[PE1-Serial0/0/0] ip address 1.1.1.1 255.255.255.0
[PE1-Serial0/0/0] quit
```

# Configure static route, so that PC1 can access the packets returned from VPN2 and find correct route to PC1 in the VPN-instance for VPN1.

```
[PE1] ip route-static vpn-instance vpn2 100.1.0.0 16 vpn-instance vpn1 1.1.1.2
```

# Define policy routing, allowing the router to search private routes within VPN1 and VPN2 for packets sent by PC1.

```
[PE1] acl number 3101
[PE1-acl-adv-3101] rule 0 permit ip vpn-instance vpn1 source 100.1.1.2 0
[PE1-acl-adv-3101] quit
[PE1] route-policy aaa permit node 10
[PE1-route-policy] if-match acl 3101
[PE1-route-policy] apply access-vpn vpn-instance vpn2
[PE1-route-policy] quit
```

# Enable routing policy at the interface Serial0/0/0.

```
[PE1] interface serial0/0/0
[PE1-Serial0/0/0] ip policy route-policy aaa
```

3.4.7 Configuring HoVPN

I. Network requirements

For those VPNs that have distinct hierarchy, an MPLS VPN covering a province and its cities. For example, incorporating the backbone network at the province level and the networks at the city level into a single MPLS VPN imposes a high requirement in performance on the equipment on the entire network, in the event that the network topology size is large. However, the requirement in equipment performance can become lower if this MPLS VPN is separated into two VPNs, the network at the province level and the network at the city level, for example.

SPE acts as a PE on the network at the province level, and is connected with a downstream MPLS VPN at the city level. UPE acts as a PE on the network at the city level and provide access service for the VPN clients which are normally low-end routers.

II. Network diagram

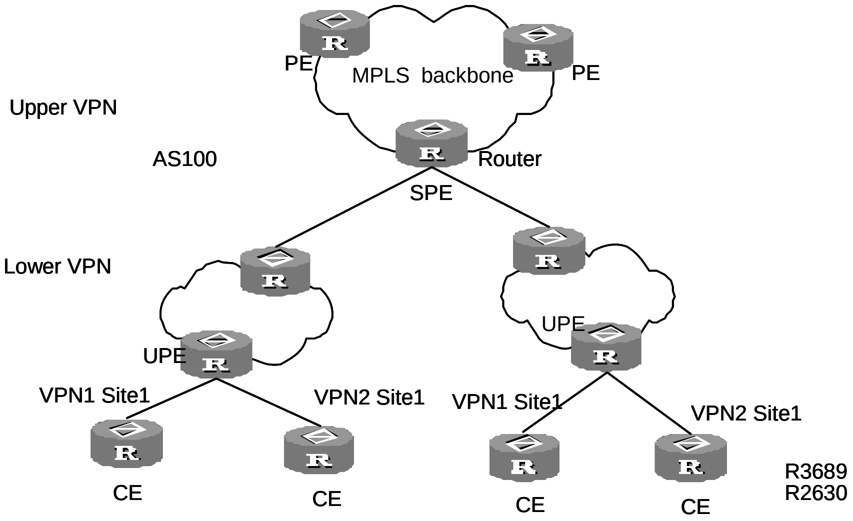


Figure 3-19 Hierarchical BGP/MPLS VPN

III. Configuration procedure

📖 **Note:**

This case only illustrates the configurations concerned with PEs in a hierarchical BGP/MPLS VPN.

---

1) Configure SPE

# Configure the basic MPLS capabilities.

```
[SPE] mpls lsr-id 1.0.0.2
[SPE] mpls
[SPE-mpls] mpls ldp
```

# Configure VPN-INSTANCE

```
[SPE] ip vpn-instance vpn1
[SPE-vpn-vpn1] route-distinguisher 100:1
[SPE-vpn-vpn1] vpn-target 100:1 both
```

# Configure interfaces (So far as a PE router concerned, its LOOPBACK 0 interface must be assigned with a host address of 32-bit mask.

```
[SPE] interface serial2/0/0
[SPE-Serial2/0/0] ip address 10.0.0.1 255.0.0.0
[SPE-Serial2/0/0] mpls
[SPE-Serial2/0/0] mpls ldp enable
[SPE] interface loopback0
```

```
[SPE-LoopBack 0] ip address 1.0.0.2 255.255.255.255
```

# Configure BGP

```
[SPE] bgp 100
[SPE-bgp] ipv4-family vpn-instance vpna
[SPE--bgp-af-vpn-instance] group 1
[SPE--bgp-af-vpn-instance] peer 1.0.0.1 group 1 as-number 100
[SPE--bgp-af-vpn-instance] peer 1.0.0.1 default-originate vpn1
[SPE--bgp-af-vpn-instance] peer 1.0.0.1 next-hop-local
[SPE--bgp-af-vpn-instance] quit
[SPE-bgp] quit
[SPE-bgp] ipv4-family vpnv4
[SPE-bgp-af-vpn] peer 1 enable
[SPE-bgp-af-vpn] peer 1.0.0.1 upe
[SPE-bgp-af-vpn] peer 1.0.0.1 default-route-advertise vpn-instance vpn1
[SPE-bgp-af-vpn] quit
[SPE-bgp] quit
```

# Configure OSPF

```
[SPE] ospf
[SPE-ospf] area 0
[SPE-ospf-area-0.0.0.0] network 0.0.0.0 0.0.0.0
[SPE-ospf-area-0.0.0.0] network 202.100.1.1 0.0.0.0
[SPE-ospf-area-0.0.0.0] import-route direct
```

2) Configure UPE

# Configure the basic MPLS capabilities.

```
[UPE] mpls lsr-id 1.0.0.1
[UPE] mpls
[UPE-mpls] mpls ldp
```

# Configure VPN-instance

```
[UPE] ip vpn-instance vpn1
[UPE-vpn-vpn1] route-distinguisher 100:1
[UPE-vpn-vpn1] vpn-target 100:1 both
```

# Configure interfaces

```
[UPE] interface serial2/0/0
[UPE-Serial2/0/0] ip address 10.0.0.2 255.0.0.0
[UPE-Serial2/0/0] mpls
[UPE-Serial2/0/0] mpls ldp enable
[UPE-Serial2/0/0] interface loopback0
[UPE-LoopBack 0] ip address 1.0.0.1 255.255.255.255
```

# Configure BGP

```
[UPE] bgp 100
[UPE-bgp] group 1
[UPE-bgp] peer 1.0.0.2 group 1
[UPE-bgp] peer 1.0.0.2 connect-interface loopback0
[UPE-bgp] ipv4-family vpnv4
[UPE-bgp-af-vpn] peer 1 enable
[UPE-bgp-af-vpn] peer 1.0.0.2 group 1
```

# Configure OSPF

```
[UPE] ospf
[UPE-ospf] area 0
[UPE-ospf-area-0.0.0.0] network 0.0.0.0 0.0.0.0
[UPE-ospf-area-0.0.0.0] import-route direct
[UPE-ospf-area-0.0.0.0] quit
```

3.4.8 Configuring OSPF Multi-Instance Sham Link

I. Network requirements

A company is connected into Wide Area Network (WAN) through routers with OSPF multi-instance enabled. OSPF is bound to the VPN1 and run between PE and CE. PEs are connected over MPLS VPN backbone network. A sham link is configured between PE1 and PE2, so that the traffic between CE1 and CE2 will be transferred along the backdoor links.

II. Network diagram

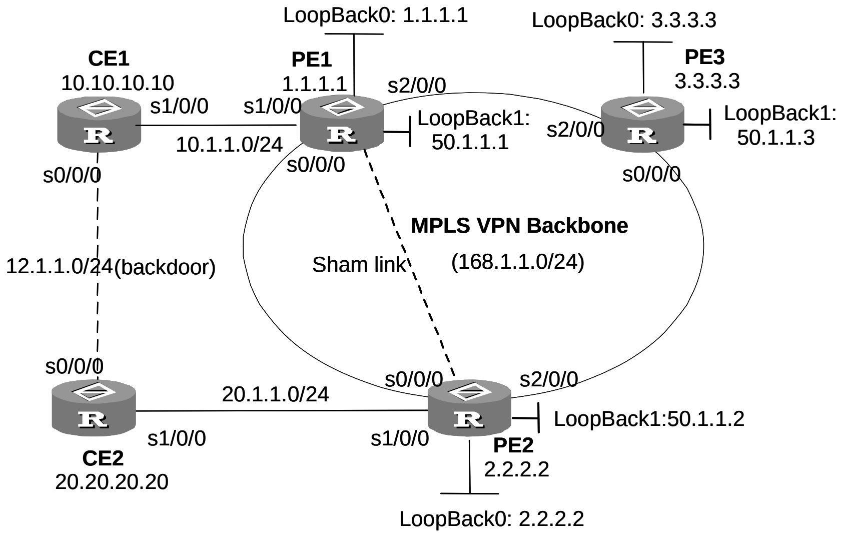


Figure 3-20 Network diagram for OSPF multi-instance

III. Configuration procedure

1) Configure PE1

# Enable MPLS and LDP.

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

# Configure VPN-instance.

```
[PE1] ip vpn-instance VPN1
[PE1-vpn-VPN1] route-distinguisher 2:1
[PE1-vpn-VPN1] vpn-target 100:1 export-extcommunity
[PE1-vpn-VPN1] vpn-target 100:1 import-extcommunity
```

# Configure the interface Serial0/0/0.

```
[PE1] interface Serial0/0/0
[PE1-Serial0/0/0] link-protocol ppp
[PE1-Serial0/0/0] ip address 168.1.12.1 255.255.255.0
[PE1-Serial0/0/0] ospf cost 1
[PE1-Serial0/0/0] mpls
[PE1-Serial0/0/0] mpls ldp enable
[PE1-Serial0/0/0] mpls ldp transport-ip interface
[PE1] interface Serial1/0/0
[PE1-Serial1/0/0] link-protocol ppp
[PE1-Serial1/0/0] ip binding vpn-instance VPN1
[PE1-Serial1/0/0] ip address 10.1.1.2 255.255.255.0
[PE1-Serial1/0/0] ospf cost 1
[PE1] interface Serial2/0/0
[PE1-Serial2/0/0] link-protocol ppp
[PE1-Serial2/0/0] ip address 168.1.13.1 255.255.255.0
[PE1-Serial2/0/0] ospf cost 1
[PE1-Serial2/0/0] mpls
[PE1-Serial2/0/0] mpls ldp enable
[PE1-Serial2/0/0] mpls ldp transport-ip interface
[PE1] interface loopback0
[PE1-LoopBack0] ip binding vpn-instance VPN1
[PE1-LoopBack0] ip address 1.1.1.1 255.255.255.255
[PE1] interface loopback1
[PE1-LoopBack1] ip address 50.1.1.1 255.255.255.255
```

# Configure BGP peer.

```
[PE1] bgp 100
[PE1-bgp] undo synchronization
[PE1-bgp] group fc internal
```

```
[PE1-bgp] peer 2.2.2.2 group fc
[PE1-bgp] peer 2.2.2.2 connect-interface LoopBack1
[PE1-bgp] peer 3.3.3.3 group fc
[PE1-bgp] peer 3.3.3.3 connect-interface LoopBack1
```

# Configure BGP to redistribute OSPF and directly connected routes.

```
[PE1-bgp] ipv4-family vpn-instance vpn1
[PE1-bgp-af-vpn-instance] import-route ospf 100
[PE1-bgp-af-vpn-instance] import-route ospf-ase 100
[PE1-bgp-af-vpn-instance] import-route ospf-nssa 100
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] undo synchronization
```

# Create a peer group in MBGP and activate the group.

```
[PE1-bgp-af-vpn] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer fc enable
[PE1-bgp-af-vpn] peer fc advertise-community
[PE1-bgp-af-vpn] peer 2.2.2.2 group fc
[PE1-bgp-af-vpn] peer 3.3.3.3 group fc
```

# Bind an OSPF process to the VPN-instance.

```
[PE1] ospf 100 router-id 1.1.1.1 vpn-instance VPN1
[PE1-ospf-100] import-route bgp
[PE1-ospf-100] area 0.0.0.1
[PE1-ospf-100-area-0.0.0.1] network 10.1.1.0  0.0.0.255
```

# Configure sham link.

```
[PE1-ospf-100-area-0.0.0.1] sham-link 1.1.1.1 2.2.2.2
```

# Configure static routes to PE2 and PE3.

```
[PE1] ip route-static 50.1.1.2 255.255.255.255 168.1.12.2
[PE1] ip route-static 50.1.1.3 255.255.255.255 168.1.13.3
```

2) Configure PE2

# Enable MPLS and LDP.

```
[PE2] mpls lsr-id 2.2.2.2
[PE2] mpls
[PE2] mpls ldp
```

# Configure the VPN-instance VPN1.

```
[PE2] ip vpn-instance VPN1
[PE2-vpn-VPN1] route-distinguisher 2:1
[PE2-vpn-VPN1] vpn-target 100:1 export-extcommunity
[PE2-vpn-VPN1] vpn-target 100:1 import-extcommunity
```

# Configure interface Serial0/0/0.

```
[PE2] interface Serial0/0/0
[PE2-Serial0/0/0] link-protocol ppp
[PE2-Serial0/0/0] ip address 168.1.12.2 255.255.255.0
[PE2-Serial0/0/0] ospf cost 1
[PE2-Serial0/0/0] mpls
[PE2-Serial0/0/0] mpls ldp enable
[PE2-Serial0/0/0] mpls ldp transport-ip interface
[PE2] interface Serial1/0/0
[PE2-Serial1/0/0] link-protocol ppp
[PE2-Serial1/0/0] ip binding vpn-instance VPN1
[PE2-Serial1/0/0] ip address 20.1.1.2 255.255.255.0
[PE2-Serial1/0/0] ospf cost 1
[PE2] interface Serial2/0/0
[PE2-Serial2/0/0] link-protocol ppp
[PE2-Serial2/0/0] ip address 168.1.23.2 255.255.255.0
[PE2-Serial2/0/0] ospf cost 1
[PE2-Serial1/0/0] mpls
[PE2-Serial1/0/0] mpls ldp enable
[PE2-Serial1/0/0] mpls ldp transport-ip interface
[PE2] interface LoopBack0
[PE2- LoopBack0] ip binding vpn-instance VPN1
[PE2- LoopBack0] ip address 2.2.2.2 255.255.255.255
[PE2] interface LoopBack1
[PE2- LoopBack1] ip address 50.1.1.2 255.255.255.255
```

# Configure BGP.

```
[PE2] bgp 100
[PE2-bgp-100] undo synchronization
[PE2-bgp-100] group fc internal
[PE2-bgp-100] peer 50.1.1.1 group fc
[PE2-bgp-100] peer 50.1.1.1 connect-interface LoopBack1
[PE2-bgp-100] peer 50.1.1.3 group fc
[PE2-bgp-100] peer 50.1.1.3 connect-interface LoopBack1
```

# Redistribute OSPF routes and directly connected routes for the VPN-instance.

```
[PE2-bgp] ipv4-family vpn-instance VPN1
[PE2-bgp-af-vpn-instance] import-route direct
[PE2-bgp-af-vpn-instance] import-route ospf-nssa 100
[PE2-bgp-af-vpn-instance] import-route ospf-ase 100
[PE2-bgp-af-vpn-instance] import-route ospf 100
[PE2-bgp-af-vpn-instance] undo synchronization
```

# MBGP enables peer.

```
[PE2-bgp-af-vpn] ipv4-family vpnv4
```

```
[PE2-bgp-af-vpn] peer fc enable
[PE2-bgp-af-vpn] peer fc advertise-community
[PE2-bgp-af-vpn] peer 50.1.1.1 group fc
[PE2-bgp-af-vpn] peer 50.1.1.3 group fc
```

# OSPF redistributes BGP routes and directly connected routes.

```
[PE2] ospf 100 router-id 2.2.2.2 vpn-instance VPN1
[PE2-ospf-100] import-route bgp
[PE2-ospf-100] import-route static
[PE2-ospf-100] area 0.0.0.1
[PE2-ospf-100] network 20.1.1.0 0.0.0.255
```

# Configure a sham link.

```
[PE2-ospf-100] sham-link 2.2.2.2 1.1.1.1
```

# Configure static routes to PE1 and PE3.

```
[PE2] ip route-static 50.1.1.1 255.255.255.255 168.1.12.1
[PE2] ip route-static 50.1.1.3 255.255.255.255 168.1.23.3
```

3) Configure CE1

# Configure interface Serial 0/0/0.

```
[CE1] interface Serial0/0/0
[CE1-Serial0/0/0] link-protocol ppp
[CE1-Serial0/0/0] ip address 12.1.1.1 255.255.255.0
[CE1-Serial0/0/0] ospf cost 1
[CE1] interface Serial1/0/0
[CE1-Serial1/0/0] link-protocol ppp
[CE1-Serial1/0/0] ip address 10.1.1.1 255.255.255.0
[CE1-Serial1/0/0] ospf cost 1
```

# Configure OSPF.

```
[CE1] ospf 100 router-id 10.10.10.10
[CE1-ospf-100] import-route direct
[CE1-ospf-100] area 0.0.0.1
[CE1-ospf-100] network 10.1.1.0 0.0.0.255
[CE1-ospf-100] network 12.1.1.0 0.0.0.255
```

4) Configure CE2

# Configure the interface Serial0/0/0.

```
[CE2] interface Serial0/0/0
[CE2-Serial0/0/0] link-protocol ppp
[CE2-Serial0/0/0] ip address 12.1.1.2 255.255.255.0
[CE2-Serial0/0/0] ospf cost 1
[CE2] interface Serial1/0/0
[CE2-Serial1/0/0] link-protocol ppp
```

```
[CE2-Serial1/0/0] ip address 20.1.1.1 255.255.255.0
[CE2-Serial1/0/0] ospf cost 1
```

# Configure OSPF.

```
[CE2] ospf 100 router-id 20.20.20.20
[CE2-ospf-100] area 0.0.0.1
[CE2-ospf-100] network 12.1.1.0 0.0.0.255
[CE2-ospf-100] network 20.1.1.0 0.0.0.255
```

3.4.9 Configuring OSPF Multi-Instance CE

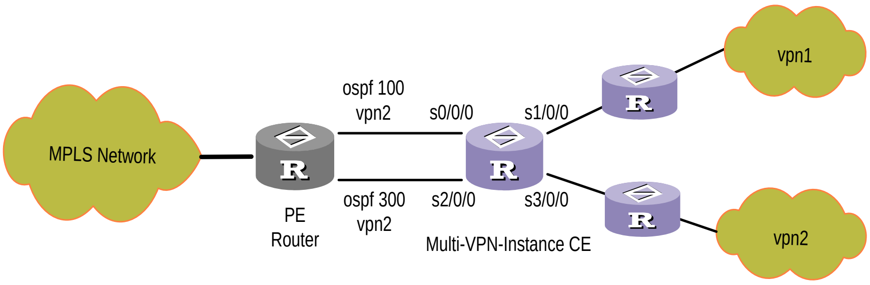


Figure 3-21 Network diagram for OSPF Multi-VPN-Instance CE

```
#
[CE] ip vpn-instance CE-VPN1
[CE-vpn- CE-VPN1] route-distinguisher 100:1
[CE-vpn- CE-VPN1] vpn-target 100:1 export-extcommunity
[CE-vpn- CE-VPN1] vpn-target 100:1 import-extcommunity
#
[CE] ip vpn-instance CE-VPN2
[CE-vpn- CE-VPN2] route-distinguisher 200:1
[CE-vpn- CE-VPN2] vpn-target 200:1 export-extcommunity
[CE-vpn- CE-VPN2] vpn-target 200:1 import-extcommunity
#
[CE] interface Serial0/0/0
[CE-Serial 0/0/0] link-protocol ppp
[CE-Serial 0/0/0] ip binding vpn-instance CE-VPN1
[CE-Serial 0/0/0] ip address 10.1.1.2 255.255.255.0
#
[CE] interface Serial1/0/0
[CE-Serial1/0/0] link-protocol ppp
[CE-Serial1/0/0] ip binding vpn-instance CE-VPN1
[CE-Serial1/0/0] ip address 10.2.1.2 255.255.255.0
[CE-Serial1/0/0] ospf cost 100
```

```
#
[CE] interface Serial2/0/0
[CE-Serial2/0/0] link-protocol ppp
[CE-Serial2/0/0] ip binding vpn-instance CE-VPN2
[CE-Serial2/0/0] ip address 20.1.1.2 255.255.255.0
#
[CE] interface Serial3/0/0
[CE-Serial3/0/0] link-protocol ppp
[CE-Serial3/0/0] ip binding vpn-instance CE-VPN2
[CE-Serial3/0/0] ip address 20.2.1.2 255.255.255.0
#
[CE] ospf 100 vpn-instance CE-VPN1
[CE-ospf-100] vpn-instance-capability simple
[CE-ospf-100] area 0.0.0.0
[CE-ospf-100-area-0.0.0.0] network 10.1.1.0 0.0.0.255
[CE-ospf-100-area-0.0.0.0] network 10.2.1.0 0.0.0.255
#
[CE] ospf 200 vpn-instance CE-VPN2
[CE-ospf-200] vpn-instance-capability simple
[CE-ospf-200] area 0.0.0.1
[CE-ospf-100-area-0.0.0.1] network 20.1.1.0 0.0.0.255
[CE-ospf-100-area-0.0.0.1] network 20.2.1.0 0.0.0.255
```

3.4.10 Configuring Inter-Provider Backbones Option A

I. Network requirements

CE1 and CE2 belong to the same VPN. CE1 accesses the network through PE1 in AS 100 and CE2 accesses the network through PE2 in AS 200.

Multi-AS BGP/MPLS VPN is implemented using Option A method. (That is, VPN-INSTANCE-to-VPN-INSTANCE method is used to manage VPN routes).

The MPLS backbone network in the same AS adopts OSPF as the IGP.

II. Network diagram

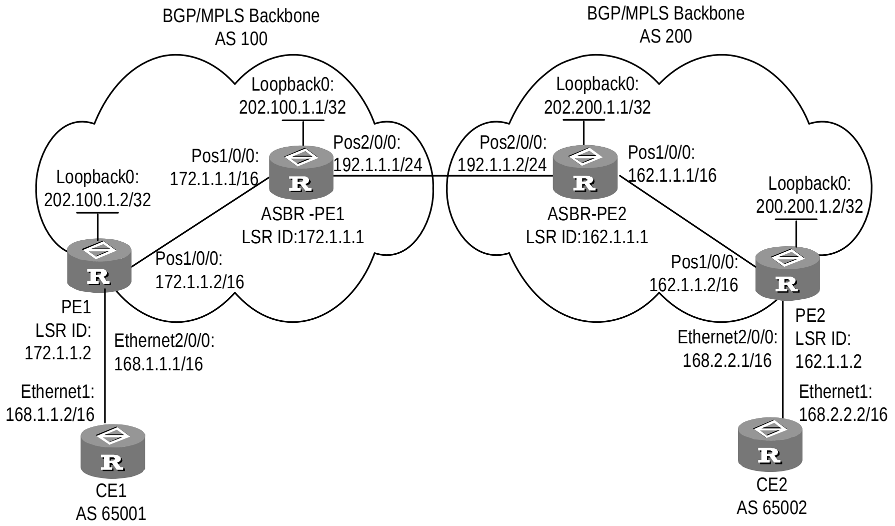


Figure 3-22 Network diagram for Inter-Provider Backbones

III. Configuration procedure

The configuration procedures include:

- Configuring OSPF on the MPLS backbone network
- Configuring basic MPLS capability on the MPLS backbone network
- Configuring VPN instances on PEs
- Configuring MP-BGP

They are introduced below in order.

1) Configuring OSPF on the MPLS backbone network to make PEs learn routes from each other

# Configure PE1.

```
[PE1] interface loopback0
[PE1-LoopBack0] ip address 202.100.1.2 255.255.255.255
[PE1-LoopBack0] quit
[PE1] interface pos1/0/0
[PE1-Pos1/0/0] ip address 172.1.1.2 255.255.0.0
[PE1-Pos1/0/0] quit
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 172.1.0.0 0.0.255.255
[PE1-ospf-1-area-0.0.0.0] network 202.100.1.2 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

# Configure ASBR-PE1.

```
[ASBR-PE1] interface loopback0
[ASBR-PE1-LoopBack 0] ip address 202.100.1.1 255.255.255.255
[ASBR-PE1-LoopBack 0] quit
[ASBR-PE1] interface pos1/0/0
[ASBR-PE1-Pos1/0/0] ip address 172.1.1.1 255.255.0.0
[ASBR-PE1-Pos1/0/0] quit
[ASBR-PE1] ospf
[ASBR-PE1-ospf-1] area 0
[ASBR-PE1-ospf-1-area-0.0.0.0] network 172.1.0.0 0.0.255.255
[ASBR-PE1-ospf-1-area-0.0.0.0] network 202.100.1.1 0.0.0.0
[ASBR-PE1-ospf-1-area-0.0.0.0] quit
[ASBR-PE1-ospf-1] quit
```

# Configure PE2.

```
[PE2] interface loopback0
[PE2-LoopBack0] ip address 202.200.1.2 255.255.255.255
[PE2-LoopBack0] quit
[PE2] interface pos1/0/0
[PE2-Pos1/0/0] ip address 162.1.1.2 255.255.0.0
[PE2-Pos1/0/0] quit
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 162.1.0.0 0.0.255.255
[PE2-ospf-1-area-0.0.0.0] network 202.200.1.2 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

# Configure ASBR-PE2.

```
[ASBR-PE2] interface loopback0
[ASBR-PE2-LoopBack0] ip address 202.200.1.1 255.255.255.255
[ASBR-PE2-LoopBack0] quit
[ASBR-PE2] interface pos1/0/0
[ASBR-PE2-Pos1/0/0] ip address 162.1.1.1 255.255.0.0
[ASBR-PE2-Pos1/0/0] quit
[ASBR-PE2] ospf
[ASBR-PE2-ospf-1] area 0
[ASBR-PE2-ospf-1-area-0.0.0.0] network 162.1.0.0 0.0.255.255
[ASBR-PE2-ospf-1-area-0.0.0.0] network 202.200.1.1 0.0.0.0
[ASBR-PE2-ospf-1-area-0.0.0.0] quit
[ASBR-PE2-ospf-1] quit
```

After the configuration, the OSPF neighbor relationship should be established between ASBR PE and the PEs of the same AS. Executing the **display ospf peer** command, you can find that the OSPF neighbor relationship is in Full state. PEs can learn Loopback addresses from each other.

The ping operation succeeds between ASBR-PE and other PEs in the same AS.

Take PE1 and ASBR-PE1 as an example:

```
[PE1] display ospf peer
                 OSPF Process 1 with Router ID 202.100.1.2
                                Neighbors
  Area 0 interface 172.1.1.2(Pos1/0/0)'s neighbor(s)
  RouterID: 202.100.1.1     Address: 172.1.1.1
        State: Full  Mode: Nbr is Slave  Priority: 1
        DR: None  BDR: None
        Dead timer expires in 40s
        Neighbor comes up for 00:01:32

[PE1] display ip routing-table
 Routing Table: public net
Destination/Mask   Protocol Pre  Cost    Nexthop         Interface
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
172.1.0.0/16       DIRECT   0    0       172.1.1.2       Pos1/0/0
172.1.1.1/32       DIRECT   0    0       172.1.1.1       Pos1/0/0
172.1.1.2/32       DIRECT   0    0       127.0.0.1       InLoopBack0
202.100.1.1/32     OSPF     10   1563    172.1.1.1       Pos1/0/0
202.100.1.2/32     DIRECT   0    0       127.0.0.1       InLoopBack0

[PE1] ping 202.100.1.1
  PING 202.100.1.1: 56  data bytes, press CTRL_C to break
    Reply from 202.100.1.1: bytes=56 Sequence=1 ttl=255 time=10 ms
    Reply from 202.100.1.1: bytes=56 Sequence=2 ttl=255 time=1 ms
    Reply from 202.100.1.1: bytes=56 Sequence=3 ttl=255 time=50 ms
    Reply from 202.100.1.1: bytes=56 Sequence=4 ttl=255 time=80 ms
    Reply from 202.100.1.1: bytes=56 Sequence=5 ttl=255 time=1 ms
  --- 202.100.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/28/80 ms

[ASBR-PE1] display ospf peer
                 OSPF Process 1 with Router ID 202.100.1.1
                                Neighbors
  Area 0 interface 172.1.1.1(Pos1/0/0)'s neighbor(s)
  RouterID: 202.100.1.2     Address: 172.1.1.2
        State: Full  Mode: Nbr is Master  Priority: 1
        DR: None  BDR: None
        Dead timer expires in 30s
        Neighbor comes up for 00:01:49

[ASBR-PE1] display ip routing-table
 Routing Table: public net
Destination/Mask   Protocol Pre  Cost     Nexthop         Interface
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
172.1.0.0/16       DIRECT   0    0        172.1.1.1       Pos1/0/0
172.1.1.1/32       DIRECT   0    0        127.0.0.1       InLoopBack0
172.1.1.2/32       DIRECT   0    0        172.1.1.2       Pos1/0/0
202.100.1.1/32     DIRECT   0    0        127.0.0.1       InLoopBack0
202.100.1.2/32     OSPF     10   1563     172.1.1.2       Pos1/0/0

[ASBR-PE1] ping 202.100.1.2
  PING 202.100.1.2: 56  data bytes, press CTRL_C to break
    Reply from 202.100.1.2: bytes=56 Sequence=1 ttl=255 time=10 ms
    Reply from 202.100.1.2: bytes=56 Sequence=2 ttl=255 time=10 ms
    Reply from 202.100.1.2: bytes=56 Sequence=3 ttl=255 time=10 ms
    Reply from 202.100.1.2: bytes=56 Sequence=4 ttl=255 time=60 ms
    Reply from 202.100.1.2: bytes=56 Sequence=5 ttl=255 time=10 ms
  --- 202.100.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 10/20/60 ms
```

2) Configuring basic MPLS capability on the MPLS backbone network to make the network forward VPN traffic

# Configure basic MPLS capability on PE1 and enable LDP on the interface connecting ASBR-PE1.

```
[PE1] mpls lsr-id 172.1.1.2
[PE1-mpls] lsp-trigger all
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface pos1/0/0
[PE1-Pos1/0/0] mpls
[PE1-Pos1/0/0] mpls ldp
[PE1-Pos1/0/0] quit
```

# Configure basic MPLS capability on ASBR-PE1 and enable LDP on the interface connecting PE1.

```
[ASBR-PE1] mpls lsr-id 172.1.1.1
[ASBR-PE1-mpls] lsp-trigger all
[ASBR-PE1-mpls] quit
[ASBR-PE1] mpls ldp
[ASBR-PE1-mpls-ldp] quit
[ASBR-PE1] interface pos1/0/0
[ASBR-PE1-Pos1/0/0] mpls
[ASBR-PE1-Pos1/0/0] mpls ldp enable
[ASBR-PE1-Pos1/0/0] quit
```

# Configure basic MPLS capability on ASBR-PE2 and enable LDP on the interface connecting PE2.

```
[ASBR-PE2] mpls lsr-id 162.1.1.1
[ASBR-PE2-mpls] lsp-trigger all
[ASBR-PE2-mpls] quit
[ASBR-PE2] mpls ldp
[ASBR-PE2-mpls-ldp] quit
[ASBR-PE2] interface pos1/0/0
[ASBR-PE2-Pos1/0/0] mpls
[ASBR-PE2-Pos1/0/0] mpls ldp enable
[ASBR-PE2-Pos1/0/0] quit
```

# Configure basic MPLS capability on PE2 and enable LDP on the interface connecting ASBR-PE2.

```
[PE2] mpls lsr-id 162.1.1.2
[PE2-mpls] lsp-trigger all
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] interface pos1/0/0
[PE2-Pos1/0/0] mpls
[PE2-Pos1/0/0] mpls ldp enable
[PE2-Pos1/0/0] quit
```

After you complete the configurations, the PEs and the ASBR-PEs in the same AS should be able to set up LDP neighborhood. Executing the **display mpls ldp session** command on the routers, you can find the Session State is “Operational” in the output. You do not need to enable MPLS on the interface connecting ASBR-PE1 and ASBR-PE2.

Take the display results on PE1 and ASBR-PE1 for example:

```
[PE1] display mpls ldp session
```

```
Displaying information about all sessions:
  Local LDP ID: 172.1.1.2:0;   Peer LDP ID: 172.1.1.1:0
  TCP Connection: 172.1.1.2 -> 172.1.1.1
  Session State: Operational
  Session Role: Active
  Session existed time: 3 minutes 32 seconds
  KeepAlive Packets Sent/Received: 11/11
  Negotiated Keepalive hold time: 60  Peer PV Limit: 0
  LDP Basic Discovery Source((A) means active):
  Pos1/0/0(A)

[ASBR-PE1] display mpls ldp session
Displaying information about all sessions:
  Local LDP ID: 172.1.1.1:0;   Peer LDP ID: 172.1.1.2:0
  TCP Connection: 172.1.1.1 <- 172.1.1.2
  Session State: Operational
  Session Role: Passive
  Session existed time: 4 minutes 37 seconds
  KeepAlive Packets Sent/Received: 14/14
  Negotiated Keepalive hold time: 60  Peer PV Limit: 0
  LDP Basic Discovery Source((A) means active):
  Pos1/0/0(A)
```

3) Configuring VPN instances on PEs and binding to the interfaces connecting to CEs

Note:

The VPN-Target attributes of VPN instances of ASBR-PE and PE in the same AS should match each other. In different ASs, the matching of VPN-Target attributes of PEs is unnecessary.

# Configure CE1.

```
[CE1] interface ethernet 1
[CE1-Ethernet1] ip address 168.1.1.2 255.255.0.0
[CE1-Ethernet1] quit
```

# Configure a VPN instance on PE1 and bind it to the interface connecting to CE1.

```
[PE1] ip vpn-instance vpna
[PE1-vpn-vpn-vpna] route-distinguisher 100:2
[PE1-vpn-vpn-vpna] vpn-target 100:1 both
[PE1-vpn-vpn-vpna] quit
```

```
[PE1] interface ethernet 2/0/0
[PE1-Ethernet2/0/0] ip binding vpn-instance vpna
[PE1-Ethernet2/0/0] ip address 168.1.1.1 255.255.0.0
[PE1-Ethernet2/0/0] quit
```

# Configure a VPN instance on ASBR-PE1 and bind it to the interface connecting to ASBR-PE2 (ASBR-PE1 regards ASBR-PE2 as its CE).

```
[ASBR-PE1] ip vpn-instance vpna
[ASBR-PE1-vpn-vpn-vpna] route-distinguisher 100:1
[ASBR-PE1-vpn-vpn-vpna] vpn-target 100:1 both
[ASBR-PE1-vpn-vpn-vpna] quit
[ASBR-PE1] interface pos 2/0/0
[ASBR-PE1-Pos2/0/0] ip binding vpn-instance vpna
[ASBR-PE1-Pos2/0/0] ip address 192.1.1.1 255.255.255.0
[ASBR-PE1-Pos2/0/0] quit
```

# Configure CE2.

```
[CE2] interface ethernet 1
[CE2-Ethernet1] ip address 168.2.2.2 255.255.0.0
[CE2-Ethernet1] quit
```

# Configure a VPN instance on PE2 and bind it to the interface connecting to CE2.

```
[PE2] ip vpn-instance vpna
[PE2-vpn-instance] route-distinguisher 200:2
[PE2-vpn-instance] vpn-target 100:1 both
[PE2-vpn-instance] quit
[PE2] interface ethernet 2/0/0
[PE2-Ethernet2/0/0] ip binding vpn-instance vpna
[PE2-Ethernet2/0/0] ip address 168.2.2.1 255.255.0.0
[PE2-Ethernet2/0/0] quit
```

# Configure a VPN instance on ASBR-PE2 and bind it to the interface connecting to ASBR-PE1 (ASBR-PE2 regards ASBR-PE1 as its CE).

```
[ASBR-PE2] ip vpn-instance vpna
[ASBR-PE2-vpn-vpn-vpna] route-distinguisher 200:1
[ASBR-PE2-vpn-vpn-vpna] vpn-target 100:1 both
[ASBR-PE2-vpn-vpn-vpna] quit
[ASBR-PE2] interface Pos 2/0/0
[ASBR-PE2-Pos2/0/0] ip binding vpn-instance vpna
[ASBR-PE2-Pos2/0/0] ip address 192.1.1.2 255.255.255.0
[ASBR-PE2-Pos2/0/0] quit
```

After the configuration, you can see the VPN instance configuration by executing the **display ip vpn-instance verbose** command on PEs.

Take the display results on PE1 and ASBR-PE1 as an example:

```
[PE1] display ip vpn-instance verbose
VPN-Instance : vpna
   No description
   Route-Distinguisher :
     100:2
   Interfaces :
     Ethernet2/0/0
   Export-ext-communities :
     100:1
   Import-ext-communities :
     100:1

[ASBR-PE1] display ip vpn-instance verbose
VPN-Instance : vpna
   No description
   Route-Distinguisher :
     100:1
   Interfaces :
     Pos2/0/0
   Export-ext-communities :
     100:1
   Import-ext-communities :
     100:1
```

The ping operations are successful to CEs on PEs, and successful between ASBR-PEs.

When pinging CE on PE, you need to specify the VPN to which the destination address belongs.

For example, ping ASBR-PE2 on ASBR-PE1:

```
[ASBR-PE1] ping -vpn-instance vpna 192.1.1.2
  PING 192.1.1.2: 56  data bytes, press CTRL_C to break
    Reply from 192.1.1.2: bytes=56 Sequence=1 ttl=255 time=10 ms
    Reply from 192.1.1.2: bytes=56 Sequence=2 ttl=255 time=10 ms
    Reply from 192.1.1.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 192.1.1.2: bytes=56 Sequence=4 ttl=255 time=1 ms
    Reply from 192.1.1.2: bytes=56 Sequence=5 ttl=255 time=60 ms
  --- 192.1.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/16/60 ms
```

Ping PE1 on CE1:

```
[CE1] ping 168.1.1.1
  PING 168.1.1.1: 56  data bytes, press CTRL_C to break
    Reply from 168.1.1.1: bytes=56 Sequence=1 ttl=255 time=1 ms
    Reply from 168.1.1.1: bytes=56 Sequence=2 ttl=255 time=60 ms
    Reply from 168.1.1.1: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 168.1.1.1: bytes=56 Sequence=4 ttl=255 time=60 ms
    Reply from 168.1.1.1: bytes=56 Sequence=5 ttl=255 time=10 ms
  --- 168.1.1.1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/26/60 ms
```

Ping CE1 on PE1:

```
[PE1] ping -vpn-instance vpna 168.1.1.2
  PING 168.1.1.2: 56  data bytes, press CTRL_C to break
    Reply from 168.1.1.2: bytes=56 Sequence=1 ttl=255 time=10 ms
    Reply from 168.1.1.2: bytes=56 Sequence=2 ttl=255 time=10 ms
    Reply from 168.1.1.2: bytes=56 Sequence=3 ttl=255 time=1 ms
    Reply from 168.1.1.2: bytes=56 Sequence=4 ttl=255 time=50 ms
    Reply from 168.1.1.2: bytes=56 Sequence=5 ttl=255 time=10 ms
  --- 168.1.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 1/16/50 ms
```

4) Configuring MP-BGP, establishing IBGP peer relationship between PEs, and establishing EBGP peer relationship between PE and CE

# Configure CE1.

```
[CE1] bgp 65001
[CE1-bgp] group 20 external
[CE1-bgp] peer 168.1.1.1 group 20 as-number 100
[CE1-bgp] quit
```

# Configure PE1 to establish EBGP peer relationship with CE1 and IBGP peer relationship with ASBR-PE1.

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpna
[PE1-bgp-af-vpn-instance] group 10 external
[PE1-bgp-af-vpn-instance] peer 168.1.1.2 group 10 as-number 65001
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] quit
[PE1-bgp] group 20
```

```
[PE1-bgp] peer 202.100.1.1 group 20
[PE1-bgp] peer 202.100.1.1 connect-interface loopback0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer 20 enable
[PE1-bgp-af-vpn] peer 202.100.1.1 group 20
[PE1-bgp-af-vpn] quit
[PE1-bgp] quit
```

# Configure ASBR-PE1 to establish EBGP peer relationship with ASBR-PE2 and IBGP peer relationship with PE1.

```
[ASBR-PE1] bgp 100
[ASBR-PE1-bgp] ipv4-family vpn-instance vpna
[ASBR-PE1-bgp-af-vpn-instance] group 10 external
[ASBR-PE1-bgp-af-vpn-instance] peer 192.1.1.2 group 10 as-number 200
[ASBR-PE1-bgp-af-vpn-instance] quit
[ASBR-PE1-bgp] group 20
[ASBR-PE1-bgp] peer 202.100.1.2 group 20
[ASBR-PE1-bgp] peer 202.100.1.2 connect-interface loopback0
[ASBR-PE1-bgp] ipv4-family vpnv4
[ASBR-PE1-bgp-af-vpn] peer 20 enable
[ASBR-PE1-bgp-af-vpn] peer 202.100.1.2 group 20
[ASBR-PE1-bgp-af-vpn] quit
[ASBR-PE1-bgp] quit
```

# Configure CE2.

```
[CE2] bgp 65002
[CE2-bgp] group 10 external
[CE2-bgp] peer 168.2.2.1 group 10 as-number 200
[CE2-bgp] quit
```

# Configure PE2 to establish EBGP peer relationship with CE2 and IBGP peer relationship with ASBR-PE2.

```
[PE2] bgp 200
[PE2-bgp] ipv4-family vpn-instance vpna
[PE2-bgp-af-vpn-instance] group 10 external
[PE2-bgp-af-vpn-instance] peer 168.2.2.2 group 10 as-number 65002
[PE2-bgp-af-vpn-instance] import-route direct
[PE2-bgp-af-vpn-instance] quit
[PE2-bgp] group 20
[PE2-bgp] peer 202.200.1.1 group 20
[PE2-bgp] peer 202.200.1.1 connect-interface loopback0
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpn] peer 20 enable
[PE2-bgp-af-vpn] peer 202.200.1.1 group 20
```

```
[PE2-bgp-af-vpn] quit
[PE2-bgp] quit
```

# Configure ASBR-PE2 to establish EBGP peer relationship with ASBR-PE1 and IBGP peer relationship with PE2.

```
[ASBR-PE2] bgp 200
[ASBR-PE2-bgp] ipv4-family vpn-instance vpna
[ASBR-PE2-bgp-af-vpn-instance] group 10 external
[ASBR-PE2-bgp-af-vpn-instance] peer 192.1.1.1 group 10 as-number 100
[ASBR-PE2-bgp-af-vpn-instance] quit
[ASBR-PE2-bgp] group 20
[ASBR-PE2-bgp] peer 202.200.1.2 group 20
[ASBR-PE2-bgp] peer 202.200.1.2 connect-interface loopback0
[ASBR-PE2-bgp] ipv4-family vpnv4
[ASBR-PE2-bgp-af-vpn] peer 20 enable
[ASBR-PE2-bgp-af-vpn] peer 202.200.1.2 group 20
[ASBR-PE2-bgp-af-vpn] quit
[ASBR-PE2-bgp] quit
```

After the configuration, you can find that the BGP peer relationship has been established in Established state between PEs and between PE and CE.

Take the display results on PE1 and ASBR-PE1 as an example:

```
[PE1] display bgp vpnv4 all peer
  Peer        AS-num Ver Queued-Tx    Msg-Rx    Msg-Tx    Up/Down  State
--------------------------------------------------------------------
168.1.1.2      65001  4         0         4         7   00:03:23 Established
202.100.1.1      100  4         0         1         1   00:03:14 Established

[ASBR-PE1] display bgp vpnv4 all peer
  Peer        AS-num Ver Queued-Tx    Msg-Rx    Msg-Tx    Up/Down  State
--------------------------------------------------------------------
192.1.1.2        200  4         0         5         6   00:03:38 Established
202.100.1.2      100  4         0         1         1   00:04:17 Established
```

CEs can learn interface routes from each other. CE1 and CE2 can be pinged successfully on each other.

```
[CE1] display ip routing-table
 Routing Table: public net
Destination/Mask   Protocol Pre  Cost   Nexthop         Interface
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
168.1.0.0/16       DIRECT   0    0      168.1.1.2       Ethernet1
168.1.1.2/32       DIRECT   0    0      127.0.0.1       InLoopBack0
168.2.0.0/16       BGP      256  0      168.1.1.1       Ethernet2/0/0
```

```
[PE1] display ip routing-table vpn-instance vpna
  vpna   Route Information
 Routing Table:  vpna   Route-Distinguisher:   100:2
Destination/Mask   Protocol Pre  Cost    Nexthop       Interface
168.1.0.0/16       DIRECT   0    0       168.1.1.1     Ethernet2/0/0
168.1.1.1/32       DIRECT   0    0       127.0.0.1     InLoopBack0
 VPN Routing Table:   Route-Distinguisher:   100:1
168.2.0.0/16       BGP      256  0       202.100.1.1   InLoopBack0

[ASBR-PE1] display ip routing-table vpn-instance vpna
  vpna   Route Information
 Routing Table:  vpna   Route-Distinguisher:   100:1
Destination/Mask   Protocol Pre  Cost   Nexthop         Interface
168.2.0.0/16       BGP      256  0      192.1.1.2       Pos2/0/0
192.1.1.0/24       DIRECT   0    0      192.1.1.1       Pos2/0/0
192.1.1.1/32       DIRECT   0    0      127.0.0.1       InLoopBack0
192.1.1.2/32       DIRECT   0    0      192.1.1.2       Pos2/0/0
 VPN Routing Table:   Route-Distinguisher:   100:2
168.1.0.0/16       BGP      256  0      202.100.1.2     InLoopBack0
[CE1] ping 168.2.2.2
  PING 168.2.2.2: 56  data bytes, press CTRL_C to break
    Reply from 168.2.2.2: bytes=56 Sequence=1 ttl=251 time=140 ms
    Reply from 168.2.2.2: bytes=56 Sequence=2 ttl=251 time=130 ms
    Reply from 168.2.2.2: bytes=56 Sequence=3 ttl=251 time=130 ms
    Reply from 168.2.2.2: bytes=56 Sequence=4 ttl=251 time=70 ms
    Reply from 168.2.2.2: bytes=56 Sequence=5 ttl=251 time=130 ms
  --- 168.2.2.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 70/120/140 ms

[CE2] ping 168.1.1.2
  PING 168.1.1.2: 56  data bytes, press CTRL_C to break
    Reply from 168.1.1.2: bytes=56 Sequence=1 ttl=251 time=130 ms
    Reply from 168.1.1.2: bytes=56 Sequence=2 ttl=251 time=190 ms
    Reply from 168.1.1.2: bytes=56 Sequence=3 ttl=251 time=70 ms
    Reply from 168.1.1.2: bytes=56 Sequence=4 ttl=251 time=130 ms
    Reply from 168.1.1.2: bytes=56 Sequence=5 ttl=251 time=190 ms
  --- 168.1.1.2 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
```

```
0.00% packet loss
round-trip min/avg/max = 70/142/190 ms
```

3.4.11 Configuring Inter-Provider Backbones Option B

I. Network requirements

CE1 and CE2 belong to the same VPN. CE1 accesses the network through PE1 in AS 100 and CE2 accesses the network through PE2 in AS 200.

Multi-AS BGP/MPLS VPN is implemented through Option B method. That is, VPN-IPv4 routes are advertised between ASBRs.

The MPLS backbone network in the same AS adopts OSPF as the IGP.

II. Network diagram

See Figure 3-22.

III. Configuration procedure

The configuration procedures include:

- Configuring OSPF on the MPLS backbone network
- Configuring basic MPLS capability on the MPLS backbone network
- Configuring VPN instances on PEs
- Configuring MP-BGP

Compared with Option A, Option B differs in the last two procedures.

1) Configuring OSPF on the MPLS backbone network to make PEs learn routes from each other

Note:

In this part:

- The configurations on PE1 and PE2 are the same as those in section 3.4.10 “Configuring Inter-Provider Backbones Option A”.
- Configuration of interface IP address between ASBR-PE1 and ASBR-PE2 is added.

# Configure PE1.

```
[PE1] interface loopback0
[PE1-LoopBack0] ip address 202.100.1.2 255.255.255.255
[PE1-LoopBack0] quit
[PE1] interface pos1/0/0
[PE1-Pos1/0/0] ip address 172.1.1.2 255.255.0.0
[PE1-Pos1/0/0] quit
[PE1] ospf
```

```
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 172.1.0.0 0.0.255.255
[PE1-ospf-1-area-0.0.0.0] network 202.100.1.2 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

# Configure ASBR-PE1.

```
[ASBR-PE1] interface loopback0
[ASBR-PE1-LoopBack 0] ip address 202.100.1.1 255.255.255.255
[ASBR-PE1-LoopBack 0] quit
[ASBR-PE1] interface pos1/0/0
[ASBR-PE1-Pos1/0/0] ip address 172.1.1.1 255.255.0.0
[ASBR-PE1-Pos1/0/0] quit
[ASBR-PE1] interface pos 2/0/0
[ASBR-PE1-Pos2/0/0] ip address 192.1.1.1 255.255.255.0
[ASBR-PE1-Pos2/0/0] quit
[ASBR-PE1] ospf
[ASBR-PE1-ospf-1] area 0
[ASBR-PE1-ospf-1-area-0.0.0.0] network 172.1.0.0 0.0.255.255
[ASBR-PE1-ospf-1-area-0.0.0.0] network 202.100.1.1 0.0.0.0
[ASBR-PE1-ospf-1-area-0.0.0.0] quit
[ASBR-PE1-ospf-1] quit
```

# Configure PE2.

```
[PE2] interface loopback0
[PE2-LoopBack0] ip address 202.200.1.2 255.255.255.255
[PE2-LoopBack0] quit
[PE2] interface pos1/0/0
[PE2-Pos1/0/0] ip address 162.1.1.2 255.255.0.0
[PE2-Pos1/0/0] quit
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 162.1.0.0 0.0.255.255
[PE2-ospf-1-area-0.0.0.0] network 202.200.1.2 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

# Configure ASBR-PE2.

```
[ASBR-PE2] interface loopback0
[ASBR-PE2-LoopBack0] ip address 202.200.1.1 255.255.255.255
[ASBR-PE2-LoopBack0] quit
[ASBR-PE2] interface pos1/0/0
[ASBR-PE2-Pos1/0/0] ip address 162.1.1.1 255.255.0.0
[ASBR-PE2-Pos1/0/0] quit
```

```
[ASBR-PE2] interface Pos 2/0/0
[ASBR-PE2-Pos2/0/0] ip address 192.1.1.2 255.255.255.0
[ASBR-PE2-Pos2/0/0] quit
[ASBR-PE2] ospf
[ASBR-PE2-ospf-1] area 0
[ASBR-PE2-ospf-1-area-0.0.0.0] network 162.1.0.0 0.0.255.255
[ASBR-PE2-ospf-1-area-0.0.0.0] network 202.200.1.1 0.0.0.0
[ASBR-PE2-ospf-1-area-0.0.0.0] quit
[ASBR-PE2-ospf-1] quit
```

After the configuration, the OSPF neighbor relationship should be established between ASBR PE and PEs in the same AS. Executing the **display ospf peer** command, you can find that the neighbor relationship is in Full state. PEs can learn Loopback addresses from each other.

ASBR-PE and other PEs in the same AS can be pinged successfully on each other. ASBR-PEs can be pinged successfully on each other.

2) Configuring basic MPLS capability on the MPLS backbone network to make the network forward VPN traffic

Note:

In this part:
The configurations on PE1, PE2, ASBR-PE1, and ASBR-PE2 are the same as those in section 3.4.10 "Configuring Inter-Provider Backbones Option A".

# Configure basic MPLS capability on PE1 and enable LDP on the interface connecting ASBR-PE1.

```
[PE1] mpls lsr-id 172.1.1.2
[PE1-mpls] lsp-trigger all
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface pos1/0/0
[PE1-Pos1/0/0] mpls
[PE1-Pos1/0/0] mpls ldp
[PE1-Pos1/0/0] quit
```

# Configure basic MPLS capability on ASBR-PE1 and enable LDP on the interface connecting PE1.

```
[ASBR-PE1] mpls lsr-id 172.1.1.1
[ASBR-PE1-mpls] lsp-trigger all
[ASBR-PE1-mpls] quit
```

```
[ASBR-PE1] mpls ldp
[ASBR-PE1-mpls-ldp] quit
[ASBR-PE1] interface pos1/0/0
[ASBR-PE1-Pos1/0/0] mpls
[ASBR-PE1-Pos1/0/0] mpls ldp
[ASBR-PE1-Pos1/0/0] quit
```

# Configure basic MPLS capability on ASBR-PE2 and enable LDP on the interface connecting PE2.

```
[ASBR-PE2] mpls lsr-id 162.1.1.1
[ASBR-PE2-mpls] lsp-trigger all
[ASBR-PE2-mpls] quit
[ASBR-PE2] mpls ldp
[ASBR-PE2-mpls-ldp] quit
[ASBR-PE2] interface pos1/0/0
[ASBR-PE2-Pos1/0/0] mpls
[ASBR-PE2-Pos1/0/0] mpls ldp
[ASBR-PE2-Pos1/0/0] quit
```

# Configure basic MPLS capability on PE2 and enable LDP on the interface connecting ASBR-PE2.

```
[PE2] mpls lsr-id 162.1.1.2
[PE2-mpls] lsp-trigger all
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] interface pos1/0/0
[PE2-Pos1/0/0] mpls
[PE2-Pos1/0/0] mpls ldp
[PE2-Pos1/0/0] quit
```

After the configuration, the LDP neighbor relationship should be established between PE and ASBR-PE in the same AS. Executing the **display mpls ldp session** command on the routers, you can find the Session State item is “Operational” in the display result.

3) Configuring VPN instances on PEs and binding to the interfaces connecting to CEs

Note:

Different from Option A, Option B method requires that the VPN-Target attribute of VPN instances of ASBR-PE and PE in the same AS should match each other. In addition, in different ASs, the matching of VPN-Target attributes of PEs is necessary.

In this part:

- The configurations on CE1, CE2, PE1, and PE2 are the same as those in section 3.4.10 "Configuring Inter-Provider Backbones Option A".
- It is unnecessary to configure VPN instances and interface binding on ASBR-PEs.

# Configure CE1.

```
[CE1] interface ethernet 1
[CE1-Ethernet1] ip address 168.1.1.2 255.255.0.0
[CE1-Ethernet1] quit
```

# Configure a VPN instance on PE1 and bind it to the interface connecting to CE1.

```
[PE1] ip vpn-instance vpna
[PE1-vpn-vpn-vpna] route-distinguisher 100:2
[PE1-vpn-vpn-vpna] vpn-target 100:1 both
[PE1-vpn-vpn-vpna] quit
[PE1] interface ethernet 2/0/0
[PE1-Ethernet2/0/0] ip binding vpn-instance vpna
[PE1-Ethernet2/0/0] ip address 168.1.1.1 255.255.0.0
[PE1-Ethernet2/0/0] quit
```

# Configure CE2.

```
[CE2] interface ethernet 1
[CE2-Ethernet1] ip address 168.2.2.2 255.255.0.0
[CE2-Ethernet1] quit
```

# Configure a VPN instance on PE2 and bind it to the interface connecting to CE2.

```
[PE2] ip vpn-instance vpna
[PE2-vpn-instance] route-distinguisher 200:2
[PE2-vpn-instance] vpn-target 100:1 both
[PE2-vpn-instance] quit
[PE2] interface ethernet 2/0/0
[PE2-Ethernet2/0/0] ip binding vpn-instance vpna
[PE2-Ethernet2/0/0] ip address 168.2.2.1 255.255.0.0
[PE2-Ethernet2/0/0] quit
```

After the configuration, you can view the VPN instance configuration by executing the **display ip vpn-instance verbose** command on PEs. CEs can be pinged successfully on PEs.

When pinging CE on PE, you need to specify the VPN to which the destination address belongs.

For example, ping CE1 on PE1:

[PE1] **ping -vpn-instance vpna 168.1.1.2**

4) Configuring MP-BGP, establishing IBGP peer relationship between PEs, and establishing EBGP peer relationship between PE and CE

📖 **Note:**

In this part:

- The configurations on CE1, CE2, PE1, and PE2 are the same as those in section 3.4.10 “Configuring Inter-Provider Backbones Option A”.
- Special configurations are necessary on ASBR-PE1 and ASBR-PE2: configuring the **undo policy vpn-target** command in VPNv4 address family view and configuring the **next-hop-local** command on IBGP peers in the AS.

# Configure CE1.

```
[CE1] bgp 65001
[CE1-bgp] group 20 external
[CE1-bgp] peer 168.1.1.1 group 20 as-number 100
[CE1-bgp] quit
```

# Configure PE1 to establish EBGP peer relationship with CE1 and IBGP peer relationship with ASBR-PE1.

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpna
[PE1-bgp-af-vpn-instance] group 10 external
[PE1-bgp-af-vpn-instance] peer 168.1.1.2 group 10 as-number 65001
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] quit
[PE1-bgp] group 20
[PE1-bgp] peer 202.100.1.1 group 20
[PE1-bgp] peer 202.100.1.1 connect-interface loopback0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer 20 enable
[PE1-bgp-af-vpn] peer 202.100.1.1 group 20
[PE1-bgp-af-vpn] quit
[PE1-bgp] quit
```

# Configure ASBR-PE1 to establish EBGP peer relationship with ASBR-PE2 and IBGP peer relationship with PE1.

```
[ASBR-PE1] bgp 100
[ASBR-PE1-bgp] group 10 external
[ASBR-PE1-bgp] peer 192.1.1.2 group 10 as-number 200
[ASBR-PE1-bgp] group 20
[ASBR-PE1-bgp] peer 202.100.1.2 group 20
[ASBR-PE1-bgp] peer 202.100.1.2 connect-interface loopback0
[ASBR-PE1-bgp] ipv4-family vpnv4
[ASBR-PE1-bgp-af-vpn] peer 20 enable
[ASBR-PE1-bgp-af-vpn] peer 202.100.1.2 group 20
[ASBR-PE1-bgp-af-vpn] peer 20 next-hop-local
[ASBR-PE1-bgp-af-vpn] peer 10 enable
[ASBR-PE1-bgp-af-vpn] peer 192.1.1.2 group 10
[ASBR-PE1-bgp-af-vpn] undo policy vpn-target
[ASBR-PE1-bgp-af-vpn] quit
[ASBR-PE1-bgp] quit
```

# Configure CE2.

```
[CE2] bgp 65002
[CE2-bgp] group 10 external
[CE2-bgp] peer 168.2.2.1 group 10 as-number 200
[CE2-bgp] quit
```

# Configure PE2 to establish EBGP peer relationship with CE2 and IBGP peer relationship with ASBR-PE2.

```
[PE2] bgp 200
[PE2-bgp] ipv4-family vpn-instance vpna
[PE2-bgp-af-vpn-instance] group 10 external
[PE2-bgp-af-vpn-instance] peer 168.2.2.2 group 10 as-number 65002
[PE2-bgp-af-vpn-instance] import-route direct
[PE2-bgp-af-vpn-instance] quit
[PE2-bgp] group 20
[PE2-bgp] peer 202.200.1.1 group 20
[PE2-bgp] peer 202.200.1.1 connect-interface loopback0
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpn] peer 20 enable
[PE2-bgp-af-vpn] peer 202.200.1.1 group 20
[PE2-bgp-af-vpn] quit
[PE2-bgp] quit
```

# Configure ASBR-PE2 to establish EBGP peer relationship with ASBR-PE1 and IBGP peer relationship with PE2.

```
[ASBR-PE2] bgp 200
[ASBR-PE2-bgp] group 10 external
[ASBR-PE2-bgp] peer 192.1.1.1 group 10 as-number 100
```

```
[ASBR-PE2-bgp] group 20
[ASBR-PE2-bgp] peer 202.200.1.2 group 20
[ASBR-PE2-bgp] peer 202.200.1.2 connect-interface loopback0
[ASBR-PE2-bgp] ipv4-family vpnv4
[ASBR-PE2-bgp-af-vpn] peer 20 enable
[ASBR-PE2-bgp-af-vpn] peer 202.200.1.2 group 20
[ASBR-PE2-bgp-af-vpn] peer 20 next-hop-local
[ASBR-PE2-bgp-af-vpn] undo policy vpn-target
[ASBR-PE2-bgp-af-vpn] peer 10 enable
[ASBR-PE2-bgp-af-vpn] peer 192.1.1.1 group 10
[ASBR-PE2-bgp-af-vpn] quit
[ASBR-PE2-bgp] quit
```

After completing the configuration, you can find that the BGP peer relationship has been established in Established state between PEs and between PE and CE by executing the **display bgp vpnv4 all peer** command on the routers.

CEs can learn interface routes from each other. CE1 and CE2 can be pinged successfully on each other.

When a PE works as an ASBR at the same time, it needs to retain all VPNv4 routing information and advertise it to other ASBRs. To this end, you must configure the **undo policy vpn-target** command on it to have it receive all VPNv4 routing information without filtering it based on VPN-target.

3.4.12 Configuring Inter-Provider Backbones Option C

I. Network requirements

CE1 and CE2 belong to the same VPN. CE1 accesses the network through PE1 in AS 100 and CE2 accesses the network through PE2 in AS 200.

Multi-AS BGP/MPLS VPN is implemented through Option C method. That is, labeled VPN-IPv4 routes are advertised between PEs through Multihop MP-EBGP to manage VPN routes.

II. Network diagram

See Figure 3-22.

III. Configuration procedure

According to the functions, the configuration procedures fall into four parts:

- Configuring OSPF on the MPLS backbone network
- Configuring basic MPLS capability on the MPLS backbone network
- Configuring VPN instances on PEs
- Configuring MP-BGP

Compared with Option A, Option C differs in the last two procedures.

1) Configuring OSPF on the MPLS backbone network to make PEs learn routes from each other

Note:

In this part:

The configurations on PE1 and PE2 are the same as those in section 3.4.11 “Configuring Inter-Provider Backbones Option B”.

# Configure PE1.

```
[PE1] interface loopback0
[PE1-LoopBack0] ip address 202.100.1.2 255.255.255.255
[PE1-LoopBack0] quit
[PE1] interface pos1/0/0
[PE1-Pos1/0/0] ip address 172.1.1.2 255.255.0.0
[PE1-Pos1/0/0] quit
[PE1] ospf
[PE1-ospf-1] area 0
[PE1-ospf-1-area-0.0.0.0] network 172.1.0.0 0.0.255.255
[PE1-ospf-1-area-0.0.0.0] network 202.100.1.2 0.0.0.0
[PE1-ospf-1-area-0.0.0.0] quit
[PE1-ospf-1] quit
```

# Configure ASBR-PE1.

```
[ASBR-PE1] interface loopback0
[ASBR-PE1-LoopBack 0] ip address 202.100.1.1 255.255.255.255
[ASBR-PE1-LoopBack 0] quit
[ASBR-PE1] interface pos1/0/0
[ASBR-PE1-Pos1/0/0] ip address 172.1.1.1 255.255.0.0
[ASBR-PE1-Pos1/0/0] quit
[ASBR-PE1] interface pos 2/0/0
[ASBR-PE1-Pos2/0/0] ip address 192.1.1.1 255.255.255.0
[ASBR-PE1-Pos2/0/0] quit
[ASBR-PE1] ospf
[ASBR-PE1-ospf-1] area 0
[ASBR-PE1-ospf-1-area-0.0.0.0] network 172.1.0.0 0.0.255.255
[ASBR-PE1-ospf-1-area-0.0.0.0] network 202.100.1.1 0.0.0.0
[ASBR-PE1-ospf-1-area-0.0.0.0] quit
[ASBR-PE1-ospf-1] quit
```

# Configure PE2.

```
[PE2] interface loopback0
```

```
[PE2-LoopBack0] ip address 202.200.1.2 255.255.255.255
[PE2-LoopBack0] quit
[PE2] interface pos1/0/0
[PE2-Pos1/0/0] ip address 162.1.1.2 255.255.0.0
[PE2-Pos1/0/0] quit
[PE2] ospf
[PE2-ospf-1] area 0
[PE2-ospf-1-area-0.0.0.0] network 162.1.0.0 0.0.255.255
[PE2-ospf-1-area-0.0.0.0] network 202.200.1.2 0.0.0.0
[PE2-ospf-1-area-0.0.0.0] quit
[PE2-ospf-1] quit
```

# Configure ASBR-PE2.

```
[ASBR-PE2] interface loopback0
[ASBR-PE2-LoopBack0] ip address 202.200.1.1 255.255.255.255
[ASBR-PE2-LoopBack0] quit
[ASBR-PE2] interface pos1/0/0
[ASBR-PE2-Pos1/0/0] ip address 162.1.1.1 255.255.0.0
[ASBR-PE2-Pos1/0/0] quit
[ASBR-PE2] interface Pos 2/0/0
[ASBR-PE2-Pos2/0/0] ip address 192.1.1.2 255.255.255.0
[ASBR-PE2-Pos2/0/0] quit
[ASBR-PE2] ospf
[ASBR-PE2-ospf-1] area 0
[ASBR-PE2-ospf-1-area-0.0.0.0] network 162.1.0.0 0.0.255.255
[ASBR-PE2-ospf-1-area-0.0.0.0] network 202.200.1.1 0.0.0.0
[ASBR-PE2-ospf-1-area-0.0.0.0] quit
[ASBR-PE2-ospf-1] quit
```

After the configuration, the OSPF neighbor relationship should be established between ASBR-PE and other PEs in the same AS. Executing the **display ospf peer** command, you can find that the neighbor relationship is in Full state. PEs can learn Loopback addresses from each other.

ASBR-PE and other PEs in the same AS can be pinged successfully on each other. ASBR-PEs can be pinged successfully on each other.

2) Configuring basic MPLS capability on the MPLS backbone network to make the network forward VPN traffic

Note:

In this part:

The configurations on PE1 and PE2 are the same as those in section 3.4.11 “Configuring Inter-Provider Backbones Option B”.

It is necessary to configure MPLS capability for interfaces between ASBR-PEs.

# Configure basic MPLS capability on PE1 and enable LDP on the interface connecting ASBR-PE1.

```
[PE1] mpls lsr-id 172.1.1.2
[PE1-mpls] lsp-trigger all
[PE1-mpls] quit
[PE1] mpls ldp
[PE1-mpls-ldp] quit
[PE1] interface pos1/0/0
[PE1-Pos1/0/0] mpls
[PE1-Pos1/0/0] mpls ldp
[PE1-Pos1/0/0] quit
```

# Configure basic MPLS capability on ASBR-PE1, enable LDP on the interface connecting PE1, and enable MPLS on the interface connecting ASBR-PE2.

```
[ASBR-PE1] mpls lsr-id 172.1.1.1
[ASBR-PE1-mpls] lsp-trigger all
[ASBR-PE1-mpls] quit
[ASBR-PE1] mpls ldp
[ASBR-PE1-mpls-ldp] quit
[ASBR-PE1] interface pos1/0/0
[ASBR-PE1-Pos1/0/0] mpls
[ASBR-PE1-Pos1/0/0] mpls ldp
[ASBR-PE1-Pos1/0/0] quit
[ASBR-PE1] interface pos2/0/0
[ASBR-PE1-Pos2/0/0] mpls
[ASBR-PE1-Pos2/0/0] quit
```

# Configure basic MPLS capability on ASBR-PE2, enable LDP on the interface connecting PE2, and enable MPLS on the interface connecting ASBR-PE1.

```
[ASBR-PE2] mpls lsr-id 162.1.1.1
[ASBR-PE2-mpls] lsp-trigger all
[ASBR-PE2-mpls] quit
[ASBR-PE2] mpls ldp
[ASBR-PE2-mpls-ldp] quit
[ASBR-PE2] interface pos1/0/0
```

```
[ASBR-PE2-Pos1/0/0] mpls
[ASBR-PE2-Pos1/0/0] mpls ldp
[ASBR-PE2-Pos1/0/0] quit
[ASBR-PE2] interface pos2/0/0
[ASBR-PE2-Pos2/0/0] mpls
[ASBR-PE2-Pos2/0/0] quit
```

Note:

In this scenario, ASBRs are connected through POS interfaces encapsulated with PPP. MPLS capability should be enabled on the interfaces to perform MPLSCP negotiation, thus to forward MPLS packet. MPLS capability need not to be enable if the interfaces adopt other link layer protocol.

# Configure basic MPLS capability on PE2 and enable LDP on the interface connecting ASBR-PE2.

```
[PE2] mpls lsr-id 162.1.1.2
[PE2-mpls] lsp-trigger all
[PE2-mpls] quit
[PE2] mpls ldp
[PE2-mpls-ldp] quit
[PE2] interface pos1/0/0
[PE2-Pos1/0/0] mpls
[PE2-Pos1/0/0] mpls ldp
[PE2-Pos1/0/0] quit
```

After the configuration, the LDP neighbor relationship should be established between PE and ASBR-PE in the same AS. Executing the **display mpls ldp session** command on the routers, you can find the Session State is “Operational" in the display result.

3) Configuring VPN instances on PEs and binding to the interfaces connecting to CEs

Note:

In this part:
The configurations on CE1, CE2, PE1, and PE2 are the same as those in section 3.4.11 “Configuring Inter-Provider Backbones Option B”.

# Configure CE1.

```
[CE1] interface ethernet 1
```

```
[CE1-Ethernet1] ip address 168.1.1.2 255.255.0.0
[CE1-Ethernet1] quit
```

# Configure a VPN instance on PE1 and bind it to the interface connecting to CE1.

```
[PE1] ip vpn-instance vpna
[PE1-vpn-vpn-vpna] route-distinguisher 100:2
[PE1-vpn-vpn-vpna] vpn-target 100:1 both
[PE1-vpn-vpn-vpna] quit
[PE1] interface ethernet 2/0/0
[PE1-Ethernet2/0/0] ip binding vpn-instance vpna
[PE1-Ethernet2/0/0] ip address 168.1.1.1 255.255.0.0
[PE1-Ethernet2/0/0] quit
```

# Configure CE2.

```
[CE2] interface ethernet 1
[CE2-Ethernet1] ip address 168.2.2.2 255.255.0.0
[CE2-Ethernet1] quit
```

# Configure a VPN instance on PE2 and bind it to the interface connecting to CE2.

```
[PE2] ip vpn-instance vpna
[PE2-vpn-instance] route-distinguisher 200:2
[PE2-vpn-instance] vpn-target 100:1 both
[PE2-vpn-instance] quit
[PE2] interface ethernet 2/0/0
[PE2-Ethernet2/0/0] ip binding vpn-instance vpna
[PE2-Ethernet2/0/0] ip address 168.2.2.1 255.255.0.0
[PE2-Ethernet2/0/0] quit
```

After the configuration, you can see the VPN instance configuration by executing the **display ip vpn-instance verbose** command on PEs. CEs can be pinged successfully on PEs.

When pinging CE on PE, you need to specify the VPN to which the destination address belongs.

For example, ping CE1 on PE1:

```
[PE1] ping -vpn-instance vpna 168.1.1.2
```

4) Configuring MP-BGP, establishing IBGP peer relationship between PEs, and establishing EBGP peer relationship between PE and CE

Note:

In this part:

- The configurations on CE1 and CE2 are the same as those in section 3.4.11 “Configuring Inter-Provider Backbones Option B”.
- The exchange of labeled IPv4 routes is configured between PE1 and ASBR-PE1, PE2 and ASBR-PE2, ASBR-PE1 and ASBR-PE2.
- ASBR-PE varies the next hop to itself when advertising routes to PEs in the same AS.
- Route-policy is configured on ASBR-PE. For the routes received from PEs in the same AS, ASBR-PE assigns MPLS labels for them when they are advertised to the ASBR of the remote AS. For the routes advertised to PEs in the same AS, ASBR-PE assigns new MPLS labels for them if they are labeled IPv4 routes.

# Configure CE1.

```
[CE1] bgp 65001
[CE1-bgp] group 20 external
[CE1-bgp] peer 168.1.1.1 group 20 as-number 100
[CE1-bgp] quit
```

# Configure PE1 to establish EBGP peer relationship with CE1, IBGP peer relationship with ASBR-PE1, and Multihop MP-EBGP peer relationship with PE2.

```
[PE1] bgp 100
[PE1-bgp] ipv4-family vpn-instance vpna
[PE1-bgp-af-vpn-instance] group 10 external
[PE1-bgp-af-vpn-instance] peer 168.1.1.2 group 10 as-number 65001
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] quit
[PE1-bgp] group 20
[PE1-bgp] peer 20 label-route-capability
[PE1-bgp] peer 202.100.1.1 group 20
[PE1-bgp] peer 202.100.1.1 connect-interface loopback0
[PE1-bgp] group 30 external
[PE1-bgp] peer 30 ebgp-max-hop
[PE1-bgp] peer 200.200.1.2 group 30 as-number 200
[PE1-bgp] peer 200.200.1.2 connect-interface loopback0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer 30 enable
[PE1-bgp-af-vpn] peer 200.200.1.2 group 30
[PE1-bgp-af-vpn] quit
[PE1-bgp] quit
```

# Configure route-policy on ASBR-PE1.

```
[ASBR-PE1] acl number 2001
[ASBR-PE1-acl-basic-2001] rule permit source 202.100.1.2 0
[ASBR-PE1-acl-basic-2001] rule deny source any
[ASBR-PE1-acl-basic-2001] quit
[ASBR-PE1] route-policy rtp-ebgp permit node 1
[ASBR-PE1-route-policy] if-match acl 2001
[ASBR-PE1-route-policy] apply mpls-label
[ASBR-PE1-route-policy] quit
[ASBR-PE1] route-policy rtp-ibgp permit node 10
[ASBR-PE1-route-policy] if-match mpls-label
[ASBR-PE1-route-policy] apply mpls-label
[ASBR-PE1-route-policy] quit
```

# Configure ASBR-PE1 to establish EBGP peer relationship with ASBR-PE2 and IBGP peer relationship with PE1.

```
[ASBR-PE1] bgp 100
[ASBR-PE1-bgp] import-route ospf
[ASBR-PE1-bgp] group 10 external
[ASBR-PE1-bgp] peer 10 label-route-capability
[ASBR-PE1-bgp] peer 10 route-policy rtp-ebgp export
[ASBR-PE1-bgp] peer 192.1.1.2 group 10 as-number 200
[ASBR-PE1-bgp] group 20
[ASBR-PE1-bgp] peer 20 label-route-capability
[ASBR-PE1-bgp] peer 20 next-hop-local
[ASBR-PE1-bgp] peer 20 route-policy rtp-ibgp export
[ASBR-PE1-bgp] peer 202.100.1.2 group 20
[ASBR-PE1-bgp] peer 202.100.1.2 connect-interface loopback0
[ASBR-PE1-bgp] quit
```

# Configure CE2.

```
[CE2] bgp 65002
[CE2-bgp] group 10 external
[CE2-bgp] peer 168.2.2.1 group 10 as-number 200
[CE2-bgp] quit
```

# Configure PE2 to establish EBGP peer relationship with CE2, IBGP peer relationship with ASBR-PE2, and Multihop MP-EBGP peer relationship with PE1.

```
[PE2] bgp 200
[PE2-bgp] ipv4-family vpn-instance vpna
[PE2-bgp-af-vpn-instance] group 10 external
[PE2-bgp-af-vpn-instance] peer 168.2.2.2 group 10 as-number 65002
[PE2-bgp-af-vpn-instance] import-route direct
[PE2-bgp-af-vpn-instance] quit
[PE2-bgp] group 20
```

```
[PE2-bgp] peer 20 label-route-capability
[PE2-bgp] peer 202.200.1.1 group 20
[PE2-bgp] peer 202.200.1.1 connect-interface loopback0
[PE2-bgp] group 30 external
[PE2-bgp] peer 30 ebgp-max-hop
[PE2-bgp] peer 202.100.1.2 group 30 as-number 100
[PE2-bgp] peer 202.100.1.2 connect-interface loopback0
[PE2-bgp] ipv4-family vpnv4
[PE2-bgp-af-vpn] peer 30 enable
[PE2-bgp-af-vpn] peer 202.100.1.2 group 30
[PE2-bgp-af-vpn] quit
[PE2-bgp] quit
```

# configure route-policy on ASBR-PE2.

```
[ASBR-PE2] acl number 2001
[ASBR-PE2-acl-basic-2001] rule permit source 200.200.1.2 0
[ASBR-PE2-acl-basic-2001] rule deny source any
[ASBR-PE2-acl-basic-2001] quit
[ASBR-PE2] route-policy rtp-ebgp permit node 1
[ASBR-PE2-route-policy] if-match acl 2001
[ASBR-PE2-route-policy] apply mpls-label
[ASBR-PE2-route-policy] quit
[ASBR-PE2] route-policy rtp-ibgp permit node 10
[ASBR-PE2-route-policy] if-match mpls-label
[ASBR-PE2-route-policy] apply mpls-label
[ASBR-PE2-route-policy] quit
```

# Configure ASBR-PE2 to establish EBGP peer relationship with ASBR-PE1 and IBGP peer relationship with PE2.

```
[ASBR-PE2] bgp 200
[ASBR-PE2-bgp] import-route ospf
[ASBR-PE2-bgp] group 10 external
[ASBR-PE2-bgp] peer 10 label-route-capability
[ASBR-PE2-bgp] peer 10 route-policy rtp-ebgp export
[ASBR-PE2-bgp] peer 192.1.1.1 group 10 as-number 100
[ASBR-PE2-bgp] group 20
[ASBR-PE2-bgp] peer 20 label-route-capability
[ASBR-PE2-bgp] peer 20 next-hop-local
[ASBR-PE2-bgp] peer 20 route-policy rtp-ibgp export
[ASBR-PE2-bgp] peer 202.200.1.2 group 20
[ASBR-PE2-bgp] peer 202.200.1.2 connect-interface loopback0
```

After the establishment of all BGP peer relationships, you can find the IPv4 route of the peer, that is, 200.200.1.2 and 202.100.1.2 respectively on PE1 and PE2. Executing the

display bgp routing label command, you can find that the two routes carry labels and the IPv4 routes learned from each other by PE1 and PE2.

CEs can learn interface routes from each other. CE1 and CE2 can be pinged successfully on each other.

3.5 Troubleshooting

3.5.1 Troubleshooting Multi-role Host Configuration

Fault 1: No routing policy is found for forwarding.

Measure: Enable debugging on the PE1 with the **debugging ip policy** command, to view routing policy.

3.5.2 Troubleshooting OSPF Multi-instance Configuration

Fault: The sham link interface cannot enter UP state.

Measure: Use the **display ip route vpn-instance** command to view if there are BGP routes to the destination address of the sham link, which are in the same VPN-instance with the OSPF procedure. If not, the sham link cannot enter UP state.

Chapter 4 MPLS L2VPN Configuration

4.1 Overview

4.1.1 Introduction to MPLS L2VPN

ATM-based and FR-based VPNs have gained widespread applications, which can enable different VPNs to share the network infrastructure of the same service provider. Yet, such traditional VPNs are not perfect due to some drawbacks, for example,

- Dependency on dedicated medium like ATM and FR. To provide the ATM-based VPN service, a service provider must construct a nationwide ATM network. If this service provider wants to develop the FR-based service, he has to construct a separate nationwide FR network. This is absolutely an enormous waste in terms of network construction.
- The VPN deployment is rather complex. This becomes more evident when adding a site onto the existing VPN, in which case, the configurations of all the edge nodes accessing this VPN site must be modified.

Some substitution solutions emerged in the process of solving these inherent drawbacks of traditional VPN. MPLS L2VPN is one among them. As the name implies, MPLS L2VPN provides L2 VPN service based on MPLS networks. With this solution, the service provider can provide the L2VPN service based on different media, such as ATM, FR, VLAN, Ethernet, and PPP, on the same MPLS network. Still, this MPLS network can provide other common services like IP, L3 VPN, traffic engineering, and QoS. This approach thus enormously saves the investment on network infrastructure.

Simply put, MPLS L2VPN transparently transmits L2 user data over MPLS networks. From the perspective of a user, this MPLS network is a L2 switching network, through which, L2 connection can be set up between sites. Take ATM as an example. You can connect a CE to another remote CE by configuring an ATM VC across an MPLS network. The interconnection thus achieved is the same as the interconnection implemented using an ATM network.

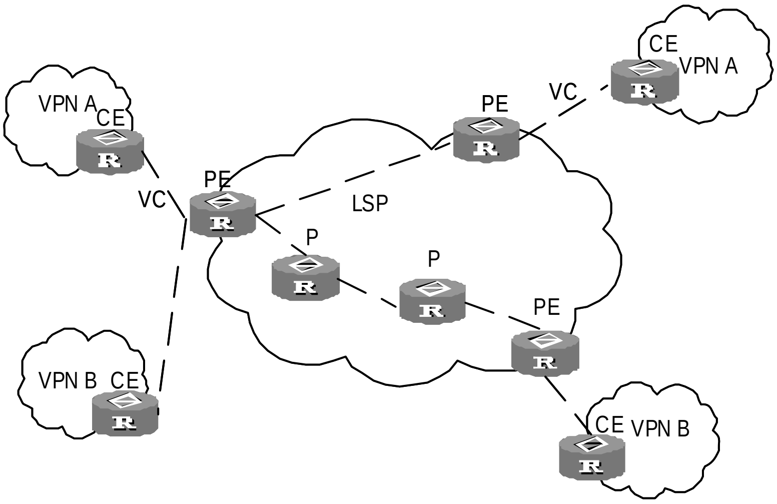


Figure 4-1 L2VPN

MPLS L2VPN offers the following benefits:

- Support multiple link-layer protocols to provide L2VPN services based on different media on the MPLS network, including ATM (ATM ALL5 and ATM cell relay), FR, VLAN, Ethernet, PPP, HDLC etc.
- Support multiple network layer protocols, such as IP, IPv6, IPX and SNA.

It provides multiple services, including L3VPN, traffic engineering, QoS etc.

- Excellent scalability. MPLS L2VPN only establishes L2 connections for users and does not redistribute and manage the routing information of users. Thus, the load on PE and the entire SP network can be significantly reduced. Thereby, the SP can support more VPNs and provide the access service for more subscribers.
- Guaranteed reliability and privacy of subscriber route. As MPLS L2VPN is not required to redistribute routing information of subscribers, it has neither needs nor means to obtain and process routes of subscribers. Thus, it guarantees the privacy of subscribers' routes.

4.1.2 MPLS L2VPN Frame Format

MPLS L2VPN frames are in such format:

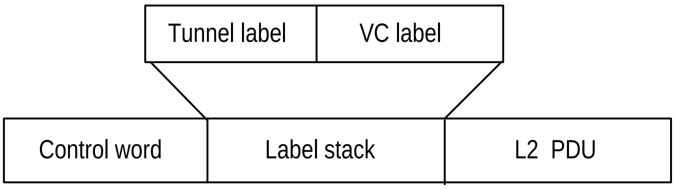


Figure 4-2 MPLS L2VPN frame format

Control word: It is unnecessary to transmit the L2 frame as a whole in transmitting 12VPN packets over MPLS network. All required is to distract the L2 frame header at the ingress and to add it at the egress. But for AAL5 and FR encapsulation at the link layer, extra information needs to be contained in L2 frame header. Control word is raised in this context to bear necessary information, which has been negotiated between ingress and egress.

Tunnel label (exterior-layer label): It may be MPLS label or GRE label, to transmit packets from one PE to another.

VC label (interior-layer label): It is the bottom-layer label to identify a PE-CE link. It has different meaning in Martini mode and in Kompella MODE. No such label is available for MPLS L2VPN in CCC mode.

These encapsulation modes at link layer are available for MPLS L2VPN: ATM AAL5, ATM cell relay, FR, Cisco HDLD, PPP, VLAN, Ethernet etc. The nodes in a same VPN currently are required to use identical encapsulation mode.

4.1.3 Packet Forwarding

MPLS L2VPN defines CE, PE and P in the same way with BGP/MPLS VPN, and their fundamentals are similar. Both of them make use of label stack to implement transparent transmission of subscriber packets over MPLS networks. First tunnels should be established between PEs either manually or through signaling protocol. When the interface connecting a PE and a CE enters UP state, PE allocates VC labels for the packets received and then stick tunnel labels to them. When they reach the remote PE, it removes tunnel labels and then forwards them to the desired CEs according the VC labels.

Figure 4-3 illustrates the label stack changes in the process of packet transmission.

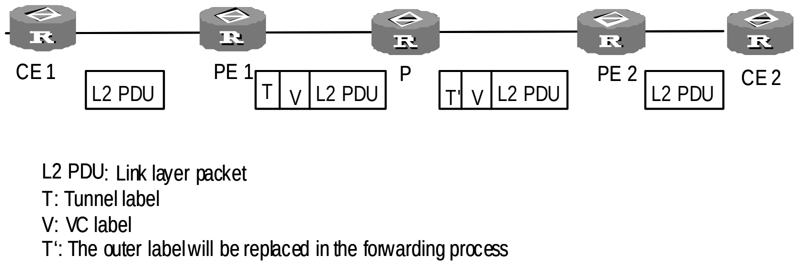

CE 1
L2 PDU
PE 1
T
V
L2 PDU
P
T'
V
L2 PDU
PE 2
L2 PDU
CE 2
L2 PDU: Link layer packet
T: Tunnel label
V: VC label
T': The outer label will be replaced in the forwarding process

Figure 4-3 Process an L2VPN label stack

4.1.4 MPLS L2VPN Implementation

By far, no official MPLS L2VPN standard has come into being. Provider-provisioned Virtual Private Network (PPVPN) workgroup of IETF has proposed several guideline drafts, among which, Martini and Kompella drafts are the most commonly known drafts. By March of 2002, these two drafts were respectively called:

draft-martini-l2circuit-trans-mpls-08.txt

draft-kompella-ppvpn-l2vpn-01.txt

The Martini draft provisions the point-to-point link implementation of L2VPN. As LDP is used as the signaling protocol for the VC label transmission between the participating parties, this implementation is called LDP/MPLS L2VPN.

Kompella draft provisions how to establish L2VPN end to end (CE-CE) over an MPLS network. So far, it adopts BGP as the signaling protocol to advertise the L2-reachable information and VC labels. Therefore, this implementation is always mentioned as BGP/MPLS L2VPN.

In addition, L2VPN service can be provided by configuring static VC labels rather than signaling. CCC is one approach for statically configuring L2VPN.

I. Introduction to CCC

Circuit Cross Connect (CCC) implements L2VPN through static configuration. Compared with the conventional MPLS L2VPN, CCC uses one tier of label for user data transmission. Therefore, its use of LSP is exclusive, and a user must manually configure two LSPs for each CCC connection, with one for each direction. These two LSPs can only be used for transmitting the data on this CCC connection and cannot be used on other L2VPN connections. Besides, they cannot be used on BGP/MPLS VPN or for carrying IP packets.

The major benefit for CCC mode is no special signaling is require to transmit L2 VPN information as long as MPLS forwarding is available. In addition, QoS is guaranteed for the LSP is privately leased.

II. MPLS L2VPN in SVC mode

Static Virtual Circuit (SVC) mode is in essence a static implementation of Martini mode. The difference is that in SVC mode the VC labels are configured manually, while LDP is not used as the signaling to transmit L2VC and link information.

III. MPLS L2VPN in Martini mode

Martini mode uses extended LDP (Martini draft extends LDP and adds VC FEC) as the signaling to transmit VC information. This mode identify a VC using VC-TYPE+VC-ID, where VC-TYPE stands for link-layer encapsulation type and VC-ID must be unique in a PE. A PE connecting two PEs uses LDP to exchange VC labels and binds together the corresponding CEs via the VC-ID. After established, a VC can transmit L2 data for two CEs.

Unlike CCC mode, Martini mode does not support local switching function. Besides, it also owns no privately leased LSP, but a LSP shared by many VCs.

In comparison with Kompella mode, it detects faults in a faster way, for it is not based on regular refreshing mechanism.

Martini mode is more applicable to a low-density L2 connection, for example, star connection.

IV. MPLS L2VPN in Kompella mode

MPLS L2VPN in Kompella mode is similar to the L3 BGP/MPLS VPN. Like BGP/MPLS VPN, the PE uses IBGP session to detect the nodes in L2VPN and transmit VPN information. In terms of label distribution, MPLS L2VPN in Kompella mode makes use of label block to assign labels for multiple connections at a time. The user can specify a local CE range to indicate the number of CEs to which the current CE can be connected. The system will assign a label block equivalent to CE range for the CE at a time. This approach allows the user to reserve some extra labels for VPNs for future use. While causing the waste of label resources, an enormous benefit of this undertaking is the reduced configuration works performed in VPN deployment and expansion. Once the size of the label blocks is determined, the system can calculate labels required in each link with a specific algorithm and forward packets with MPLS LSP. MPLS L2VPN also (in the same way as BGP/MPLS VPN) differentiates VPNs with VPN-target, which enable flexible VPN networking.

Unlike MPLS L2VPN in Martini mode, the Kompella mode does not operate directly on CE-CE connections, but partitions different VPNs in the SP network and then numbers the CEs in every VPN. For establishing a connection between two CEs, you only need to specify the IDs for local and remote CEs, as well as the circuit ID (for example, VPI/VCI of ATM) allocated by the local CE for the target connection.

Note:

The configuration of CE is relatively simple and only the interface involved is configured, so only PE configuration is detailed here.

If you have configured both L2VPN and L3VPN services, L3VPN service must comply with L2VPN service. If you remove L2VPN service, you can go on using L3VPN service.

4.2 Configuration of MPLS L2VPN in CCC Mode

Perform the following tasks to configure CCC on a PE:

- Configure interface
- Enable MPLS
- Configure static LSP
- Enable MPLS L2VPN
- Enable CCC on an interface
- Create CCC connection

It suffices to enabled MPLS and bidirectional static LSP on a P router.

4.2.1 Configuring the Interface Connecting CE

Only some compulsory configuration tasks are listed here. For optional tasks, refer to *V 2.41 Operation Manual – Link Layer Protocol*.

I. Configuring PPP, HDLC or Ethernet interface

For a PPP, HDLC or Ethernet interface, you just need to configure the corresponding link-layer protocol in the interface view.

📖 **Note:**

- When an Ethernet interface is configured with L2VPN, it does not support subinterfaces.
- When a main Ethernet interface has subinterfaces, if you try to configure L2VPN for the main interface, the system will display an alert message, telling you that you must first delete the subinterfaces.

II. Configuring ATM interface

For an ATM interface, you should perform the following configuration in the interface view.

Table 4-1 Configure ATM interface

Operation	Command
Create an ATM PVC and enter the PVC view	**pvc** [*name*] *vpi/vci*

For ATM, you can use the main interface or subinterface to connect the CE interface.

III. Configuring FE interface

For a FR interface, you should perform the following configuration in the interface view.

Table 4-2 Configure FR interface

Operation	Command
Configure interface encapsulation type as FR	**link-protocol fr** [**nonstandard** | **ietf**]
Configure FR interface type	**fr interface-type** { **dce** | **dte** | **nni** }
Configure FR LMI protocol type	**fr lmi type** { **ansi** | **nonstandard** | **q933a** }

Operation	Command
Configure static or dynamic FR address mapping	**fr map ip** { *protocol-address* [*ip-mask*] | *default* } *dlci* [**broadcast**] [**nonstandard** | **ietf**] **fr inarp** [**ip**] [*dlci*]
Allocate VC for the interface	**fr dlci** *dlci*

For FR, you can use the main interface or subinterface to connect the CE interface.

IV. Configuring ATM interface

For a VLAN subinterface, you should perform the following configuration in the interface view.

Table 4-3 Configure VLAN subinterface

Operation	Command
Configure encapsulation type and associated VLAN ID for Ethernet or Gigabit Ethernet subinterface	**vlan-type dot1q vid** *vid*

⚠ **Caution:**

L2VPN support these types of interfaces: Ethernet interface/subinterface, serial interface and ATM interface/subinterface.

For VLAN, only the Ethernet subinterface can server as CE interface. If a main Ethernet interface is used as CE interface, its encapsulation type is Ethernet, not VLAN, by default.

In L2VPN, each subinterface can only be configured with one VC. If multiple VCs have been configured, only the first one is valid.

Since L2VPN cannot fragment large packets on a P router, you must configure an MTU less than 1450 on the CE to avoid errors caused by incorrect fragmentation on a P router.

4.2.2 Enabling MPLS

MPLS underlies MPLS L2VPN. Therefore, you should enable MPLS before configuring the MPLS L2VPN parameters.

Perform the following configuration in the system view.

Table 4-4 Enable MPLS

Operation	Command
Configure LSR ID	**mpls lsr-id** *X.X.X.X*
Enable MPLS	**mpls**

4.2.3 Configuring Static LSP

CCC makes use of static LSP for transparently transmitting L2 packets over an SP network. Therefore, two static LSPs must be configured on the two PEs and all the in-between P routers, with each in one direction.

Perform the following configuration in MPLS view.

Table 4-5 Configure a static LSP

Operation	Command
Create an egress for a static LSP	**static-lsp egress** *lsp-name* **l2vpn incoming-interface** *interface-type interface-num* **in-label** *in-label*
Remove the egress of the static LSP	**undo static-lsp egress** *lsp-name* **l2vpn**
Create an ingress for the static LSP	**static-lsp ingress** *lsp-name* { **l2vpn | destination** *ip-add* } { **nexthop** *next-hop-addr* **| outgoing-interface** *interface-type interface-num* } **out-label** *out-label*
Remove the ingress of the static LSP	**undo static-lsp ingress** *lsp-name* **l2vpn**
Create a transit for the static LSP	**static-lsp transit** *lsp-name* **l2vpn incoming-interface** *interface-type interface-num* } **in-label** *in-label* { **nexthop** *next-hop-addr* **| outgoing-interface** *interface-type interface-num* } **out-label** *out-label*
Remove the transit of the static LSP	**undo static-lsp transit** *lsp-name* **l2vpn**

4.2.4 Enabling MPLS L2VPN

Perform the following configuration in system view.

Table 4-6 Enable MPLS L2VPN

Operation	Command
Enable MPLS L2VPN	**mpls l2vpn**

4.2.5 Creating CCC Connection

CCC connections fall into local connection and remote connection. Local connection refers to the connection established between two local CEs. With local connection, switching can be directly implemented on PE without using static LSP. Remote connection refers to the connection between a local CE and a remote CE, that is, two CEs connected to different PEs. In this case, two static LSPs (one in each direction) are required for PE-PE packet transmission.

Perform the following configurations in system view.

Table 4-7 Create a CCC connection

Operation	Command
Create a local CCC connection	**ccc** *ccc-connection-name* **interface** *type number* **out-interface** *outinterface-type outinterface-num*
Create a remote CCC connection	**ccc** *ccc-connection-name* **interface** *type number* **transmit-lsp** *transmit-lsp-name* **receive-lsp** *receive-lsp-name*

⚠ **Caution:**

A remote CCC connection uses its LSP in an exclusive way.

Therefore, two static LSPs (with each in one direction) must be configured for each remote CCC connection, rather than having two CCC connections share the same static LSP. A static LSP that has been used by a remote CCC connection cannot be used for other purposes like carrying IP or BGP/MPLS VPN data. For this reason, when creating a static LSP for a CCC connection, you are recommended to assign an IP address beyond the local network to the FEC of the CCC connection to prevent the likelihood of selecting the LSP for routing.

For one FR interface, L2 MPLS VPN can only be encapsulated on one subinterface. Therefore, the following configuration is invalid:

ccc vpntest interface Serial6/0/0.2 out-interface Serial6/0/1.1

ccc vpnfr interface Serial6/0/0.1 transmit-lsp 2to3 receive-lsp 3to2

4.3 Configuration of MPLS L2VPN in SVC Mode

Perform the following tasks to configure SVC on a PE:

- Configure interface
- Enable MPLS, MPLS LDP
- Enable MPLS L2VPN
- Configure PE-PE tunnel

- Create SVC connection

Refer to section 4.2 "Configuration of MPLS L2VPN in CCC Mode" for the first three steps.

4.3.1 Configuring PE-PE Tunnel

Current two types of tunnels are available, GRE tunnel and LSP tunnel.

I. Configuring GRE tunnel

Table 4-8 Configure GRE tunnel

Operation	Command
Create a tunnel interface	**Interface tunnel** *num*
Configure tunnel source address (tunnel interface view)	**source** *X.X.X.X*
Configure tunnel destination address (tunnel interface view)	**destination** *X.X.X.X*

II. Configuring LSP tunnel

Table 4-9 Configure LSP tunnel

Operation	Command
Configure LSP creation policy	**lsp-trigger** { **all** | **ip-prefix** *ip-prefix* }

⚠ **Caution:**

Since LSP is created by MPLS according to routing information, to create a LSP to the destination address, first make sure host routing information of every PE is transmitted to the peer by routing protocol.

4.3.2 Creating SVC Connection

Perform the following configurations in interface view.

Table 4-10 Create an SVC connection

Operation	Command
Create an SVC connection	**mpls static-l2vc destination** *destination-router-id* **transmit-vpn-label** *transmit-label-value* **receive-vpn-label** *receive-label-value*

Operation	Command
Delete an SVC connection	**undo mpls static-l2vc**

⚠ **Caution:**

You must guarantee the validity of transmit and receive labels of L2VPN in SVC mode.

4.4 Configuration of MPLS L2VPN in Martini Mode

Perform the following tasks to configure the MPLS L2VPN in Martini mode on a PE:

- Configure interface
- Enable MPLS L2VPN
- Enable MPLS and configure LDP remote-peer
- Configure PE-PE tunnel
- Create a Martini connection

The first two steps are identical with those for CCC mode. See section 4.3 “Configuration of MPLS L2VPN in SVC Mode” for configuring PE-PE tunnel.

4.4.1 Configuring LDP Remote-Peer

LDP/MPLS L2VPN depends on the LDP remote-peer for VC label switching. Therefore, before configuring a connection, you must enable LDP and configure the remote-peer of LDP.

Refer to LDP Configuration of MPLS Module for configuring LDP remote-peer.

4.4.2 Creating a Martini Connection

IP address of the remote PE and VC ID are the two main parameters in the LDP connection command. Where, the combination of VC ID and encapsulation type should be unique on the PE.

Perform the following configuration in interface view.

Table 4-11 Create a Martini connection

Operation	Command
Create a Martini connection	**mpls l2vc** *ip-address vc-id*
Delete a Martini connection	**undo mpls l2vc**

⚠ **Caution:**

With LDP/MPLS L2VPN, the VC ID assigned to a link must be unique among all the links with the same encapsulation type. Any encapsulation change is likely to cause VC ID collision. Suppose that both the interfaces serial0 encapsulated with HDLC and serial1 encapsulated with PPP have created the LDP connections, both of which are assigned with VC ID 1. If the link layer encapsulation type on serial1 is changed to HDLC, there will be two CCC-HDLC encapsulated LDP connections with the same VC ID of 1. To avoid the VC ID collision of these two connections, the LDP connection on serial1 will be automatically deleted.

4.5 Configuration of MPLS L2VPN in Kompella Mode

Perform the following tasks to configure the MPLS L2VPN in Kompella mode on a PE:

- Configure interface
- Enable MPLS and MPLS L2VPN.
- Configure BGP parameter
- Create and configure VPN
- Create CE and configure CE connection

The first two steps are identical with those for CCC mode, but you should configure in advance some reserved interfaces for future expansion.

4.5.1 Configuring BGP Parameters

The Kompella mode uses BGP as the signaling protocol to allocate VC labels, so you should configure BGP parameters on PE. For detailed configuration of BGP parameters, refer to BGP Configuration of Routing Protocol Module.

When BGP configuration is completed, you can activate the parameters for the peer group in MPLS L2VPN address family view with the following commands:

I. Entering L2VPN address family view

Perform the following configurations in BGP view.

Table 4-12 Enter L2VPN address family view

Operation	Command
Enter L2VPN address family view	**l2vpn-family**
Exit L2VPN address family view	**undo l2vpn-family**

When the **undo** command is executed, the system returns to BGP view and delete the L2VPN address family.

II. Activating the peer (group)

Perform the following configurations in L2VPN view.

Table 4-13 Activate the peer (group)

Operation	Command
Activate the peer (group)	**peer** { *peer-address* **|** *group-name* } **enable**
Deactivate the peer (group)	**undo peer** { *peer-address* | *group-name* } **enable**

By default, only the peer of BGP IPv4 unicast address family is activated, the peer of other types is inactive and cannot exchange routing information.

Perform the following configurations in system view.

4.5.2 Creating and Configuring VPN

I. Creating VPN

For BGP MPLS L2VPN, you must create a VPN view of MPLS L2VPN on a PE and specify its encapsulation type, which must be consistent with that for the CE interface.

Perform the following configurations in system view.

Table 4-14 Create VPN

Operation	Command
Create a VPN and specify its encapsulation type	**mpls l2vpn** *vpn-name* [**encapsulation** { **atm-aal5** | **ethernet** | **fr** | **hdlc** | **ppp** | **vlan** }]
Enter the MPLS L2VPN view	**mpls l2vpn** *vpn-name*
Delete the MPLS L2VPN view	**undo mpls l2vpn** *vpn-name*

II. Configuring VPN

Configure VPN-target and RD in the VPN view of MPLS L2VPN, which are identical with those of BGP/MPLS VPN will not be detailed here. But it should be noted that you must first configure RD for an MPLS L2VPN before other commands and you cannot modify the RD once you have configured it. The only way out is to delete the MPLS L2VPN and create another.

You can also configure L2 MTU for the VPN, which must be globally consistent. If the MTU values for the same VPN on two PEs are different, then the two PEs cannot exchange reachable information and no links can be established between them.

Perform the following configurations in MPLS L2VPN view.

Table 4-15 Configure VPN

Operation	Command
Configure RD for MPLS L2VPN	**route-distinguisher** *route-distinguisher*
Configure VPN-target for MPLS L2VPN	**vpn-target** *vpn-target-ext-community* [**import-extcommunity** | **export-extcommunity** | **both**]
Delete the VPN-target of MPLS L2VPN	**undo vpn-target** *vpn-target-ext-community* [**import-extcommunity** | **export-extcommunity** | **both**]
Configure L2 MTU for MPLS L2VPN	**mtu** *mtu*

4.5.3 Creating CE and Configuring CE Connection

I. Creating CE

You need create on PE a CE which is consistent with the one physically connected to PE and specify a unique ID for it. You can also specify the CE range.

Perform the following configurations in MPLS L2VPN view.

Table 4-16 Create CE

Operation	Command
Create a CE or modify CE range	**ce** *name* **id** *id* [**range** *range*] [**default-offset** *offset*]
Enter the CE	**ce** *name*
Delete the CE	**undo ce** *name*

CE ID uniquely identifies a CE in a VPN, so it must be unique in a VPN. For the sake of convenience, you are recommended to number the CE IDs from 1 and with consecutive natural number.

CE range indicates how many other CEs a CE can be connected to at most. If label resource is sufficient (which is often the case), you can set a CE range larger than the actual needs taking in account the future VPN size. Then you can minimize the modification in future if it is required to add CEs into the VPN in later expansion.

You have to modify the preset CE range if it is less than the needs in VPN expansion. For example, if current CE range is 10, while 20 CEs are required in expansion, you need to modify the value to 20. The existing ten links will not be cut off in modifying CE range, since the system just applies for another block of 10 labels, instead of releasing the existing label block and applying for another block of 20 labels.

Suppose a corporation has ten CEs in its VPN, but the expanded network may have 20 CEs, so you can set the CE range as 20. Then the system will allocate labels for the future ten CEs in advance, so you only need to modify those CEs newly connected to the PE in future expansion.

⚠ **Caution:**

You can only modify CE range to a larger value, but not a less value. For example, you can change CE range from 10 to 20, but not from 10 to 5. The only way to alter it to a less value: First delete the current CE range and then create another.

II. Configuring CE connection

To create a CE connection in MPLS L2VPN CE view, you just need to specify the CE interface and the ID of the peer CE (CE offset). You can preset some reserved connections for future expansion.

Perform the following configurations in MPLS L2VPN CE view

Table 4-17 Create CE connection

Operation	Command
Create a CE connection	**connection** [**ce-offset** *offset*] { **interface** *interface-type interface-num* }
Delete a CE connection	**undo connection** [**ce-offset** *offset*] { **interface** *interface-type interface-num* }

If the optional parameter *CE offset* is not specified, then

1) If this is the first connection for the CE, CE offset is defaulted to 1.
2) Otherwise, CE offset is set to the former CE offset plus 1.

You can have CE IDs increment beginning at 1 when planning VPNs so that you can configure connections according to CE IDs when making configuration. This allows you to use the default CE offset instead of configuring one for most connections, thus simplifying the configuration.

4.6 Displaying and Debugging MPLS L2VPN

After accomplishing the configuration tasks described earlier, you can execute the **display** command in any view to view the running state of the configured MPLS L2VPN and thus to evaluate the effect of the configurations.

Execute the **debugging** command in user view to debug MPLS L2VPN.

Table 4-18 Monitoring and maintenance of L2VPN

Operation	Command
Display CCC connection information	**display ccc** [*ccc-name* | **type** [**local** | **remote**]]
Display SVC connection information	**display mpls static-l2vc** [**interface** *interface-type interface -num*]
Display Martini connection information	**display mpls l2vc** [**interface** *interface-type interface-num* | **verbose**]
Display L2VPN information at a specific interface	**display mpls l2vpn forwarding-info** [*vc-label*] **interface** *interface-type interface-num*
Display all L2VPN information	**display bgp l2vpn all**
Enable Kompella MPLS L2VPN debugging	**debugging bgp** [{ { **keepalive** | **open** | **packet** | **update** | **route-refresh** } [**receive** | **send**] [**verbose**] | **event** }]
Enable MPLS L2VPN debugging	**debugging mpls l2vpn** { **all** | **advertisement** | **error** | **event** | **connections** [**interface** *interface-type interface-num*] }

4.7 MPLS L2VPN Configuration Example

4.7.1 Configuring CCC-Based MPLS L2VPN

I. Network requirements

Connect CE and PE using serial interface, and the encapsulation protocol at link layer is PPP. It is required to set up a local connection between CE-A and CE-B, and a remote connection between CE-A and CE-C.

II. Network diagram

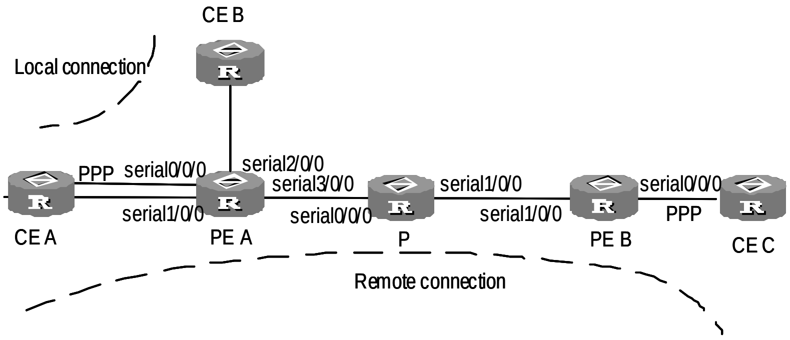


Figure 4-4 Network diagram for CCC configuration

III. Configuration procedure

1) Configure PE-A:

# Globally enable MPLS.

```
[3Com] mpls lsr-id 172.1.1.1
[3Com] mpls
```

# Globally enable MPLS L2VPN.

```
[3Com] mpls l2vpn
```

# Configure the interface SERIAL 0/0/0.

```
[3Com] interface serial0/0/0
[3Com-Serial0/0/0] link-protocol ppp
```

# Configure the interface SERIAL 1/0/0.

```
[3Com] interface serial 1/0/0
[3Com-Serial1/0/0] link-protocol ppp
```

# Configure the interface SERIAL 2/0/0.

```
[3Com] interface serial 2/0/0
[3Com-Serial2/0/0] link-protocol ppp
```

# Enable MPLS on the interface SERIAL 3/0/0.

```
[3Com] interface serial 3/0/0
[3Com-Serial3/0/0] link-protocol ppp
[3Com-Serial3/0/0] mpls
```

# Configure a local connection.

```
[3Com] ccc local-conn interface serial0/0/0 outgoing-interface serial2/0/0
```

# Configure a static LSP, with the out-label 100 and the outgoing interface SERIAL 3/0/0.

```
[3Com] mpls
[3Com-mpls] static-lsp ingress PEA-PEB destination 10.0.0.0 l2vpn
outgoing-interface serial3/0/0 out-label 100 pre 2 metric 3
```

# Configure a static LSP, with the in-label 201 and the incoming interface SERIAL 3/0/0.

```
[3Com-mpls] static-lsp egress PEB-PEA l2vpn incoming-interface serial3/0/0
in-label 201
```

# Configure a remote connection.

```
[3Com] ccc remote-connection interface serial3/0/0 transmit-lsp PEA-PEB
receive-lsp PEB-PEA
```

2) Configure PE-B:

# Globally enable MPLS.

```
[3Com] mpls lsr-id 10.0.0.1
```

```
[3Com] mpls
```

# Globally enable MPLS L2VPN.

```
[3Com]mpls l2vpn
```

# Configure the interface SERIAL 0/0/0.

```
[3Com] interface serial 0/0/0
[3Com-Serial0/0/0] link-protocol ppp
```

# Enable MPLS on the interface SERIAL1/0/0.

```
[3Com] interface serial 1/0/0
[3Com-Serial1/0/0] link-protocol ppp
[3Com-Serial1/0/0] mpls
```

# Configure a static LSP, with the out-label 100 and outgoing interface SERIAL 1/0/0.

```
[3Com-mpls] static-lsp ingress PEB-PEA destination 10.0.0.0 l2vpn
outgoing-interface serial 1/0/0 out-label 200 pre 2 metric 3
```

# Configure a static LSP, with the in-label 201 and incoming interface SERIAL 1/0/0.

```
[3Com-mpls] static-lsp egress PEA-PEB l2vpn incoming-interface serial 1/0/0
in-label 101
```

# Configure a remote connection.

```
[3Com] ccc remote-conn interface serial1/0/0 transmit-lsp PEB-PEA receive-lsp
PEA-PEB
```

3) Configure P:

```
[3Com] mpls lsr-id 10.0.0.2
[3Com] mpls
[3Com-mpls] mpls l2vpn
```

# Configure a static LSP, with the in-label 100, incoming interface SERIAL0/0/0, out-label 101, and the outgoing interface SERIAL1/0/0.

```
[3Com-mpls] static-lsp transit PEA-PEB l2vpn incoming-interface serial 0/0/0
in-label 100 outgoing-interface serial 1/0/0 out-label 101
```

# Configure a static LSP, with the in-label 200, incoming interface SERIAL1/0/0, out-label 201, and the outgoing interface SERIAL0/0/0.

```
[3Com-mpls] static-lsp transit PEB-PEA l2vpn incoming-interface serial1/0/0
in-label 200 outgoing-interface serial 0/0/0 out-label 201
```

⚠ **Caution:**

- The conditions for a CCC local connection to enter UP state:

The physical states of the two CE interfaces are in UP state.

The encapsulation type for the two CE interfaces is consistent and supported in current MPLS L2VPN.

- For a MPLS L2VPN of VLAN encapsulation type, the VLAN IDs for the two CE interfaces can be inconsistent.

4.7.2 Configuring SVC-Based MPLS L2VPN

I. Network requirements

Configure a remote SVC connection encapsulated with FR from CE1 at PE1 side to CE2 at PE2 side.

Note:

To communicate normally, the DCE/DTE settings on CE1 and CE2 must match. On the path CE1-PE1-PE3-CE4 in this scenario, set CE1 to DCE, PE1 to DTE, PE2 to DCE and CE2 to DTE.

II. Network diagram

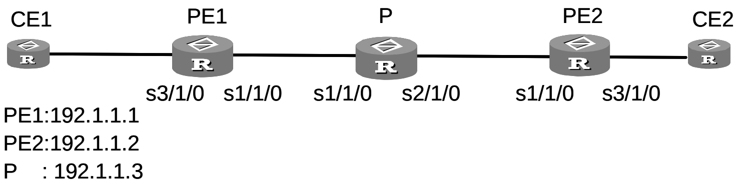


Figure 4-5 Network diagram for SVC-based MPLS L2VPN

III. Configuration procedure

1) Configure PE1

# Configure LSR ID, enable MPLS, LDP and MPLS L2VPN.

```
[3Com-mpls] mpls lsr-id 192.1.1.1
[3Com] mpls
[3Com] mpls ldp
[3Com] mpls l2vpn
```

# Configure CE interface.

```
[PE1] interface serial3/1/0
[PE1-serial3/1/0] fr dlci 101
```

# Configure serial interface.

```
[PE1] interface serial1/1/0
[PE1-serial1/1/0] mpls ldp enable
[PE1-serial1/1/0] ip address 168.1.1.1 255.255.0.0
```

# Enable OSPF.

```
[3Com] ospf 1
[3Com -ospf-1] area 0.0.0.0
[3Com -ospf-1-area-0.0.0.0] network 192.1.1.1 0.0.0.0
[3Com -ospf-1-area-0.0.0.0] network 168.1.0.0 0.0.255.255
```

# Configure LSP or LSP setup triggering between PE1 and PE2.

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

# Configure SVC connection

```
[PE1] interface serial3/1/0
[PE1-s3/1/0] mpls static-l2vc destination 192.1.1.3 transmit-vpn-label 111
receive-vpn-label 333
```

2) Configure PE2

# Configure LSR ID, enable MPLS, LDP and MPLS L2VPN.

```
[3Com-mpls] mpls lsr-id 192.1.1.2
[3Com] mpls
[3Com] mpls ldp
[3Com] mpls l2vpn
```

# Configure CE interface.

```
[PE2] interface serial3/1/0
[PE2- serial3/1/0] fr linterface-type dce
[PE2- serial3/1/0] fr dlci 101
```

# Configure serial interface.

```
[PE1] interface serial1/1/0
[PE1-serial1/1/0] mpls
[PE1-serial1/1/0] mpls ldp enable
[PE1-serial1/1/0] ip address 169.1.1.1 255.255.0.0
```

# Enable OSPF.

```
[3Com] ospf 1
[3Com -ospf-1] area 0.0.0.0
[3Com -ospf-1-area-0.0.0.0] network 192.1.1.2 0.0.0.0
[3Com -ospf-1-area-0.0.0.0] network 169.1.0.0 0.0.255.255
```

# Configure LSP or LSP setup triggering between PE1 and PE2.

```
[PE2] mpls
```

```
[PE2-mpls] lsp-trigger all
```

# Configure SVC connection.

```
[PE2-s3/1/0] mpls static-l2vc destination 192.1.1.1 transmit-vpn-label 333
receive-vpn-label 111
```

3) Configure P

# Configure LSR ID, enable MPLS, LDP and MPLS L2VPN.

```
[3Com-mpls] mpls lsr-id 192.1.1.2
[3Com] mpls
[3Com] mpls ldp
[3Com] mpls l2vpn
```

# Configure serial interface.

```
[P] interface serial1/1/0
[P-serial1/1/0] ip address 168.1.1.2 255.255.0.0
[P] interface serial2/1/0
[P-serial2/1/0] ip address 169.1.1.2 255.255.0.0
```

# Configure LSP or LSP setup triggering between PE1 and PE2.

```
[PE2] mpls
[PE2-mpls] lsp-trigger all
```

4.7.3 Configuring Martini MPLS L2VPN

I. Network requirements

Adopt VLAN to access CEs and establish a remote connection between CE A and CE B.

II. Network diagram

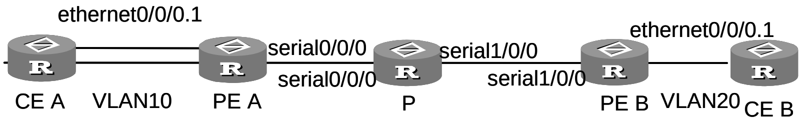


Figure 4-6 Network diagram for Martini MPLS L2VPN

III. Configuration procedure

1) Configure PE A

# Configure LSR ID, enable MPLS, LDP and MPLS L2VPN.

```
[3Com-mpls] mpls lsr-id 192.1.1.1
[3Com] mpls
[3Com] mpls ldp
[3Com] mpls l2vpn
```

# Configure VLAN subinterface.

```
[3Com] interface ethermet0/0/0.1
[3Com-Ethernet0/0/0.1] vlan-type dot1q vid 20
```

# Configure the serial interface.

```
[3Com] interface serial 0/0/0
[3Com-serial0/0/0] ip address 168.1.1.1 255.255.0.0
[3Com-serial 0/0/0] mpls
[3Com-serial 0/0/0] mpls ldp enable
```

# Assign an address to the loopback interface, which will be taken as route ID.

```
[3Com] interface loopback 0
[3Com-LoopBack0] ip address 192.1.1.1 255.255.255.255
```

# Enable OSPF.

```
[3Com] ospf 1
[3Com-ospf-1] area 0.0.0.0
[3Com-ospf-1-area-0.0.0.0] network 192.1.1.1 0.0.0.0
[3Com-ospf-1-area-0.0.0.0] network 168.1.0.1 0.0.255.255
[3Com-ospf-1-area-0.0.0.0] network 192.2.1.0 0.0.0.255
[3Com-ospf-1-area-0.0.0.0] quit
```

# Configure an LDP remote peer.

```
[3Com] mpls ldp remote-peer 1
[3Com-remote-peer-1] remote-peer 192.1.1.2 255.255.255.255
```

# Configure Martini MPLS L2VPN connection.

```
[3Com] interface Ethernet0/0/0.1
[3Com-Ethernet0/0/0.1] mpls l2vc 192.1.1.2 20
```

2) Configure PE B

# Configure LSR ID, enable MPLS, LDP and MPLS L2VPN.

```
[3Com] mpls lsr-id 192.1.1.2
[3Com] mpls
[3Com] mpls ldp
[3Com] mpls l2vpn
```

# Configure the VLAN subinterface.

```
[3Com-LoopBack0] interface ethernet0/0/0.1
[3Com-Ethernet0/0/0.1] vlan-type dot1q vid 20
```

# Configure the serial interface.

```
[3Com] interface serial 1/0/0
[3Com-serial1/0/0] ip address 169.1.1.1 255.255.0.0
[3Com-serial1/0/0] mpls
[3Com-serial 1/0/0] mpls ldp enable
```

# Assign an address to the loopback interface, which will be taken as the LSR ID.

```
[3Com] interface loopback 0
[3Com-LoopBack0] ip address 192.1.1.2 255.255.255.255
```

# Enable OSPF.

```
[3Com] ospf 1
[3Com-ospf-1] area 0.0.0.0
[3Com-ospf-1-area-0.0.0.0] network 192.1.1.2 0.0.0.0
[3Com-ospf-1-area-0.0.0.0] network 169.1.0.0 0.0.255.255
[3Com-ospf-1-area-0.0.0.0] network 192.2.0.0 0.0.0.255
[3Com-ospf-1-area-0.0.0.0] quit
```

# Configure an LDP remote-peer

```
[3Com] mpls ldp remote-peer 1
[3Com-mpls-remote1] remote-peer 192.1.1.1 255.255.255.255
```

# Configure Martini MPLS L2VPN connection.

```
[3Com] interface Ethernet0/0/0.1
[3Com-Ethernet0/0/0.1] mpls l2vc 192.1.1.1 20
```

3) Configure P

# Configure LSR ID, enable MPLS, LDP and MPLS L2VPN.

```
[3Com] mpls lsr-id 192.1.1.3
[3Com] mpls
[3Com] mpls ldp
[3Com] mpls l2vpn
```

# Assign an address to the loopback interface, which will be taken as the LSR ID.

```
[3Com]interface loopback 0
[3Com-LoopBack0] ip address 192.1.1.3 255.255.255.255
```

# Configure the serial interface.

```
[3Com-LoopBack0] interface serial0/0/0
[3Com-serial0/0/0] mpls ldp enable
[3Com-serial0/0/0] ip address 168.1.1.2 255.255.0.0
[3Com] interface serial1/0/0
[3Com-serial0/0/0] mpls
[3Com-serial0/0/0] mpls ldp enable
[3Com-serial1/0/0] ip address 169.1.1.2 255.255.0.0
```

# Enable OSPF.

```
[3Com] ospf 1
[3Com-ospf-1] area 0.0.0.0
[3Com-ospf-1-area-0.0.0.0] network 168.1.0.0 0.0.255.255
[3Com-ospf-1-area-0.0.0.0] network 169.1.0.0 0.0.255.255
[3Com-ospf-1-area-0.0.0.0] network 192.1.1.3 0.0.0.0
```

⚠ **Caution:**

The conditions for a Martini connection to go up are:

- The two CE interfaces are in UP state.
- Two tunnels (GRE or LSP, one in each direction) have been established between two PEs.
- The encapsulation type for the two CE interfaces is consistent and supported in current MPLS L2VPN.
- LDP remote session has been set up between two PEs and is in UP state.
- To establish a GRE or LSPF tunnel, you have to specify the route to the peer PE, so it is required to configure IGP (for example, OSPF) on the routers along the route,

4.7.4 Configuring Kompella MPLS L2VPN

I. Network requirements

CE and PE are connected through ATM interface. Create a connected VPN, in which three CEs are contained: CE-A, CE-B and CE-C. Since two CEs will be added in later expansion, the CE range for each CE is set to 4 and VCs have been allocated for the future two CEs. In the future expansion, only configuring the PE for which new CEs are added is only required.

II. Network diagram

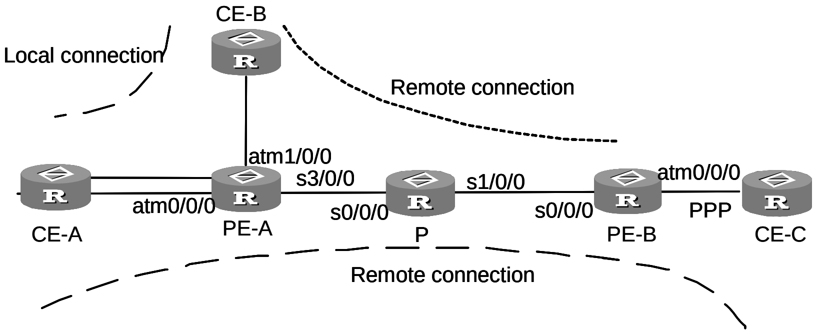


Figure 4-7 Network diagram for Kompella MPLS VPN

III. Configuration procedure

1) Configure PE-A

# Configure LSR ID; enable MPLS L2VPN.

```
[3Com] mpls lsr-id 192.1.1.1
```

```
[3Com] mpls
[3Com] mpls l2vpn
```

# Assign an address to the loopback interface.

```
[3Com] interface loopback 0
[3Com-LoopBack0] ip address 192.1.1.1 255.255.255.255
```

# Configure the serial interface.

```
[3Com-LoopBack0] interface serial 3/0/0
[3Com-Serial3/0/0] ip address 168.1.1.1 255.255.0.0
[3Com-Serial3/0/0] mpls ldp enable
```

# Configure the CE interface for CE-A.

```
[3Com] interface atm0/0/0.1
[3Com-Atm0/0/0.1] pvc CEA-CEB 100/101
[3Com-Atm0/0/0.1] interface atm0/0/0.2
[3Com-Atm0/0/0.2] pvc CEA-CEC 100/102
```

# Reserve PVCs for future CEs.

```
[3Com-Atm0/0/0.1] interface atm0/0/0.3
[3Com-Atm0/0/0.3] pvc CEA-CED 100/103
[3Com-Atm0/0/0.3] interface atm0/0/0.4
[3Com-Atm0/0/0.4] pvc CEA-CEE 100/104
```

# Configure the CE interface for CE-B.

```
[3Com] interface atm1/0/0.1
[3Com-Atm1/0/0.1] pvc CEB-CEA 200/101
[3Com] interface atm1/0/0.2
[3Com-Atm1/0/0.2] pvc CEB-CEC 200/102
```

# Reserve PVCs for future CEs.

```
[3Com] interface atm1/0/0.3
[3Com-Atm1/0/0.3] pvc CEB-CED 200/103
[3Com] interface atm1/0/0.4
[3Com-Atm1/0/0.4] pvc CEB-CEE 200/104
```

# Enable OSPF.

```
[3Com] ospf 1
[3Com-ospf-1] area 0.0.0.0
[3Com-ospf-1-area-0.0.0.0] network 192.1.1.1 0.0.0.0
[3Com-ospf-1-area-0.0.0.0] network 168.1.0.0 0.0.255.255
```

# Configure LSP or LSP setup triggering between PE-A and PE-B.

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

# Configure BGP parameter.

```
[3Com] bgp 100
[3Com-bgp] group 192 internal
[3Com-bgp] peer 192.1.1.2 connect-interface LoopBack0
[3Com-bgp] peer 192.1.1.2 group 192 as-number 100
[3Com-bgp] peer 192.1.1.3 connect-interface LoopBack0
[3Com-bgp] peer 192.1.1.3 group 192 as-number 100
[3Com-bgp] l2vpn-family
[3Com-bgp-af-l2vpn] peer 192 enable
```

# Configure Kompella connection.

```
[3Com] mpls l2vpn vpna encapsulation atm-aal5
[3Com-l2vpn-vpna] route-distinguisher 100:1
[3Com-l2vpn-vpna] vpn-target 100:1 both
```

# Create CE-A.

```
[3Com-l2vpn-vpna] ce ce-a id 1 range 4
```

# Configure local connection with CE-B.

```
[3Com-l2vpn-vpna-ce-ce-a] connection ce-offset 2 atm0/0/0.1
```

# Configure remote connection with CE-C.

```
[3Com-l2vpn-vpna-ce-ce-a] connection atm0/0/0.2
```

# Configure the connections for future expansion.

```
[3Com-l2vpn-vpna-ce-ce-a] connection atm0/0/0.3
[3Com-l2vpn-vpna-ce-ce-a] connection atm0/0/0.4
```

# Create CE-B.

```
[3Com-l2vpn-vpna] ce ce-b id 2 range 4
```

# Configure local connection with CE-A.

```
[3Com-l2vpn-vpna-ce-ce-b] connection ce-offset 3 atm1/0/0.1
```

# Configure remote connection with CE-C.

```
[3Com-l2vpn-vpna-ce-ce-b] connection atm1/0/0.2
```

# Configure the connections for future expansion.

```
[3Com-l2vpn-vpna-ce-ce-b] connection atm1/0/0.3
[3Com-l2vpn-vpna-ce-ce-b] connection atm1/0/0.4
```

2) Configure PE-B

# Configure MPLS RD, globally enable MPLS and MPLS L2VPN.

```
[3Com] mpls lsr-id 192.1.1.2
[3Com] mpls
[3Com] mpls ldp
[3Com] mpls l2vpn
```

# Assign an address to the loopback interface.

```
[3Com] interface loopback 0
[3Com-LoopBack0] ip address 192.1.1.2 255.255.255.255
```

# Configure serial interface.

```
[3Com-LoopBack0] interface serial 0/0/0
[3Com-Serial0/0/0] ip address 169.1.1.1 255.255.0.0
[3Com-Serial0/0/0] mpls ldp enable
```

# Configure ATM subinterface and PVC.

```
[3Com] interface atm0/0/0.1
[3Com-Atm0/0/0.1] pvc CEC-CEA 300/101
[3Com] interface atm0/0/0.2
[3Com-Atm0/0/0.2] pvc CEC-CEB 300/102
```

# Reserve PVC for future CE.

```
[3Com-Atm0/0/0.2] interface atm0/0/0.3
[3Com-Atm0/0/0.3] pvc CEC-CED 300/103
[3Com]interface atm0/0/0.4
[3Com-Atm0/0/0.4] pvc CEC-CEE 300/104
```

# Enable OSPF.

```
[3Com] ospf 1
[3Com -ospf-1] area 0.0.0.0
[3Com -ospf-1-area-0.0.0.0] network 192.1.1.1 0.0.0.0
[3Com -ospf-1-area-0.0.0.0] network 168.1.0.0 0.0.255.255
```

# Configure LSP.

```
[PE2] mpls
[PE2-mpls] lsp-trigger all
```

# Configure BGP parameter.

```
[3Com] bgp 100
[3Com-bgp] group 192 internal
[3Com -bgp] peer 192.1.1.1 connect-interface LoopBack0
[3Com -bgp] peer 192.1.1.1 group 192 as-number 100
[3Com -bgp] peer 192.1.1.3 connect-interface LoopBack0
[3Com -bgp] peer 192.1.1.3 group 192 as-number 100
[3Com -bgp] l2vpn-family
[3Com -bgp-af-l2vpn] peer 192 enable
```

# Configure Kompella connection.

```
[3Com] mpls l2vpn vpna encapsulation atm-aal5
[3Com-l2vpn-vpna] route-distinguisher 100:1
[3Com-l2vpn-vpna] vpn-target 100:1 both
```

# Create CE-C.

```
[3Com-l2vpn-vpna-ce-ce-c] ce ce-c id 3 range 4
```

# Configure connection with CE-A.

```
[3Com-l2vpn-vpna-ce-ce-c] connection atm0/0/0.1
```

# Configure remote connection with CE-B.

```
[3Com-l2vpn-vpna-ce-ce-c] connection atm0/0/0.2
```

# Configure connection for future expansion.

```
[3Com-l2vpn-vpna-ce-ce-c] connection atm0/0/0.3 ce-offset 4
[3Com-l2vpn-vpna-ce-ce-c] connection atm0/0/0.4
```

3) Configure P:

# Configure MPLS RD, globally enable MPLS and MPLS L2VPN.

```
[3Com] mpls lsr-id 192.1.1.3
[3Com] mpls
[3Com-mpls] mpls ldp
```

# Assign an address to the loopback interface.

```
[3Com] interface loopback 0
[3Com-LoopBack0] ip address 192.1.1.3 255.255.255.255
```

# Configure the serial interface.

```
[3Com-LoopBack0] interface serial 0/0/0
[3Com-Serial0/0/0] link-protocol ppp
[3Com-Serial0/0/0] ip address 168.1.1.2 255.255.0.0
[3Com-Serial0/0/0] mpls
[3Com-Serial0/0/0] mpls ldp enable
[3Com] interface serial 1/0/0
[3Com-Serial1/0/0] link-protocol ppp
[3Com-Serial1/0/0] ip address 169.1.1.2 255.255.0.0
[3Com-Serial1/0/0] mpls
[3Com-Serial1/0/0] mpls ldp enable
```

# Enable OSPF.

```
[3Com] ospf 1
[3Com-ospf-1] area 0.0.0.0
[3Com-ospf-1-area-0.0.0.0] network 192.1.1.3 0.0.0.0
[3Com-ospf-1-area-0.0.0.0] network 168.1.0.0 0.0.255.255
[3Com-ospf-1-area-0.0.0.0] network 169.1.0.0 0.0.255.255
```

# Configure LSP, LSP setup triggering between PE1 and PE2.

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

4.8 Troubleshooting MPLS L2VPN

Symptom 1:

Configuring Layer 2 VPN on a VLAN interface fails.

Solution:

- Check that MPLS/BGP VPN, WebSwitch, Multicast or VLL is not enabled on the interface.
- Check that the VLAN interface is not a Super VLAN or Sub-VLAN. You can configure Layer 2 VPN only on normal VLAN interfaces.

Symptom 2:

After configuring L2VPN, pinging peer end fails. Check the state of VC and find out that it is down. The value of Remote is invalid.

Solution:

Step 1: Check that the PEs at the two ends are using the same encapsulation type and MTU to have the VC go up.

Step 2: Check that the Remote parameter is configured at both ends and the remote addresses are correctly configured.

Security

Table of Contents

Chapter 1 Network Security Configuration

1.1 Introduction to the Network Security Features Provided by V 2.41

A router must be able to withstand the various malicious attacks from the public network. As sometimes, the accidental but destructive access of the user may also result in significant performance decrease and even the operation failure, its security seems more crucial.

3Com routers provide the following network security characteristics:

- AAA services based on Remote Authentication Dial-In User Service (RADIUS) provide the security services of Authentication, Authorization, and Accounting on accessing subscribers for preventing illegal accessing.
- Authentication protocol supports CHAP and PAP authentication on PPP line.
- Packet filter implemented through Access Control List (ACL) allows of specifying the type of packets that the router will permit or deny.
- Application Specific Packet Filter (ASPF), or status firewall, is an advanced communication filtering approach that checks the application layer information and monitors connection-oriented application layer protocol state, maintain the state information of each connection, and dynamically makes decision in permitting or deny a packet.
- IPSec (IP Security): it guarantees the privacy, integrity and validity of the data packets while transmitted on the Internet through encryption and data source authentication on the IP layer.
- IKE (Internet Key Exchange) provides the services of auto-negotiated key exchange and Security Association (SA) establishment to simplify the use and management of IPSec.
- Event log is used to record system security events and trace illegal access in real time.
- Address translation provided by NAT Gateway (GW), which separates the public network from the intranet, makes the IP addresses of the internal devices unknown to the public network and hence prevents the attacks initiated from it.
- Adjacent router authentication: ensuring reliable route information to be exchanged.
- Hierarchical view protection divides users into four levels, each assigned with a configuration right, and a user cannot access the view of a higher level.

In the following chapters tells you how to configure AAA and RADIUS, access control list, packet filter and IPSec/IKE. Refer to related parts for other contents: refer to PPP configuration in the link layer protocol part for PPP authentication protocol, networking protocol part for address translation, IP route part for adjacent router authentication.

1.2 Hierarchical Command Line Protection

The system command lines are protected in a hierarchical way. In this approach, the command lines are divided into viewing level, monitoring level, configuring level, and management level. You will be unable to use the commensurate level of commands unless you have provided the correct login password.

1.3 RADIUS-Based AAA

AAA is used for accessing user management. It can be implemented via multiple protocols but the AAA discussed here is RADIUS-based.

AAA provides the functions of:

- Hierarchical user management. The users are allowed to perform the operations like managing and maintaining the system configuration data, and monitoring and maintaining the equipment that are crucial to the normal operation of the system. Therefore, it is necessary to strictly manage the users by classifying them into different levels and granting each with a specific right. In this case, a low-level user is allowed to perform but only some viewing operations and only a high-level user can modify data, maintain the equipment, and perform some other sensitive operations. However, all the users must undergo the password authentication before they can access the system.
- PPP authentication. With it, user name authentication will be performed before the setup of a PPP connection is allowed.
- PPP address management and allocation. When setting up a PPP connection, the system may assign the IP address that has been specified to the PPP user.

The next chapter will cover the details of RADIUS protocol and its configurations, user password configuration, and PPP user address configuration. For PPP authentication protocols, refer to PPP Configuration in Part Link Layer Protocol (LLP) Configuration.

1.4 Packet Filter and Firewall

1.4.1 Firewall Concept

Firewall can prevent unauthorized or unauthenticated users on the Internet from accessing a protected network while allowing the users on the internal network to access web sites on the Internet and transceive E-mails. It can also work as an Internet access right control GW by permitting only some particular users inside the organization to access the Internet.

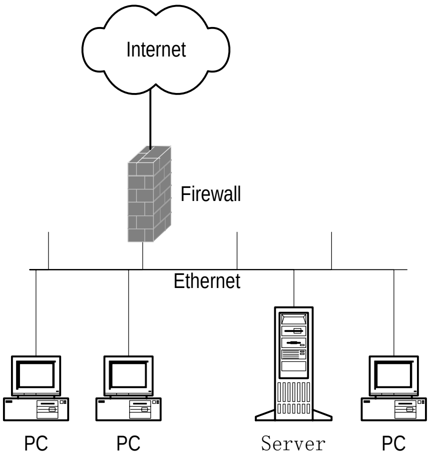


Figure 1-1 A firewall separating the intranet from the Internet

The firewall is not only applied to the Internet connection, but also used to protect the mainframe and crucial resources like data on the intranet of the organization. Access to the protected data should be permitted by the firewall, even if the access is initiated from the organization.

An external network user must pass through the firewall before it can access the protected network resources. Likewise, an intranet user must pass through the firewall before it can access the external network resources. Thus, the firewall plays the role of "guard" and discards the denied packets.

1.4.2 Firewall Classification

Normally, firewalls are classified into two categories: network layer firewalls and application layer firewalls. Network layer firewalls mainly obtain the header information of packet, such as protocol, source address, destination address, and destination port. Alternatively, they can directly obtain a segment of header data. The application layer firewalls, however, analyze the whole information traffic.

Firewalls that you often meet are divided into the following categories:

- Application gateway: It verifies all the application layer data in packets that will traverse it. Take a File Transfer Protocol (FTP) application GW as an example. From the perspective of the client of a connection, the FTP application GW is an FTP server. But from the perspective of the server, it is an FTP client. All the FTP packets transmitted on the connection must pass this FTP application GW.
- Circuit-Level Gateway: The "circuit" in this particular context refers to Virtual Circuit (VC). Before TCP or UDP is allowed to open a connection or VC, the session reliability must be verified. The packet transmission is allowed only if the handshake has been proved valid and accomplished. After a session is set up, its information will be written into the valid connection table maintained by the firewall. A packet can be permitted only if the session information carried by it matches an

entry in the valid connection table. After the session is terminated, the session entry will be deleted from the table. Circuit-level GW authenticates a connection only at the session layer. If the authentication is passed, any application can be run on the connection. Take FTP as an example. A circuit-level GW only authenticates an FTP session at the TCP layer at the beginning of the session. If the authentication is passed, all the data can be transmitted on this connection until the session is terminated.

- Packet filter: Such a firewall filters each packet depending on the items that defined by the user. For example, it compares the packets with the defined rules in source and destination addresses for a match. A packet filter neither considers the status of sessions, nor analyzes the data. If the user specifies that the packets carrying port number 21 or a port number no less than 1024 are permitted, all the packets matching the condition will be able to pass through the firewall. If the configured rules are properly set for the actual applications, many packets that bring potential threat to the security can be filtered at this layer.
- Network Address Translation: Also called address proxy, NAT makes it possible for a private network to access an external network. The NAT mechanism is to substitute an external network address and port of router for the IP address and port of a host on a private network and vice versa. In other words, it fulfills the conversion between <Private address + Port number> and <Public address + Port number>. The private address discussed here refers to an internal network or host address, and public address refers to a globally unique IP address on the Internet. Internet Assigned Number Authority (IANA) provisioned that that the following IP address ranges are reserved for private addresses:

10.0.0.0 to 10.255.255.255

172.16.0.0 to 172.31.255.255

192.168.0.0 to 192.168.255.255

In other words, the addresses in these three ranges will be used inside an organization or companies rather than assigned on the Internet. A company can select a proper internal network address ranges, taking into consideration the number of the internal hosts and networks in the near future. The internal network addresses of different companies can be the same. However, it will be very likely to cause chaos if a company selects a segment beyond the three ranges given above as the internal network address. NAT allows internal hosts to access the Internet resources while keeping their “privacy”.

1.4.3 Packet Filter

I. Function

Normally, a packet filter filters the IP packets. For the packets that the router will forward, the filter will first obtain the header information of each packet, including upper protocol carried by the IP layer, source and destination addresses of the packet, and source and destination ports. Then, it compares them with the preset rules to determine whether the packet should be forwarded or discarded.

Figure 1-2 illustrates the elements selected by a packet filter for decision making (on IP packets), given the upper layer carried by IP is TCP/UDP.

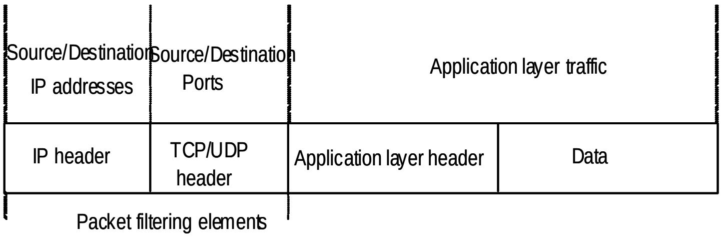

Source/Destination IP addresses
Source/Destination Ports
Application layer traffic
IP header
TCP/UDP header
Application layer header
Data
Packet filtering elements

Figure 1-2 Packet filtering elements

Most packet filter systems do not make any operations on data itself or make contents-based filtering.

II. ACL

Before the system can filter the packets, you should configure some rules in ACLs to specify the types of packets allowed or denied.

A user should configure an ACL according to the security policy and apply it to a particular interface or the whole equipment. After that, the router will examine all the packets on the interface or all the interfaces based on the ACL and make forwarding/discard decision on the packets matching the rules. In this way, it plays the role of a firewall.

The ACL for packet filtering and the complicated traffic classification rules for QoS are processed together. The fundamentals and operations of them are the same except of the actions taken after the matching.

1.5 Security Authentication before Route Information Exchange

As far as a backbone router is concerned, a correctly maintained forwarding table is essential to the proper operation of the router. The maintenance of route forwarding table depends on the dynamic route information exchanging between neighboring routers.

I. Necessity of implementing security authentication before route information exchange

As the neighboring routers on a network need to exchange enormous route information, there is the likelihood for a router to receive the network equipment attacking information sent from unreliable routers. If available with the route authentication function, a router will be able to authenticate the switching route update packets received from the neighboring routers and hence make sure to receive only the reliable route information.

II. Authentication Implementation

The routers exchanging route information share the same password key that is sent along with the route information packets. The routers receiving the route information will authenticate the packets, and verify the password key carried by the packets. If the key carried by the packets is the same as the shared password key, the packets will be accepted. If not, they will be discarded.

Authentication implementations fall into simple text authentication and MD5 authentication. The former sends password keys in plain text providing lower security, whereas the latter sends encrypted password keys providing higher security.

Chapter 2 AAA and RADIUS/HWTACACS Protocol Configuration

2.1 Overview

2.1.1 Introduction to AAA

Authentication, Authorization and Accounting (AAA) provide a uniform framework used for configuring these three security functions to implement the network security management.

The network security mentioned here refers to access control and it includes:

- Which user can access the network server?
- Which service can the authorized user enjoy?
- How to keep accounts for the user who is using network resource?

Accordingly, AAA provides the following services:

I. Authentication

AAA supports the following authentication methods:

- None authentication: All users are trusted and are not authenticated. Generally, this method is not recommended.
- Local authentication: User information (including username, password, and attributes) is configured on the Broadband Access Server (BAS). Local authentication features high speed but low cost; the information stored in this approach is however limited depending on the hardware capacity.
- Remote authentication: Supports both RADIUS and HWTACACS protocols. In this approach, the BAS acts as the client to communicate with the RADIUS or TACACS server. With respect to RADIUS, you can use the standard RADIUS protocol or Huawei extended RADIUS protocol to complete authentication in collaboration with devices like iTELLIN/CAMS.

II. Authorization

AAA supports the following authorization methods:

- Direct authorization: All users are trusted and directly authorized to pass.
- Local authorization: Users are authorized according to the attributes related to their accounts on the BAS.
- HWTACACS authorization: Users are authorized using a TACACS server.
- If-authenticated authorization: Users are authorized to pass if they are authenticated and using any allowed method other than none authentication.

- RADIUS authorization following successful authentication: With RADIUS, users are authorized only after they pass authentication. In other words, you cannot perform RADIUS authorization without authentication.

III. Accounting

AAA supports the following accounting methods:

- None accounting: does not require accounting.
- Remote accounting: conducted through a RADIUS server or TACACS server.

AAA usually utilizes a Client/Server model, where the client is the router that controls user access and the server stores user information. The framework of AAA thus allows for good scalability and centralized user information management. Being a management framework, AAA can be implemented using multiple protocols. In V 2.41, AAA is implemented based on RADIUS or HWTACACS.

2.1.2 Introduction to the RADIUS Protocol

I. What is RADIUS

Remote Authentication Dial-In User Service (RADIUS) is a distributed information switching protocol in Client/Server model. RADIUS can prevent the network from interruption of unauthorized access and it is often used in the network environments where both high security and remote user access are required. For example, it is often used for managing a large number of scattered dial-in users that use serial ports and modems. The RADIUS system is an important auxiliary part of a Network Access Server (NAS).

The RADIUS service involves three components:

- Protocol: Based on the UDP/IP layer, RFC2865 and RFC2866 define the RADIUS frame format and the message transfer mechanism, and use 1812 as the authentication port and 1813 as the accounting port.
- Server: RADIUS server runs on the computer or workstation at the center, and contains information on user authentication and network service access.
- Client: Located at the Network Access Server (NAS) side. It can be placed anywhere in the network.

As the RADIUS client, the NAS (a router for example) is responsible for passing user information to a designated RADIUS server and acts on the response returned from the server (such as connecting/disconnecting users). The RADIUS server receives user connection requests, authenticates users, and returns the required information to the NAS.

In general, the RADIUS server maintains three databases, namely, Users, Clients and Dictionary, as shown in the following figure. “Users” stores user information such as username, password, applied protocols, and IP address; “Clients” stores information about RADIUS clients such as shared key; and "Dictionary" stores the information for interpreting RADIUS protocol attributes and their values.

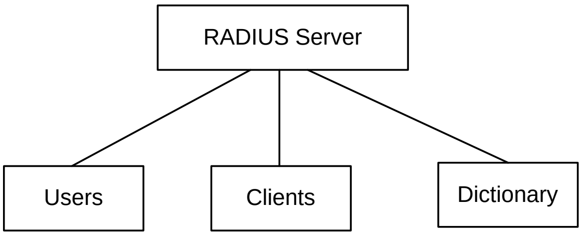


Figure 2-1 Components of RADIUS server

In addition, RADIUS servers can act as the client of some other AAA servers to provide the proxy authentication or accounting service. They support multiple user authentication methods, such as PPP-based PAP, CHAP and UNIX-based login.

II. Basic message exchange procedures in RADIUS

In most cases, user authentication using a RADIUS server always involves a device that can provide the proxy function, such as the NAS. Transactions between the RADIUS client and RADIUS server are authenticated through a shared key, and user passwords are sent encrypted over the network for the security sake. The RADIUS protocol combines the authentication and authorization processes by sending authorization information in the authentication response message. See the following figure.

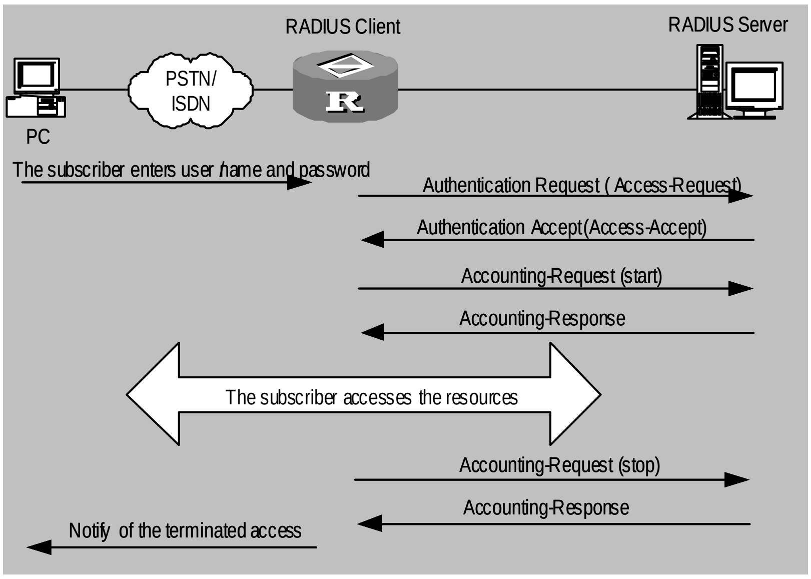

RADIUS Client
RADIUS Server
PSTN/
ISDN
PC
The subscriber enters user name and password
Authentication Request (Access-Request)
Authentication Accept(Access-Accept)
Accounting-Request (start)
Accounting-Response
The subscriber accesses the resources
Accounting-Request (stop)
Accounting-Response
Notify of the terminated access

Figure 2-2 The basic message interaction procedures of RADIUS

Following is how RADIUS operates:

1) The user enters the username and password.

Having received the username and password, the RADIUS client sends the authentication request (Access-Request) to the RADIUS server.

2) The RADIUS server compares the received user information against that in the Users database. If the authentication succeeds, it sends back an authentication response (Access-Accept) containing the information of user's right. If the authentication fails, it returns an Access-Reject message.
3) The RADIUS client acts on the returned authentication result to accept or deny the user. If it is allowed to accept the user, the RADIUS client sends an accounting start request (Accounting-Request) to the RADIUS server, with the value of Status-Type being "start".
4) The RADIUS server returns a start-accounting response (Accounting-Response).
5) The RADIUS client sends a stop-accounting request (Accounting-Request) to the RADIUS server, with the value of Status-Type being "stop".
6) The RADIUS server returns a stop-accounting response (Accounting-Response).

III. RADIUS packet structure

RADIUS uses UDP to transmit messages; with timer management, retransmission, and slave server mechanisms, it ensures the smooth message exchange between the RADIUS server and the client. The following figure shows the RADIUS packet structure.

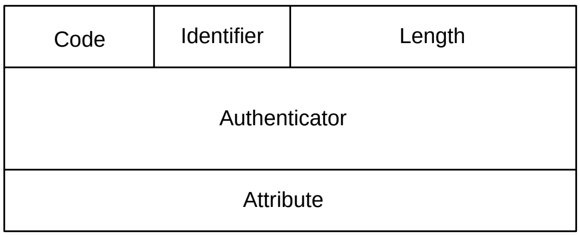


Figure 2-3 RADIUS packet structure

The Identifier field is used for matching request packets and response packets. It varies with the Attribute field and the received valid response packets, but keeps unchanged during retransmission. The 16-byte Authenticator field is used to authenticate the request transmitted by the RADIUS server, and it also applies to the password hidden algorithm. There are two kinds of authenticators: Request and Response.

- Request Authenticator is the random code of 16 bytes in length.
- Response Authenticator is the result of applying the MD5 algorithm to Code, Identifier, Request Authenticator, Length, Attribute and shared-key.

1) The Code field decides the type of a RADIUS packet, as shown in the following table.

Table 2-1 Code values

Code	Packet type	Description
1	Access-Request	The packet carries user information and is transmitted by the client to the server to help the client determine whether the user can access the network. The packet carries the required attribute of User-Name and some other options, such as NAS-IP-Address, User-Password, and NAS-Port.
2	Access-Accept	The packet is transmitted by the server to the client. If all the attribute values carried in the Access-Request are acceptable, the server allows the user to pass authentication and sends back an Access-Accept response.
3	Access-Reject	The packet is transmitted by the server to the client. If any attribute value carried in the Access-Request is unacceptable, the server rejects the user and sends back an Access-Reject response.
4	Accounting-Request	The packet carries user information and is transmitted by the client to the server to request the server to start accounting. The server can determine whether to start accounting according to the field of the Acct-Status-Type attribute. The attributes carried in this type of packet are basically the same as those carried by an Access-Request packet.
5	Accounting-Response	The packet is transmitted by the server to the client, notifying that the server has received the Accounting-Request and has correctly recorded the accounting information. The packet carries such information as input/output bytes and packets, and session duration.

2) The Attribute field contains special authentication, authorization, and accounting information that provides the configuration details of a request or response. This field is represented by the triplet of Type and Length and Value. The following table lists the major standard attribute values defined by RFC:

Table 2-2 Attribute values

Type	Attribute type	Type	Attribute type
1	User-Name	23	Framed-IPX-Network
2	User-Password	24	State
3	CHAP-Password	25	Class
4	NAS-IP-Address	26	Vendor-Specific

Type	Attribute type	Type	Attribute type
5	NAS-Port	27	Session-Timeout
6	Service-Type	28	Idle-Timeout
7	Framed-Protocol	29	Termination-Action
8	Framed-IP-Address	30	Called-Station-Id
9	Framed-IP-Netmask	31	Calling-Station-Id
10	Framed-Routing	32	NAS-Identifier
11	Filter-ID	33	Proxy-State
12	Framed-MTU	34	Login-LAT-Service
13	Framed-Compression	35	Login-LAT-Node
14	Login-IP-Host	36	Login-LAT-Group
15	Login-Service	37	Framed-AppleTalk-Link
16	Login-TCP-Port	38	Framed-AppleTalk-Network
17	(unassigned)	39	Framed-AppleTalk-Zone
18	Reply_Message	40-59	(reserved for accounting)
19	Callback-Number	60	CHAP-Challenge
20	Callback-ID	61	NAS-Port-Type
21	(unassigned)	62	Port-Limit
22	Framed-Route	63	Login-LAT-Port

The RADIUS protocol is extensible. The Attribute 26 (Vender-Specific) defined in it allows a user to define an extended attribute. The following figure illustrates the structure of a RADIUS packet:

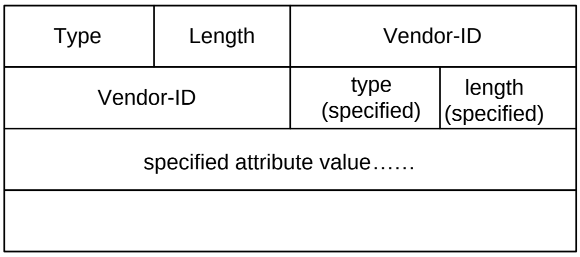


Figure 2-4 A RADIUS packet segment containing the extended attribute

2.1.3 Introduction to the HWTACACS Protocol

I. What is HWTACACS

HWTACACS is an enhanced security protocol based on TACACS (RFC1492). Similar to the RADIUS protocol, it implements AAA for different types of users (such as PPP/VPDN/login users) through communications with TACACS servers in the Server/Client model.

Compared with RADIUS, HWTACACS provides more reliable transmission and encryption, and therefore is more suitable for security control. The following table lists the primary differences between HWTACACS and RADIUS protocols.

Table 2-3 Comparison between HWTACACS and RADIUS

HWTACACS	RADIUS
Adopts TCP, providing more reliable network transmission.	Adopts UDP.
Encrypts the entire packet except for the standard HWTACACS header.	Encrypts only the password field in authentication packets.
Separates authentication from authorization. For example, you can provide authentication and authorization on different TACACS servers.	Brings together authentication and authorization.
Suitable for security control.	Suitable for accounting.
Supports to authorize the use of configuration commands.	Not supports.

In a typical HWTACACS application, a dial-up or terminal user needs to log onto the router for operations. Working as the client of HWTACACS in this case, the router sends the username and password to the TACACS server for authentication. After passing authentication and being authorized, the user can log onto the router to perform operations, as shown in the following figure.

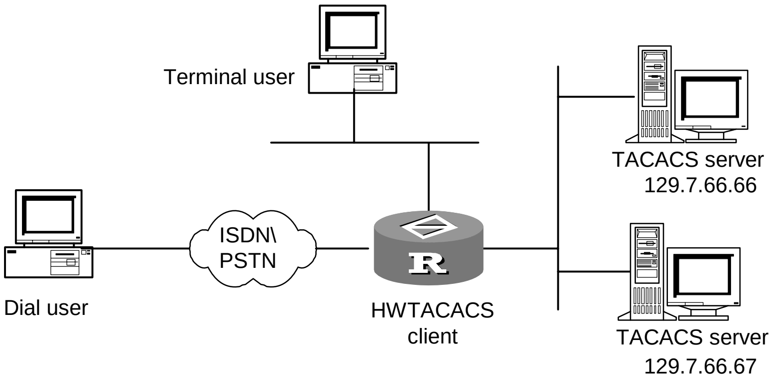


Figure 2-5 Network diagram for a typical HWTACACS application

II. Basic message exchange procedures in HWTACACS

For example, use HWTACACS to implement authentication, authorization, and accounting for a telnet user. The basic message exchange procedures are as follows:

1) A user requests access to the router; the TACACS client sends a start-authentication packet to TACACS server upon receipt of the request.
2) The TACACS server sends back an authentication response requesting for the username; the TACACS client asks the user for the username upon receipt of the response.
3) The TACACS client sends an authentication continuance packet carrying the username after receiving the username from the user.
4) The TACACS server sends back an authentication response, requesting for the login password. Upon receipt of the response, the TACACS client requests the user for the login password.
5) After receiving the login password, the TACACS client sends an authentication continuance packet carrying the login password to the TACACS server.
6) The TACACS server sends back an authentication response indicating that the user has passed the authentication.
7) The TACACS client sends the user authorization packet to the TACACS server.
8) The TACACS server sends back the authorization response, indicating that the user has passed the authorization.
9) Upon receipt of the response indicating an authorization success, the TACACS client pushes the configuration interface of the router to the user.
10) The TACACS client sends a start-accounting request to the TACACS server.
11) The TACACS server sends back an accounting response, indicating that it has received the start-accounting request.
12) The user logs off; the TACACS client sends a stop-accounting request to the TACACS server.
13) The TACACS server sends back a stop-accounting packet, indicating that the stop-accounting request has been received.

The following figure illustrates the basic message exchange procedures:

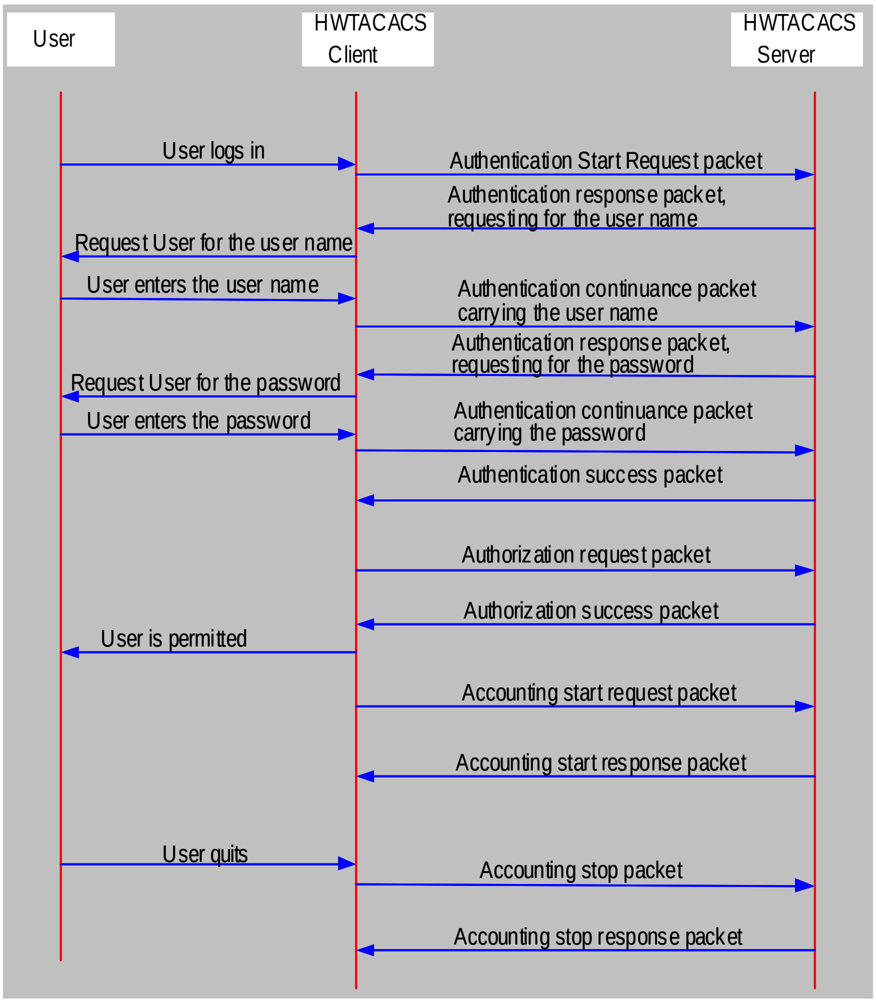

User
HWTACACS Client
HWTACACS Server
User logs in
Authentication Start Request packet
Authentication response packet, requesting for the user name
Request User for the user name
User enters the user name
Authentication continuance packet carrying the user name
Authentication response packet, requesting for the password
Request User for the password
User enters the password
Authentication continuance packet carrying the password
Authentication success packet
Authorization request packet
Authorization success packet
User is permitted
Accounting start request packet
Accounting start response packet
User quits
Accounting stop packet
Accounting stop response packet

Figure 2-6 The AAA implementation procedures for a telnet user

Note:

As the V 2.41 software is designed compatible with the configurations of LAN switches, you can probably see in the HyperTerminal some commands and parameters that are only supported by LAN switches when configuring your router. These commands and parameters are beyond the scope of this manual.

2.2 Configuring AAA

AAA configuration tasks include:

1) Create an ISP domain and set the related attributes

- Create an ISP domain
- Configure an AAA scheme

- Configure the ISP domain state
- Set an access limit
- Enable accounting optional
- Define a local IP pool and allocate IP addresses to PPP users

2) Create a local user and set the related attributes (for local authentication only)

2.2.1 Creating an ISP Domain and Setting the Related Attributes

I. Creating an ISP domain

An Internet service provider (ISP) domain is a group of users that belong to the same ISP. For a username in the *userid@isp-name* format, gw20010608@huawei163.net for example, the isp-name (huawei163.net) following the @ sign is the ISP domain name. When receiving a connection request from a user named *userid@isp-name*, the router system considers the *userid* part as the username for authentication and the *isp-name* part as the domain name.

The purpose of introducing ISP domain settings is to support the multi-ISP application environment, where one access device might access users of different ISPs. Because the attributes of ISP users, such as username and password formats, can be different, you must differentiate them through setting ISP domains. In ISP domain view, you can configure a complete set of exclusive ISP domain attributes on a per-ISP domain basis, including an AAA scheme.

For 3Com Series Routers, each supplicant belongs to an ISP domain. Up to 16 domains can be configured in the system. If a user has not reported its ISP domain name, the system puts it into the default domain.

Perform the following configurations in system view.

Table 2-4 Create/delete an ISP domain

Operation	Command
Create an ISP domain or enter the view of a specified domain.	**domain** [*isp-name* | **default** { **disable** | **enable** *isp-name* }]
Remove a specified ISP domain.	**undo domain** *isp-name*

By default, the default ISP domain in the system is system.

II. Configuring an AAA scheme for an domain to reference

You can configure authentication, authorization, and accounting schemes in two modes:

1) Bundled mode

In bundled mode, you can specify an AAA scheme by using the **scheme** command. If you specify a RADIUS or HWTACAS scheme, all of the authentication, authorization, and accounting are accomplished by the specified RADIUS or HWTACAS scheme. That is, you cannot specify a separate scheme for authentication, authorization, or accounting.

If you specify to use the local authentication scheme, only authentication and authorization are implemented, and no accounting is implemented.

If you configure the **scheme radius-scheme** *radius-scheme-name* **local** or **scheme authentication hwtacacs-scheme** *hwtacacs-scheme-name* **local** command, the local authentication scheme is the alternate scheme for use when the RADIUS server or TACACS server is not responding properly. That is, the local authentication scheme is used only when the RADIUS server or TACACS server is not available.

If you want the system to use the local scheme as the first scheme, the local authentication scheme is the only scheme for authentication, and you cannot configure any RADIUS or HWTACACS scheme at the same time, or configure to use no authentication scheme. That is, you can only specify the **local** keyword in the **scheme** command. The same is true for the **none** keyword.

Perform the following configuration in ISP domain view.

Table 2-5 Configure the related attributes of the ISP domain

Operation	Command
Configure an AAA scheme for the domain.	**scheme** { **radius-scheme** *radius-scheme-name* [**local**] | **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** }
Restore the default AAA scheme.	**undo scheme** [**radius-scheme** | **hwtacacs-scheme** | **none**]

The default AAA scheme is **local**.

2) Separated mode

In separated mode, you can use the **authentication**, **authorization**, and the **accounting** commands to configure schemes for authentication, authorization, and accounting separately. For example, you can configure the system to use a RADIUS scheme for authentication and authorization and a HWTACACS scheme for accounting optionally. This mode supports more flexible and rich combinations of schemes.

The following describes details about the implementation of services supported by AAA in separated mode.

- For terminal users

Authentication: The scheme can be RADIUS, HWTACACS, local, RADIUS and local, HWTACACS and local, or none.

Authorization: The scheme can be HWTACACS or none.

Accounting: The scheme can be RADIUS, HWTACACS, or none.

You can configure any combination of the above schemes for authentication, authorization, and accounting of terminal users.

- For FTP users

For FTP users, only authentication is supported.

The authentication scheme can be RADIUS, HWTACACS, local, RADIUS and local, or HWTACACS-local.

- For PPP and L2TP users

Authentication: The scheme can be RADIUS, HWTACACS, local, RADIUS and local, HWTACACS and local, or none.

Authorization: The scheme can be HWTACACS or none.

Accounting: The supported scheme can be RADIUS, HWTACACS, or none.

You can configure any combination of the above schemes for authentication, authorization, and accounting of PPP and L2TP users.

- For portal services

Only RADIUS authentication and accounting are supported.

- For DVPN services

Authentication and authorization: Only RADIUS, local, and RADIUS and local schemes are supported.

Accounting: Only RADIUS scheme is supported.

Perform the following configuration in ISP domain view.

Table 2-6 Configure the related attributes of the ISP domain

Operation	Command
Configure an authentication scheme for the domain	**authentication** { **radius-scheme** *radius-scheme-name* [**local**] | **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** }
Restore the default authentication scheme of the domain	**undo authentication**
Configure an authentication scheme for the domain	**authorization** { **hwtacacs-scheme** *hwtacacs-scheme-name* | **none** }
Restore the default authentication scheme of the domain	**undo authorization**
Configure an accounting scheme for the domain	**accounting** { **radius-scheme** *radius-scheme-name* | **hwtacacs-scheme** *hwtacacs-scheme-name* | **none** }

Operation	Command
Remove the accounting scheme used by the domain	**undo accounting**

By default, no separate authentication, authorization, or accouting scheme is available.

Note that:

1) If both separate and bundled authentication, authorization, and accounting schemes are configured, the separate authentication, authorization, and accounting schemes are preferred.
2) Since RADIUS and local schemes do not support the separate of authentication and authorization, pay attention to the following when configuring authentication and authorization:

- If you configure the **scheme radius-scheme** or **scheme local** command for a domain without configuring the **authentication** command:

  a. If you have configured the **authorization none** command, the authorization information returned by the RADIUS and local schemes are still valid.

  b. If you have configured the **authorization hwtacacs** command, the HWTACACS scheme will be employed for authorization.

- If you configure both the **scheme radius-scheme** or **scheme local** command and the **authentication hwtacacs-scheme** command, the HWTACACS scheme will be employed for authentication, but no authorization will be performed.

III. Configuring the ISP domain state

Every ISP has active/block states. If an ISP domain is in active state, the users in it can request for network service, while in block state, its users cannot request for any network service, which will not affect the users already online. An ISP is in the active state when it is first created. Users in the domain are allowed to request network service.

Perform the following configuration in ISP domain view.

Table 2-7 Configure the ISP domain state

Operation	Command
Configure the ISP domain state.	**state** { **active** | **block** }

By default, an ISP domain is active when it is created.

IV. Setting an access limit

You can specify the maximum number of users that an ISP domain can accommodate by setting an access limit. For any ISP domain, there is no access limit by default.

Perform the following configuration in ISP domain view.

Table 2-8 Configure an access limit

Operation	Command
Set an access limit to limit the number of users that the domain can accommodate.	**access-limit** { **disable** | **enable** *max-user-number* }
Restore the default value.	**undo access-limit**

By default, an ISP domain has no limit on the user number upon its creation.

V. Enabling accounting optional

If a user is configured with **accounting optional**, the router does not disconnect the user during the accounting even when it finds no available accounting server or fails to communicate with the accounting server.

Unlike the **scheme none** command, with the **accounting optional** command, the system sends accounting information to the accounting server but does not terminate the connection regardless of whether the accounting server responds or performs the accounting service. However, with the **scheme none** command, the system neither sends accounting information to the accounting server nor terminates the connection. If you specify RADIUS or HWTACACS in the **scheme** command without configuring **accounting optional**, the system sends accounting information to the accounting server and if the server does not respond or perform accounting service terminates the connection.

Perform the following configuration in ISP domain or RADIUS view.

Table 2-9 Enable/disable accounting optional

Operation	Command
Enable accounting optional.	**accounting optional**
Disable accounting optional.	**undo accounting optional**

By default, when an ISP domain is created, accounting optional is disabled.

VI. Defining an address pool and allocating IP addresses to PPP domain users

PPP users can obtain IP addresses from the router through PPP address negotiation. Three approaches are available for address allocation on an interface:

- Directly allocate IP addresses on the interface without configuring an address pool.

- Define an address pool in system view and assign it (only one is allowed) to the interface in the view of this interface for assigning addresses to the connected ends.
- Define address pools in domain view and directly allocate the addresses from the pools to the login domain PPP users.

The first two approaches apply to the situation where PPP users are not authenticated; for the configuration procedures, see the part of PPP configuration in *V 2.41 Operation Manual – Link Layer Protocol*. The last approach applies to the situation where PPP users are authenticated; for the configuration procedures, see the following.

Perform the following configuration in ISP domain view.

Table 2-10 Define an IP address pool for PPP domain users

Operation	Command
Define an IP address pool for allocating addresses to PPP users.	**ip pool** *pool-number low-ip-address* [*high-ip-address*]
Delete the specified address pool.	**undo ip pool** *pool-number*

By default, no address pool is configured.

The following are the principles of IP address allocation to PPP users in AAA:

1) For a domain user with a name either in the form of userid or userid@default, the address is allocated as follows:

- If RADIUS or TACACS authentication/authorization applies, the address that the server has issued to the user is allocated, if there is any.
- If the server issues an address pool instead of an address, the router searches the address pool in domain view for an address.
- In case no address can be allocated with the above two methods or local authentication is used, the router searches the address pool in domain view for an address and allocates it to the user if one is found.

2) For a user that is not to be authenticated, the router allocates address using the specified address pool (defined in system view) on the interface.

2.2.2 Creating a Local User and Setting the Related Attributes

Create a local user and configure the related attributes on the router if you select the local authentication scheme in AAA.

Note:

If you use a radius-scheme or hwtacacs-scheme to authenticate users, you must appropriately configure the RADIUS or TACACS server (whether it can be configured and how are decided by the server); the local configuration in this case has no effect.

I. Creating a local user

A local user is a group of users set on NAS (a router). The username is the unique identifier of a user. A user requesting network service can pass local authentication as long as its information has been added to the local user database of NAS.

Perform the following configuration in system view

Table 2-11 Create/delete a local user and the relevant properties

Operation	Command
Add a local user.	**local-user** *user-name*
Delete a local user by specifying its type.	**undo local-user** { *user-name* **|** **all** }

By default, there is no local user in the system.

II. Setting attributes of a local user

The attributes of a local user include user password display mode, user password, user state, and the type of service that is authorized to the user.

Perform the following configuration in system view.

Table 2-12 Set the password display mode for local users

Operation	Command
Set the password display mode for all local users.	**local-user password-display-mode** { **cipher-force** **|** **auto** }
Cancel the password display mode for local users.	**undo local-user password-display-mode**

Where, **auto** means that the password display mode will be the one specified by the user at the time of configuring password (see the **password** command in the following table for reference), and **cipher-force** means that the password display mode of all the accessing users must be in cipher text.

Perform the following configurations in local user view.

Table 2-13 Set/remove the attributes concerned with a specified user

Operation	Command
Set a password for a specified user.	**password** { **simple** | **cipher** } *password*
Remove the password set for the specified user.	**undo password**
Set the state of the specified user.	**state** { **active** | **block** }
Remove the state of the specified user.	**undo state** { **active** | **block** }
Set a service type for the specified user.	**service-type** { **dvpn** | **telnet** | **ssh** | **terminal** | **pad** }
Cancel a service available for users.	**undo service-type** { **dvpn** | **telnet** | **ssh** | **terminal** | **pad** }
Set a priority level for the user.	**level** *level*
Restore the default priority level.	**undo level**
Set the directory that can be accessed if the user is an FTP user.	**service-type ftp** [**ftp-directory** *directory*]
Restore the default directory that can be accessed if the user is an FTP user.	**undo service-type ftp** [**ftp-directory**]
Set the attributes of callback number and call number of PPP users.	**service-type ppp** [**callback-nocheck** | **callback-number** *callback-number* | **call-number** *call-number* [*subcall-number*]]
Restore the default callback number and call number of PPP users.	**undo service-type ppp** [**callback-nocheck** | **callback-number** | **call-number**]

By default, no service is authorized to users. The default user priority level is 0.

Note:

- If the configured authentication method requires username and password (including local, RADIUS, and HWTACACS authentication), your user priority determines which level of commands you can access after logging onto the system. If the authentication method is none or only requires password, your interface priority determines which level of commands you can access.
- The ciphertext password set by the **password cipher** command is 64 characters long in V 2.41 RT-0011 or later versions, but it is only 24 characters long in ealier versions. As this may cause password loss when you downgrade V 2.41 RT-0011 or later versions to an ealier version of V 2.41 RT-0011, you are recommended to back up your configuration file before doing that.

2.3 Configuring the RADIUS Protocol

The RADIUS protocol is configured scheme by scheme. In a real networking environment, a RADIUS scheme can comprise an independent RADIUS server or a pair of primary and secondary RADIUS servers with the same configuration but different IP addresses. Accordingly, attributes of every RADIUS scheme include IP addresses of primary and secondary servers, shared key, and RADIUS server type.

Actually, the RADIUS protocol configurations only define the parameters necessary for the information interaction between a NAS and a RADIUS server. To validate these parameter settings, you also need to reference the RADIUS scheme containing those parameter settings in ISP domain view. For more information about the configuration commands, refer to the section “2.2 Configuring AAA”.

RADIUS protocol configuration includes:

- Create a RADIUS scheme
- Configure RADIUS authentication/authorization servers
- Configure RADIUS accounting servers and the related attributes
- Configure the shared key for RADIUS packet encryption
- Set the maximum number of RADIUS request attempts
- Set the supported RADIUS server type
- Set RADIUS server state
- Set the username format acceptable to the RADIUS server
- Set the unit of data flows destined for the RADIUS server
- Configure the source address in the RADIUS packets sent by NAS
- Set timers regarding RADIUS server
- Enable the RADIUS server to send traps when it goes down

Among these tasks, creating a RADIUS scheme and configuring RADIUS authentication/authorization servers are required, while other tasks are optional at your discretion.

2.3.1 Creating a RADIUS Scheme

As mentioned earlier, the RADIUS protocol is configured scheme by scheme. Therefore, before performing other RADIUS protocol configurations, you must create a RADIUS scheme and enter its view.

You can use the following commands to create/delete a RADIUS scheme.

Perform the following configurations in system view.

Table 2-14 Create/delete a RADIUS scheme

Operation	Command
Create a RADIUS scheme and enter its view.	**radius scheme** *radius-scheme-name*

Operation	Command
Delete a RADIUS scheme.	**undo radius scheme** *radius-scheme-name*

A RADIUS scheme can be referenced by several ISP domains at the same time.

By default, the system has a RADIUS scheme named system whose attributes are all default values.

⚠ **Caution:**

FTP, terminal, and SSH are not standard attribute values of the RADIUS protocol, so you need to define them in the attribute login-service (the standard attribute 15):
login-service(50) = SSH
login-service(51) = FTP
login-service(52) = Terminal
After that, reboot the RADIUS server to validate them.

2.3.2 Configuring RADIUS Authentication/Authorization Servers

You can use the following commands to configure IP address and port number of RADIUS authentication/authorization servers.

Perform the following configuration in RADIUS view.

Table 2-15 Configure IP address and port number of RADIUS authentication/authorization servers

Operation	Command
Configure IP address and port number of the primary RADIUS authentication/authorization server.	**primary authentication** *ip-address* [*port-number*]
Restore IP address and port number of the primary RADIUS authentication/authorization server to the default values.	**undo primary authentication**
Configure IP address and port number of the secondary RADIUS authentication/authorization server.	**secondary authentication** *ip-address* [*port-number*]
Restore IP address and port number of the secondary RADIUS authentication/authorization server to the default values.	**undo secondary authentication**

As the authorization information from the RADIUS server is sent to RADIUS clients in authentication response packets, so you do not need to specify a separate authorization server.

In real networking environments, you may specify two RADIUS servers as primary and secondary authentication/authorization servers respectively, or specify one server to function as both.

2.3.3 Configuring RADIUS Accounting Servers and the Related Attributes

I. Configuring RADIUS accounting servers

You can use the following commands to configure IP address and port number of RAIUDS accounting servers.

Perform the following configuration in RADIUS view.

Table 2-16 Configure IP address and port number of RADIUS accounting servers

Operation	Command
Configure IP address and port number of the primary RADIUS accounting server.	**primary accounting** *ip-address* [*port-number*]
Restore the default IP address and port number of the primary RADIUS accounting server.	**undo primary accounting**
Configure IP address and port number of the secondary RADIUS accounting server.	**secondary accounting** *ip-address* [*port-number*]
Restore the default IP address and port number of the secondary RADIUS accounting server.	**undo secondary accounting**

In practice, you can specify two RADIUS servers as the primary and the secondary accounting servers respectively; or specify one server to function as both.

For normal interaction between the NAS and a RADIUS server, you must ensure the connectivity of the routes between the RADIUS server and the NAS before configuring the IP address and UDP port of the RADIUS server. In addition, since RADIUS uses different UDP ports for authentication/authorization and accounting, you must assign different numbers to the authentication/authorization port and the accounting port, which are 1812 and 1813 respectively as recommended by RFC2138/2139. You can assign port numbers different from the two recommended in the RFC, however. (For example, in the early stage of RADIUS server implementation, 1645 and 1646 were often assigned to the authentication/authorization port and accounting port). When doing this, make sure that the port settings on the router and the RADIUS server are consistent.

By default, IP address of the primary/secondary accounting server is 0.0.0.0; the UDP port number of the accounting server is 1813.

II. Enabling the stop-accounting packet buffer and retransmission

Since the stop-accounting packet affects the bill and eventually the charge to a user, it has importance for both users and the ISP. Therefore, the NAS should make its best effort to send every stop-accounting packet to the RADIUS accounting server. If the NAS receives no response from the RADIUS accounting server to a stop-accounting packet that it has sent for a specified period of time, it buffers and resends the packet until the RADIUS accounting server responds, or discards the packet if the number of transmission attempts reaches the configured limit. You can use the following commands to enable the NAS to buffer stop-accounting packets and set the maximum number of transmission attempts.

Perform the following configuration in RADIUS view.

Table 2-17 Enable the stop-accounting packet buffer and set the maximum number of transmission attempts

Operation	Command
Enable the stop-accounting packet buffer.	**stop-accounting-buffer enable**
Disable the stop-accounting packet buffer.	**undo stop-accounting-buffer enable**
Enable stop-accounting packet retransmission and specify the maximum number of transmission attempts.	**retry stop-accounting** *retry-times*
Restore the default maximum number of transmission attempts.	**undo retry stop-accounting**

By default, the stop-accounting packet buffer is enabled and the maximum number of packet transmission attempts is 500.

III. Configuring the maximum number of real-time accounting request attempts

A RADIUS server usually determines the online state of a user using the connection timeout timer. If the RADIUS sever receives no real-time accounting packets from the NAS for a long time, it considers that the line or device fails and stops user accounting. To work with this feature of the RADIUS server, the NAS is required to terminate user connections simultaneously with the RADIUS server when unpredictable faults occur. 3Com Series Routers allow you to set the maximum number of continuous real-time accounting request attempts. The NAS terminates a user connection if it receives no response after the number of transmitted real-time accounting requests exceeds the configured limit.

You can use the following command to set the maximum number of real-time accounting request attempts.

Perform the following configuration in RADIUS view.

Table 2-18 Set the maximum number of real-time accounting request attempts

Operation	Command
Set the maximum number of real-time accounting request attempts.	**retry realtime-accounting** *retry-times*
Restore the default maximum number of real-time accounting request attempts.	**undo retry realtime-accounting**

Set the connection timeout time on the RADIUS server to T, the real-time accounting interval on NAS to t. Then, the *retry-times* of NAS is the rounded value of T divided by t. So you should set T to a number that can be divided exactly by t.

By default, the maximum number of real-time accounting request attempts is 5.

2.3.4 Setting the Shared Key for RADIUS Packet Encryption

The RADIUS client (the router) and RADIUS server use the MD5 algorithm to encrypt the exchanged packets between them. The two ends verify the packets using a shared key. Only when the same key is used can they properly receive the packets and make responses.

Perform the following configurations in RADIUS view.

Table 2-19 Set the shared key for RADIUS packet encryption

Operation	Command
Set the shared key for RADIUS authentication/authorization packet encryption.	**key authentication** *string*
Restore the default shared key for RADIUS authentication/authorization packet encryption.	**undo key authentication**
Set the shared key for RADIUS accounting packet encryption.	**key accounting** *string*
Restore the default shared key for RADIUS accounting packet encryption.	**undo key accounting**

By default, the shared key huawei is used for RADIUS authentication/authorization and accounting packet encryption.

2.3.5 Setting the Maximum Number of RADIUS Request Attempts

Since RADIUS uses UDP packets to carry data, the communication process is not reliable. If the RADIUS server does not respond to the NAS before the response timer times out, the NAS should retransmit the RADIUS request. After the number of transmission attempts exceeds the specified *retry-times*, the NAS considers the communication with the current RADIUS server has been disconnected and turns to another RADIUS server.

You can use the following command to set the maximum number of allowed RADIUS request attempts.

Perform the following configurations in RADIUS view.

Table 2-20 Set the maximum number of RADIUS request attempts

Operation	Command
Set the maximum number of RADIUS request attempts.	**retry** *retry-times*
Restore the default maximum number of RADIUS request attempts.	**undo retry**

By default, a RADIUS request can be sent up to three times.

2.3.6 Configuring the User Re-authentication at Reboot Function

I. Introduction to the user re-authenctication at reboot function

On the CAMS server, there is a kind of user called exclusive user, each of which has its concurrent online number set to 1. With the AAA solution implemented jointly by the router and CAMS server, the router prompts that an exclusive user is already online in the following situation:

- The router reboots after an exclusive user passes the authentication/authorization and begins being accounted.
- The CAMS server has not performed online user detection.
- The exclusive user logs into the router again.

After this, the user cannot access network resources normally unless the network administrator manually removes the online information of the user on the CAMS server.

To solve the above problem, you can enable the user re-authentication at reboot on the router. With this function enabled, the following occurs whenever the router reboots:

- The router generates an Accounting-On packet, which includes information such as the NAS-ID, NAS-IP (source IP), and session ID of the user.
- The router sends the Accounting-On packet to the CAMS server at a specified interval.
- When receiving an Accounting-On packet, the CAMS server sends a response packet to the router, locates and deletes information about the original online users according to information about NAS-ID, NAS-IP, and session ID in the Accounting-On packet, and ends the accounting based on the last accounting update packet.
- When receiving the response packet from the CAMS server, the router stops sending Accounting-On packets.

- If the router has sent the specified maximum number of Accounting-On packets without receiving any response packet from the CAMS server, the router stops sending Accounting-On packets.

Note:

The primary attributes of an Accounting-On packet (that is, the NAS-ID, NAS-IP, and session ID) are often generated by the router automatically, where the NAS-IP attribute is the IP address for the outbound interface of the packet by default. You can also configure the NAS-IP attribute manually by using the **nas-ip** command, in which case you must be sure to specify a correct and valid IP address.

II. Configuration Prerequisites

Create a RADIUS scheme and specify to use the CAMS server for RADIUS authentication and accounting.

III. Configuring user re-authenctication at reboot

The following table describes the user re-authentication at reboot configuration tasks.

Table 2-21 Configure user re-authentication at reboot

No.	To do…	Use the command…	Remarks
1	Enter system view	**system-view**	—
2	Enter RADIUS scheme view	**radius scheme** *radius-scheme-name*	—
3	Enable user Re-authentication at reboot	**accounting-on enable** [**send** *times*] [**interval** *interval*]	By default, the function is not enabled. The default maximum times for sending Accounting-On packets is 15, and the default sending interval is three seconds.

2.3.7 Setting the Supported RADIUS Server Type

You can use the following command to set the supported RADIUS server type.

Perform the following configurations in RADIUS view.

Table 2-22 Set the supported RADIUS server type

Operation	Command
Set the supported RADIUS server type.	**server-type** { **huawei | standard | portal** }
Restore the RADIUS server type to the default setting.	**undo server-type**

By default, RADIUS server type is **standard**.

2.3.8 Setting RADIUS Server State

For primary and secondary servers (no matter they are authentication/authorization servers or accounting servers) in a RADIUS scheme, if the primary server is disconnected from the NAS due to some fault, the NAS automatically turns to the secondary server. However, after the primary one recovers, the NAS does not resume the communication with it at once; instead, the NAS continues communicating with the secondary one and turns to the primary one again only after the secondary one fails. To have the NAS communicate with the primary server right after its recovery, you can manually set the primary server state to **active**.

When both primary and secondary servers are active or blocked, the NAS sends packets to the primary one only.

Perform the following configurations in RADIUS view.

Table 2-23 Set RADIUS server state

Operation	Command
Set the state of the primary RADIUS authentication/authorization server.	**state primary authentication** { **block | active** }
Set the state of the primary RADIUS accounting server.	**state primary accounting** { **block | active** }
Set the state of the secondary RADIUS authentication/authorization server.	**state secondary authentication** { **block | active** }
Set the state of the secondary RADIUS accounting server.	**state secondary accounting** { **block | active** }

By default, the state of each server in a RADIUS scheme is **active**.

2.3.9 Setting Username Format Acceptable to RADIUS Server

As mentioned above, the supplicants are generally named in userid@isp-name format. The part following "@" is the ISP domain name. 3Com Series Routers will put the users into different ISP domains according to the domain names. However, some earlier

RADIUS servers reject the username including ISP domain name. In this case, you have to remove the domain name before sending the username to the RADIUS server. 3Com Router provides the following command to specify whether the username to be sent to the RADIUS server carries ISP domain name or not.

Table 2-24 Set username format acceptable to RADIUS server

Operation	Command
Set the username format transmitted to the RADIUS server.	**user-name-format** { **with-domain** | **without-domain** }

🕮 **Note:**

If a RADIUS scheme is configured not to allow usernames to include ISP domain names, the RADIUS scheme shall not be simultaneously used in more than one ISP domain. Otherwise, the RADIUS server will regard two users in different ISP domains as the same user by mistake, if they have the same username (excluding their respective domain names.)

By default, the username sent from NAS to the RADIUS server includes ISP domain name.

2.3.10 Setting the Unit of Data Flows Destined for RADIUS Server

3Com Series Routers provide you with the following command to define the unit of the data flow sent to RADIUS servers.

Table 2-25 Set the unit of data flows destined for RADIUS server

Operation	Command
Set the unit of data flows transmitted to RADIUS server.	**data-flow-format data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } **packet** { **giga-packet** | **kilo-packet** | **mega- packet** | **one-packet** }
Restore the default unit.	**undo data-flow-format**

In a RADIUS scheme, the default data unit is byte and the default data packet unit is one packet.

2.3.11 Configuring Source Address for RADIUS Packets Sent by NAS

Perform the following configuration.

Table 2-26 Configure source address for the RADIUS packets sent by the NAS

Operation	Command
Configure the source address to be carried in the RADIUS packets sent by the NAS(RADIUS view).	**nas-ip** *ip-address*
Cancel the configured source address to be carried in the RADIUS packets sent by the NAS(RADIUS view).	**undo nas-ip**
Configure the source address to be carried in the RADIUS packets sent by the NAS(System view).	**radius nas-ip** *ip-address*
Cancel the configured source address to be carried in the RADIUS packets sent by the NAS(System view).	**undo radius nas-ip**

You can use either command to bind a source address with the NAS.

By default, no source address is specified and the source address of a packet is the address of the interface where it is sent.

2.3.12 Setting Timers Regarding RADIUS Server

I. Setting the response timeout timer

If the NAS receives no response from the RADIUS server after sending a RADIUS request (authentication/authorization or accounting request) for a period of time, the NAS has to resend the request, thus ensuring the user can obtain the RADIUS service.

You can use the following commands to set the response timeout timer.

Perform the following configuration in RADIUS view.

Table 2-27 Set the response timeout timer

Operation	Command
Set the response timeout timer.	**timer response-timeout** *seconds*
Restore the default response timeout timer.	**undo timer response-timeout**

By default, the response timeout timer for the RADIUS server is set to three seconds.

II. Setting the quiet timer for the primary RADIUS server

Perform the following configuration in RADIUS view.

Table 2-28 Configure the quiet timer for the primary RADIUS server

Operation	Command
Configure the quiet timer for the primary RADIUS server.	**timer quiet** *minutes*

Operation	Command
Restore the default setting.	**undo timer quiet**

By default, the primary RADIUS server must wait five minutes before it can resume the active state.

III. Setting a realtime accounting interval

The setting of real-time accounting interval is indispensable to real-time accounting. After an interval value is set, the NAS transmits the accounting information of online users to the RADIUS accounting server at intervals of this value.

Perform the following configuration in RADIUS view.

Table 2-29 Set a real-time accounting interval

Operation	Command
Set a real-time accounting interval.	**timer realtime-accounting** *minutes*
Restore the default real-time accounting interval.	**undo timer realtime-accounting**

In the command, *minutes* represents the interval for realtime accounting and it must be a multiple of three.

The setting of real-time accounting interval somewhat depends on the performance of the NAS and the RADIUS server: a shorter interval requires higher device performance. You are therefore recommended to adopt a longer interval when there are a large number of users (more than 1000, inclusive). The following table recommends the ratio of *minutes* to the number of users.

Table 2-30 Recommended ratio of interval to user number

User number	Interval for realtime accounting (minute)
1 – 99	3
100 – 499	6
500 – 999	12
ƒ1000	ƒ15

The realtime accounting interval defaults to 12 minutes.

2.3.13 Enabling the RADIUS Server to Send Traps when It Goes Down

Perform the following configuration in system view.

Table 2-31 Enable the RADIUS server to send traps when it goes down

Operation	Command
Enable the RADIUS server to send traps when it goes down	**radius trap** { **authentication-server-down** | **accounting-server-down** }
Disable the RADIUS server to send traps when it goes down	**undo radius trap** { **authentication-server-down** | **accounting-server-down** }

By default, the RADIUS server does not send traps when it goes down.

2.3.14 Configuring a Local RADIUS Authentication Server

The 3Com router provides a simple local RADIUS server function for authentication and authorization, which is called the local RADIUS authentication server function.

The following table describes the local RADIUS authentication server configuration tasks.

Table 2-32 Configure a local RADIUS authentication server

Operation	Command
Configure a local RADIUS authentication server	**local-server nas-ip** *ip-address* **key** *password*
Disable a local RADIUS authentication server	**undo local-server nas-ip** *ip-address*

By default, the system creates a local RADIUS authentication server with the NAS-IP of 127.0.0.1 and the key of huawei.

Note:

- With the local RADIUS authentication server function, the UDP port for authentication/authorization service must be 1645, and the UDP port for accounting service must be 1646.
- The packet encryption key configured using the **local-server nas-ip** command must be identical to that configured using the **key authentication** command in RADIUS scheme view.
- Up to 16 local RADIUS authentication servers can be configured, including the one created by the system by default.

2.4 Configuring HWTACACS Protocol

The configuration tasks of HWTACACS include:

- Create a HWTACACS scheme
- Configure TACACS authentication servers
- Configure TACACS authorization servers
- Configure TACACS accounting servers
- Configure a key for securing the communication with a TACACS server
- Set the username format acceptable to a TACACS server
- Set the unit of data flows destined for a TACACS server
- Configure the source address to be carried by the HWTACACS packets sent by NAS
- Set timers regarding TACACS server
- Enable the online TACACS user to change its password

Note:

In contrast to the settings in RADIUS server, note the following points when configuring a TACACS server:

- The system does not check whether users are using the current HWTACACS scheme when you change most of its attributes, except when you delete the scheme.
- By default, the TACACS server has no key.

Among these configuration tasks, creating a HWTACAS scheme and configuring TACACS authentication/authorization server are required, while others are optional at your discretion.

2.4.1 Creating a HWTACAS scheme

As aforementioned, HWTACACS protocol is configured scheme by scheme. Therefore, you must create a HWTACACS scheme and enter HWTACACS view before you perform other configuration tasks.

Perform the following configuration in system view.

Table 2-33 Create a HWTACACS scheme

Operation	Command
Create a HWTACACS scheme and enter HWTACACS view.	**hwtacacs scheme** *hwtacacs-scheme-name*

Operation	Command
Delete a HWTACACS scheme.	**undo hwtacacs scheme** *hwtacacs-scheme-name*

If the HWTACACS scheme you specify does not exist, the system creates it and enters HWTACACS view.

In HWTACACS view you can configure the HWTACACS scheme.

The system supports up to 128 HWTACACS schemes. You can only delete the schemes that are not being used.

By default, no HWTACACS scheme exists.

2.4.2 Configuring TACACS Authentication Servers

Perform the following configuration in HWTACACS view.

Table 2-34 Configure TACACS authentication servers

Operation	Command
Configure the TACACS primary authentication server.	**primary authentication** *ip-address* [*port*]
Delete the TACACS primary authentication server.	**undo primary authentication**
Configure the TACACS secondary authentication server.	**secondary authentication** *ip-address* [*port*]
Delete the TACACS secondary authentication server.	**undo secondary authentication**

The primary and secondary authentication servers cannot use the same IP address. Otherwise, the system will prompt unsuccessful configuration. The default port number is 49.

If you execute this command repeatedly, the new settings will replace the old settings.

You can remove a server that cannot be removed otherwise, only when it is not used by any active TCP connection for sending authentication packets. This delete does not affect the packets sent before the operation.

2.4.3 Configuring TACACS Authorization Servers

Perform the following configuration in HWTACACS view.

Table 2-35 Configure TACACS authorization servers

Operation	Command
Configure the primary TACACS authorization server.	**primary authorization** *ip-address* [*port*]
Delete the primary TACACS authorization server.	**undo primary authorization**
Configure the secondary TACACS authorization server.	**secondary authorization** *ip-address* [*port*]
Delete the secondary TACACS authorization server.	**undo secondary authorization**

Note:

If TACACS authentication is configured for a user without TACACS authorization server, the user cannot log in regardless of its user type.

The primary and secondary authorization servers cannot use the same IP address. Otherwise, the system will prompt unsuccessful configuration. The default port number is 49.

If you execute this command repeatedly, the new settings will replace the old settings.

You can remove a server that cannot be removed otherwise, only when it is not used by any active TCP connection for sending authorization packets.

2.4.4 Configuring TACACS Accounting Servers and the Related Attributes

I. Configuring TACACS accounting servers

Perform the following configuration in HWTACACS view.

Table 2-36 Configure TACACS accounting servers

Operation	Command
Configure the primary TACACS accounting server.	**primary accounting** *ip-address* [*port*]
Delete the primary TACACS accounting server.	**undo primary accounting**
Configure the secondary TACACS accounting server.	**secondary accounting** *ip-address* [*port*]
Delete the secondary TACACS accounting server.	**undo secondary accounting**

The primary and secondary accounting servers cannot use the same IP address. Otherwise, the system will prompt unsuccessful configuration. The default port number is 49.

The default IP address of TACACS accounting server is 0.0.0.0.

If you execute this command repeatedly, the new settings will replace the old settings.

You can remove a server that cannot be removed otherwise, only when it is not used by any active TCP connection for sending accounting packets.

II. Enabling stop-accounting packet retransmission

Perform the following configuration in HWTACACS view.

Table 2-37 Configure stop-accounting packet retransmission

Operation	Command
Enable stop-accounting packet retransmission and set the allowed maximum number of transmission attempts.	**retry stop-accounting** *retry-times*
Disable stop-accounting packet retransmission.	**undo retry stop-accounting**

By default, stop-accounting packet retransmission is enabled, and the allowed maximum number of transmission attempts is 100.

2.4.5 Configuring Source Address for HWTACACS Packets Sent by NAS

Perform the following configuration.

Table 2-38 Configure the source address to be carried in HWTACACS packets sent by the NAS

Operation	Command
Configure the source address to be carried in HWTACACS packets sent by the NAS(HWTACACS view).	**nas-ip** *ip-address*
Delete the configured source address to be carried in the HWTACACS packets sent by the NAS (HWTACACS view).	**undo nas-ip**
Configure the source address to be carried in the **hwtacacs** packets sent by the NAS(System view).	**hwtacacs nas-ip** *ip-address*
Cancel the configured source address to be carried in the **hwtacacs** packets sent by the NAS(System view).	**undo hwtacacs nas-ip**

By default, no source address is specified and the source address to be carried in a packet is the address of the interface where the packet is sent.

2.4.6 Setting a Key for Securing the Communication with TACACS Server

When using a TACACS server as an AAA server, you can set a key to improve the communication security between the router and the TACACS server.

Perform the following configuration in HWTACACS view.

Table 2-39 Set a key for securing the communication with the TACACS server

Operation	Command
Configure a key for securing the communication with the TACACS accounting, authorization or authentication server.	**key** { **accounting** | **authorization** | **authentication** } *string*
Delete the configuration.	**undo key** { **accounting** | **authorization** | **authentication** }

No key is configured by default.

2.4.7 Setting the Username Format Acceptable to the TACACS Server

Username is usually in the “userid@isp-name” format, with the domain name following “@”.

If a TACACS server does not accept the username with domain name, you can remove the domain name and resend it to the TACACS server.

Perform the following configuration in HWTACACS view.

Table 2-40 Set the username format acceptable to the TACACS server

Operation	Command
Send username with domain name.	**user-name-format with-domain**
Send username without domain name.	**user-name-format without-domain**

By default, each username sent to a TACACS server contains a domain name.

2.4.8 Setting the Unit of Data Flows Destined for the TACACS Server

Perform the following configuration in HWTACACS view.

Table 2-41 Set the unit of data flows destined for the TACACS server

Operation	Command
Set the unit of data flows destined for the TACACS server.	**data-flow-format data** [**byte** | **giga-byte** | **kilo-byte** | **mega-byte**] **data-flow-format packet** [**giga-packet** | **kilo-packet** | **mega-packet** | **one-packet**]

Operation	Command
Restore the default unit of data flows destined for the TACACS server.	**undo data-flow-format** [**data** | **packet**]

The default data flow unit is byte.

2.4.9 Setting Timers Regarding TACACS Server

I. Setting the response timeout timer

Since HWTACACS is implemented based on TCP, server response timeout or TCP timeout may terminate the connection to the TACACS server.

Perform the following configuration in HWTACACS view.

Table 2-42 Set the response timeout timer

Operation	Command
Set the response timeout time.	**timer response-timeout** *seconds*
Restore the default setting.	**undo timer response-timeout**

The default response timeout timer is set to five seconds.

II. Setting the quiet timer for the primary TACACS server

Perform the following configuration in HWTACACS view.

Table 2-43 Set the quiet timer for the primary TACACS server

Operation	Command
Set the quiet timer for the primary TACACS server.	**timer quiet** *minutes*
Restore the default setting.	**undo timer quiet**

By default, the primary TACACS server must wait five minutes before it can resume the active state.

III. Setting a realtime accounting interval

The setting of real-time accounting interval is indispensable to real-time accounting. After an interval value is set, the NAS transmits the accounting information of online users to the RADIUS accounting server at intervals of this value.

Perform the following configuration in HWTACACS view.

Table 2-44 Set a real-time accounting interval

Operation	Command
Set a real-time accounting interval.	**timer realtime-accounting** *minutes*
Restore the default real-time accounting interval.	**undo timer realtime-accounting**

The interval is in minutes and must be a multiple of 3.

The setting of real-time accounting interval somewhat depends on the performance of the NAS and the TACACS server: a shorter interval requires higher device performance. You are therefore recommended to adopt a longer interval when there are a large number of users (more than 1000, inclusive). The following table recommends the ratio of *minutes* to the number of users.

Table 2-45 Recommended ratio of the interval to the number of users

User number	Real-time accounting interval (in minutes)
1 – 99	3
100 – 499	6
500 – 999	12
ƒ1000	ƒ15

The real-time accounting interval defaults to 12 minutes.

2.4.10 Enabling the Online TACACS User to Change the Password

Perform the following configuration in user view.

Table 2-46 Enable the online TACACS user to change the password

Operation	Command
Enable the online TACACS user to change the password	**hwtacacs change-password self**

After this command is configured, the system guides the TACACS online user through to change the password. Three chances are available for changing the password. Failure to do so makes the TACACS server quit this operation automatically.

This function is only valid for terminal users (including console, AUX, TTY, and VTY) configured with TACACS authentication.

Note:

To allow a TACACS user to change its password, you must ensure that this function is enabled on the TACACS server in addition to the TACACS client.
This function does not work with Cisco Security ACS V3.1 (TACACS Server).

2.5 Displaying and Debugging AAA and RADIUS/HWTACACS Protocols

After the above configuration, execute the **display** commands in any view to view the running of the AAA and RADIUS/HWTACACS configurations and to check the configuration effect. Execute the **reset** commands in user view to reset the configurations. Execute the **debugging** commands in user view for debugging.

Table 2-47 Display and debug the AAA protocol

Operation	Command
Display the configuration information of the specified or all the ISP domains.	**display domain** [*isp-name*]
Display related information of user's connection.	**display connection** [**domain** *isp-name* | **hwtacacs-scheme** *hwtacacs-scheme-name* | **ip** *ip-address* | **mac** *mac-address* | **radius-scheme** *radius-scheme-name* | **ucibindex** *ucib-index* | **user-name** *user-name*]
Display related information of the local user	**display local-user** [**domain** *isp-name* | **service-type** { **pad** | **telnet** | **ssh** | **terminal** | **ftp** | **ppp** } | **state** { **active** | **block** } | **user-name** *user-name*]

Table 2-48 Display and debug the RADIUS protocol

Operation	Command
Display the specified or all the RADIUS schemes or display the statistics about RADIUS.	**display radius** [*radius-scheme-name* | **statistics**]
Display the statistics on RADIUS packets.	**display radius statistics**
Display information on the stop-accounting packets in the buffer.	**display stop-accounting-buffer** { **radius-scheme** *radius-server-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }
Enable RADIUS packet debugging.	**debugging radius packet**

Operation	Command
Disable RADIUS packet debugging.	**undo debugging radius packet**
Clear stop-accounting packets from the buffer.	**reset stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }
Reset the statistics of RADIUS server.	**reset radius statistics**

Table 2-49 Display and debug the HWTACACS protocol

Operation	Command
Display the specified or all the HWTACACS schemes.	**display hwtacacs** [*hwtacacs-scheme-name* [**statistics**]]
Display information on the stop-accounting packets in the buffer.	**display stop-accounting-buffer hwtacacs-scheme** *hwtacacs-scheme-name*
Enable HWTACACS debugging.	**debugging hwtacacs** { **all** | **error** | **event** | **message** | **receive-packet** | **send-packet** }
Disable HWTACACS debugging.	**undo debugging hwtacacs** { **all** | **error** | **event** | **message** | **receive-packet** | **send-packet** }
Clear stop-accounting packets from the buffer.	**reset stop-accounting-buffer** { **hwtacacs-scheme** *hwtacacs-scheme-name* }
Reset the statistics about TACACS servers.	**reset hwtacacs statistics** {**accounting** | **authentication** | **authorization** | **all** }

2.6 AAA and RADIUS/HWTACACS Configuration Example

2.6.1 Telnet/SSH User Authentication/Accounting Using RADIUS Server

Note:

Configuring authentication and accounting on the RADIUS server for SSH users is similar to Telnet users. The following example is based on Telnet users.

At present, RADIUS and HWTACACS do not support FTP user accounting.

I. Network Requirements

Configure the router to enable the RADIUS server to provide authentication and accounting services for Telnet users accessing the router (see the following figure).

Connect the router to the RADIUS server device (functions as both authentication and accounting servers) whose IP address is 10.110.91.146. On the router, set both the shared keys for encrypting authentication and accounting packets to "expert”.

You can use a Huawei CAMS server as the RADIUS server. Set server-type in the RADIUS scheme to standard or huawei if a third-party RADIUS server is used and to huawei if a huawei CAMS server is used. On the RADIUS server, set both the shared keys for encrypting authentication and accounting packets to "expert”; set the authentication and accounting port numbers; add the usernames and login passwords of the Telnet users. If the router is configured in the RADIUS scheme to send the full username (both *userid* and *isp-name*) to the RADIUS server, the usernames added onto the RADIUS server are in the *userid@isp-name* format.

II. Network diagram

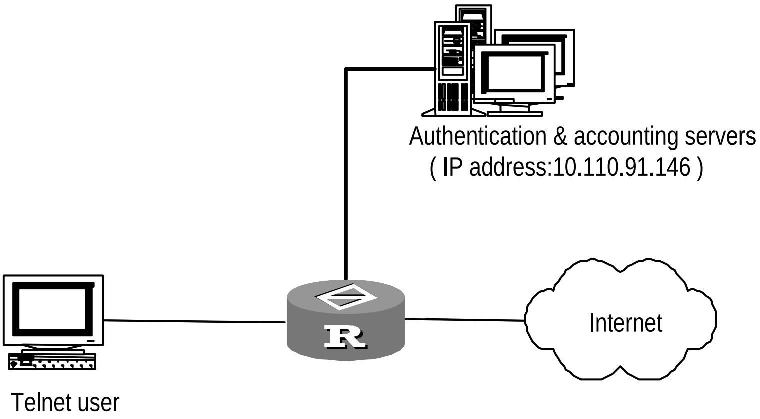

Authentication & accounting servers
(IP address:10.110.91.146)
Internet
Telnet user

Figure 2-7 Configure remote RADIUS authentication for Telnet users

III. Configuration procedure

# Apply AAA authentication to Telnet users, that is, the scheme mode.

```
[3Com-ui-vty0-4] authentication-mode scheme
```

# Configure domain.

```
[3Com] domain cams
[3Com-isp-cams] access-limit enable 10
[3Com-isp-cams] accounting optional
[3Com-isp-cams] quit
```

# Configure a RADIUS scheme, adopting remote authentication.

```
[3Com] radius scheme cams
```

```
[3Com-radius-cams] primary authentication 10.110.91.146 1812
[3Com-radius-cams] primary accounting 10.110.91.146 1813
[3Com-radius-cams] key authentication expert
[3Com-radius-cams] key accounting expert
[3Com-radius-cams] server-type Huawei
[3Com-radius-cams] user-name-format with-domain
[3Com-radius-cams] quit
```

# Associate the domain to the RADIUS scheme.

```
[3Com] domain cams
[3Com-isp-cams] scheme radius-scheme cams
```

Telnet users use usernames in the *userid*@cams format to log onto the network and are to be authenticated as CAMS domain users.

2.6.2 Configuring FTP/Telnet User Local Authentication

Note:

Configuring local authentication for FTP users is similar to that for Telnet users. The following example is based on Telnet users.

I. Network requirements

Configure the router to authenticate the login Telnet users at the local (see the following figure).

II. Network diagram

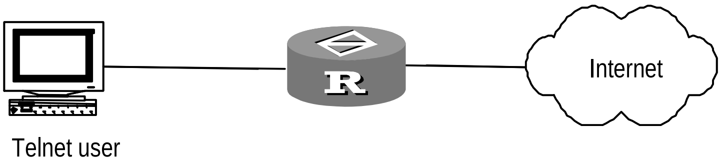


Figure 2-8 Local authentication for Telnet users

III. Configuration procedure

# Apply AAA authentication to Telnet users.

```
[3Com-ui-vty0-4] authentication-mode scheme
```

# Create a local user telnet.

```
[3Com] local-user telnet
[3Com-luser-telnet] service-type telnet
```

```
[3Com-luser-telnet] password simple huawei
[3Com] domain system
[3Com-isp-system] scheme local
```

Telnet users use usernames in the "*userid*@system" format to log onto the network and are to be authenticated as users of the system domain.

2.6.3 PPP Authentication/Accounting/Authorization with TACACS Servers

I. Network requirements

Configure the router to use a TACACS server to assign IP addresses and provide authentication, accounting, and authorization services to login PPP users (see the following figure).

Connect the router to one TACACS server (providing the services of authentication, authorization, and accounting) with the IP address 10.110.91.146. On the router, set the shared key for authentication, authorization, and accounting packet encryption to "expert". Configure the router to send usernames to the TACACS server with *isp-name* removed.

On the TACACS server, set the shared key for encrypting the packets exchanged with the router to "expert"; add the usernames and passwords of PPP users.

II. Network diagram

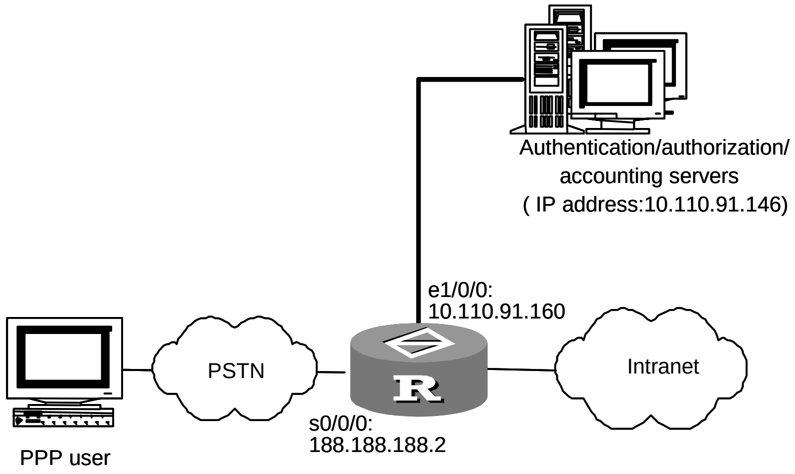


Figure 2-9 Configure remote PPP user authentication with HWTACACS

III. Configuration procedure

# Configure a HWTACACS scheme.

```
[3Com] hwtacacs scheme hwtac
[3Com-hwtacacs-hwtac] primary authentication 10.110.91.146 1812
[3Com-hwtacacs-hwtac] primary authorization 10.110.91.146 1813
[3Com-hwtacacs-hwtac] primary accounting 10.110.91.146 1814
```

```
[3Com-hwtacacs-hwtac] key authentication expert
[3Com-hwtacacs-hwtac] key authorization expert
[3Com-hwtacacs-hwtac] key accounting expert
[3Com-hwtacacs-hwtac] user-name-format with-domain
[3Com-hwtacacs -hwtac] quit
```

# Associate the domain with the hwtacacs.

```
[3Com] domain hwtacacs
[3Com-isp-hwtacacs] scheme hwtacacs-scheme hwtac
[3Com-isp-hwtacacs] ip pool 1 200.1.1.1 200.1.1.99
[3Com-isp-hwtacacs] quit
```

# Configure the serial interface.

```
[3Com] interface serial 0/0/0
[3Com-Serial0/0/0] link-protocol ppp
[3Com-Serial0/0/0] ppp authentication-mode pap domain hwtacacs
[3Com-Serial0/0/0] ip address 188.188.188.2 255.255.255.0
[3Com-Serial0/0/0] remote address pool 1
```

# Configure the Ethernet interface.

```
[3Com-Serial0/0/0] interface ethernet 1/0/0
[3Com-ethernet 1/0/0] ip address 10.110.91.160 255.255.255.0
```

2.6.4 Configuration Example of Separate AAA Schemes for PPP Users

I. Network requirements

In the environment shown in the following figure, a RADIUS server is required to assign IP addresses to PPP users and implement authentication and authorization, and a TACACS server is required to implement accounting.

The IP address of the RADIUS server is 10.110.91.145, and the shared key for the router and the RADIUS server is router. Set the router to remove the domain name in a user name and then transfer the resulted part to the RADIUS server.

The IP address of the TACACS server is 10.110.91.146, and the shared key for the router and the TACACS server is expert. Set the router to remove the domain name in a user name and then transfer the resulted part to the TACACS server.

II. Network diagram

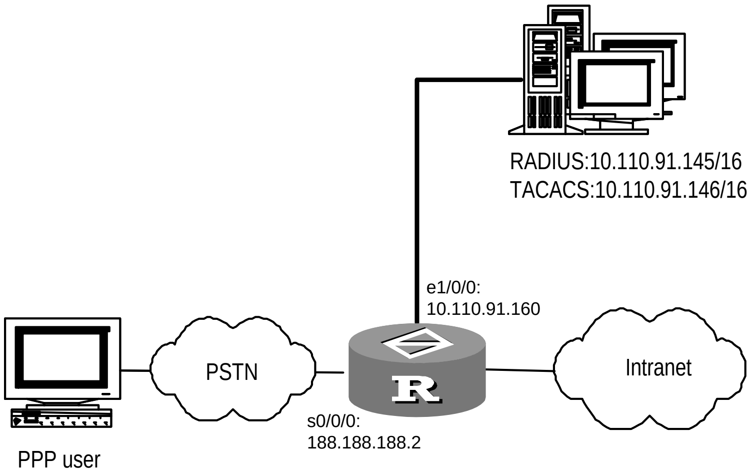


Figure 2-10 Configure separate AAA schemes for PPP users

III. Configuration procedure

# Configure the RADIUS scheme.

```
[3Com] radius scheme radius
[3Com-radius-radius] primary authentication 10.110.91.145 1812
[3Com-radius-radius] key authentication router
[3Com-radius-radius] user-name-format without-domain
[3Com-radius-radius] quit
```

# Configure the HWTACACS scheme.

```
[3Com] hwtacacs scheme hwtac
[3Com-hwtacacs-hwtac] primary accounting 10.110.91.146 1814
[3Com-hwtacacs-hwtac] key accounting expert
[3Com-hwtacacs-hwtac] user-name-format without-domain
[3Com-hwtacacs-hwtac] quit
```

# Configure the authentication, authorization, and accounting schemes of domain1.

```
[3Com] domain domain1
[3Com-isp-domain1] authentication radius-scheme radius
[3Com-isp-domain1] ip pool 1 200.1.1.1 200.1.1.99
[3Com-isp-domain1] accounting hwtacacs-scheme hwtac
[3Com-isp-domain1] quit
```

# Configure the serial interface.

```
[3Com] interface serial 0/0/0
[3Com-Serial0/0/0] link-protocol ppp
[3Com-Serial0/0/0] ppp authentication-mode pap domain domain1
```

```
[3Com-Serial0/0/0] ip address 188.188.188.2 255.255.255.0
[3Com-Serial0/0/0] remote address pool 1
```

# Configure the Ethernet interface.

```
[3Com-Serial0/0/0] interface ethernet 1/0/0
[3Com-ethernet1/0/0] ip address 10.110.91.160 255.255.255.0
```

In addition, you must configure the shared key for packets between the RADIUS or TACACS server and the router on the RADIUS and TACACS server respectively, and add the PPP user name and password. The related configuration is omitted here.

2.6.5 Configuring TACACS+ Server Authentication/Accounting

I. Network requirements

As shown in Figure 2-11, one TACACS+ server with IP address 10.110.91.146, serving the purposes of authentication, authentication, and accounting servers, is connected to a router.

To enable the TACACS+ server to provide one-time password authentication/accounting service to users that telnet to the router, do the following:

- Set the shared keys for packet exchange with the authentication, authorization, and accounting servers to expert.
- Add a fully qualified username, test@tacacs for example, for Telnet users on the TACACS+ server. (As The TACACS+ server provides one-time password authentication, so the router sends fully qualified usernames to the server.)

II. Network diagram

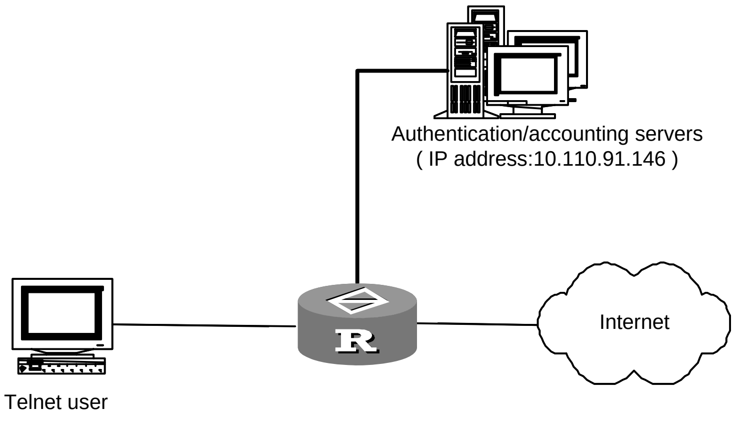

Authentication/accounting servers
(IP address:10.110.91.146)
Internet
Telnet user
R

Figure 2-11 Configure remote TACACS+ authentication for the Telnet user

III. Configuration procedure

1) Configure the router

# Configure Telnet users to use AAA authentication.

```
[3Com] user-interface vty0 4
[3Com-ui-vty0-4] authentication-mode scheme
```

# Configure the domain name.

```
[3Com] domain tacacs
[3Com-isp-tacacs] access-limit enable 10
[3Com-isp-tacacs] accounting optional
[3Com-isp-tacacs] quit
```

# Configure TACACS schemes.

```
[3Com] hwtacacs scheme system
[3Com-hwtacacs-system] primary authentication 10.110.91.146
[3Com-hwtacacs-system] primary authorization 10.110.91.146
[3Com-hwtacacs-system] primary accounting 10.110.91.146
[3Com-hwtacacs-system] key authentication expert
[3Com-hwtacacs-system] key authorzation expert
[3Com-hwtacacs-system] key accounting expert
[3Com-hwtacacs-system] user-name-format with-domain
[3Com-hwtacacs-system] quit
```

# Associate the domain with the TACACS scheme.

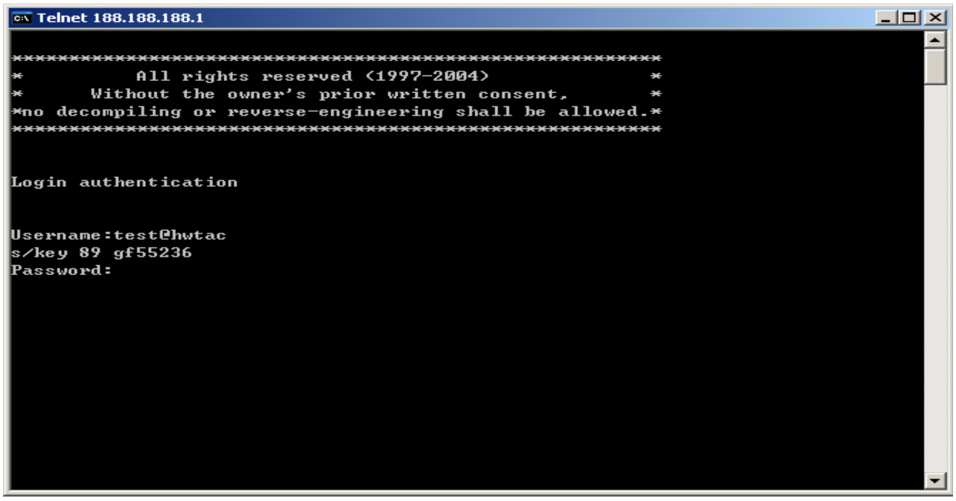
```
[3Com] domain tacacs
[3Com-isp-tacacs] scheme hwtacacs-scheme system
```

2) Configure the TACACS+ server

- Configure IP address
- Configure shared keys
- Add Telnet username test@ tacacs
- Enable one-time password authentication

3) Login process

Configuring one-time password authentication for Telnet users are in these steps:

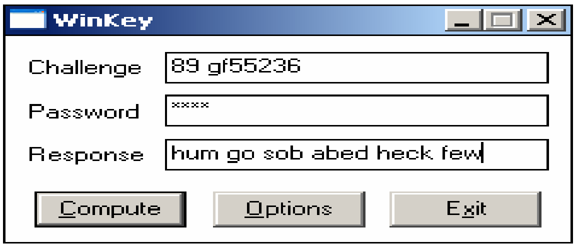


```
*********************************************************
*          All rights reserved (1997-2004)              *
*      Without the owner's prior written consent,       *
*no decompiling or reverse-engineering shall be allowed.*
*********************************************************


Login authentication


Username:test@hwtac
s/key 89 gf55236
Password:
```

Figure 2-12 Telnet user login interface

Step 1: Type username test@ tacacs.

Step 2: Choose to use the winkey.exe calculator to get the login password at the prompt "s/key 89 gf55236".



Challenge: 89 gf55236
Password: ****
Response: hum go sob abed heck few

Figure 2-13 Calculate login password

In the above figure:

Type the prompt "89 gf55236" in the Challenge field.

Type private password (test for example) in the Password field.

The Response field outputs the calculation result, that is, the password you need to type in the login interface.

Step 3: Type the calculated password in the login interface and you are authorized to access.

2.7 Troubleshooting AAA

2.7.1 Troubleshooting the RADIUS Protocol

The RADIUS protocol of the TCP/IP protocol suite is located at the application layer. It mainly provisions how to exchange user information between a NAS and a RADIUS server of an ISP. So it is very likely to get invalid.

- Symptom 1: User authentication/authorization always fails

Troubleshooting:

Check that:

1) The username is in the *userid@isp-name* format or a default ISP domain is specified on the NAS.
2) The user exists in the database on the RADIUS server.
3) The password input by the user is correct.
4) The same shared key is configured on both the RADIUS server and the NAS.
5) The NAS can communicate with the RADIUS server (by pinging the RADIUS server).

- Symptom 2: RADIUS packets cannot reach the RADIUS server.

Troubleshooting:

Check that:

1) The communication links (at both physical and link layers) between the NAS and the RADIUS server work well.
2) The IP address of the RADIUS server is correctly configured on the NAS.
3) Authentication/Authorization and accounting UDP ports are set in consistency with the port numbers set on the RADIUS server.

- Symptom 3: A user passes the authentication and gets an authorization already, but its charging bill cannot be sent to the RADIUS server.

Troubleshooting:

Check that:

1) The accounting port number is correctly set.
2) The authentication/authorization and accounting servers are correctly configured on the NAS. For example, the fault can occur in the situation where one server is configured on the NAS to provide all the services of authentication/authorization and accounting, despite the fact that different server devices are used to provide the services.

2.7.2 Troubleshooting the HWTACACS Protocol

See the previous section if you encounter an HWTACACS fault.

Chapter 3 Portal Configuration

3.1 Portal Overview

3.1.1 Introduction to Portal

Portal is also called portal website. Portal authentication is also called web authentication, which mainly falls into two categories: fast authentication and normal authentication. Portal features the following advantages:

- No client program is required on a portal client.
- Powerful ability to support new services: Operators can implement information inquiry, online shopping, and other services on the home pages of portal servers, bringing to bear their roles as portals.
- With fast authentication, neither user name nor password is required for network access.

Portal works on this principle: Unauthenticated users can only access certain website servers, and any access packets to any other servers on the Internet are redirected to a portal server unconditionally for authentication.

3.1.2 Portal System Composition

As shown in Figure 3-1, a portal system consists of four basic factors: authentication client, access device, portal server and authentication/accounting server.

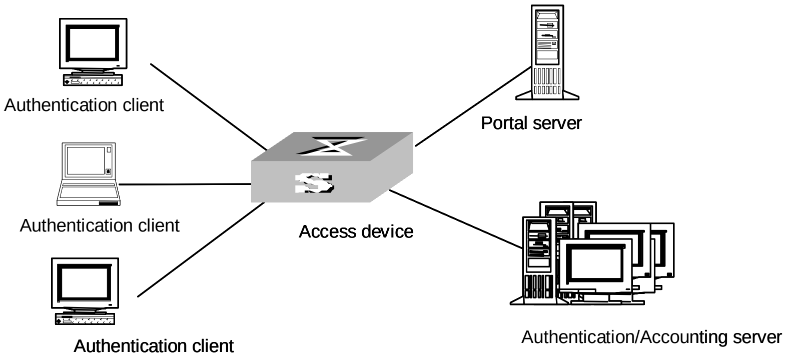


Figure 3-1 Portal system composition

- Authentication client: A web browser running hypertext transfer protocol/secure HTTP (HTTP/HTTPS). Before a client is successfully authenticated, all HTTP requests from it are redirected to the portal server.
- Access device: Forwards by force the HTTP requests from an authentication client to the portal server unconditionally before the client is successfully authenticated.

The access device communicates with the authentication/accounting server to perform authentication and accounting. The access device in this manual refers to a 3Com router.

- Portal server: A web server, which can be accessed using a standard web browser. The portal server provides free portal services and the web-based authentication interface. The access device and the portal server interact to authenticate the clients. Internet content providers (ICPs) can use portal servers to provide users with services such as information inquiry and online shopping.
- Authentication/Accounting server: Performs user authentication and accounting. The access device and the authentication/accounting server communicate with each other through the remote authentication dial-in user service (RADIUS) protocol.

⚠ **Caution:**

- With portal services, no network address translation (NAT) devices can exist among authentication clients, access device, portal server, and authentication/accounting server.
- Currently, only RADIUS servers can be configured as authentication/accounting servers. TACACS authentication/accounting servers and local authentication do not support portal services.

3.1.3 Portal Authentication Procedures

On a 3Com router, the procedures for normal portal authentication are as follows:

- When receiving the first HTTP packet from a user logging in, the router determines whether this user is a portal user. If yes, the router only allows the user to access the contents of the specified websites (portal servers and the predefined free access addresses).
- When receiving HTTP packets for access to other sites from a portal user, the router redirects the packets to the portal server by TCP spoofing.
- The portal server provides web pages for the user to enter the user name and password, which are then forwarded to the router.
- The router sends the user name and password to the RADIUS server for authentication. Upon successful RADIUS authentication, the user is allowed to access the Internet. From then on, the router no longer redirects HTTP packets from the user.

With fast portal authentication, a user is also redirected to the portal server when opening a web page. However, the user only needs to click the connection button, rather than enter the user name and password, to initiate fast authentication. In addition, the attribute fields of the user name and password in the authentication request sent from the portal server to the router are filled randomly, while the router fills the configured user name and password in the authentication request it sends to the RADIUS server. If the user name and the password match those on the RADIUS server, the user is authenticated successfully.

3.1.4 Portal Operating Modes

On 3Com routers, the portal feature can be implemented in two methods (also called operating modes): direct authentication, and re-DHCP authentication.

- In direct authentication mode: Before passing the authentication, a user with a public IP address can only access the portal server and the predefined free IP addresses. After passing the authentication, the user can access the Internet.
- In re-DHCP authentication mode: Before passing the authentication, a user with a private IP address from the DHCP server can only access the portal server and the predefined free IP addresses. After passing the authentication, the user can obtain a public IP address to access the Internet.

Both fast portal authentication and normal portal authentication support these two authentication methods.

3.1.5 Authentication-Free Users and Free IP Addresses

I. Authentication-free users

Authentication-free users can access the Internet without portal authentication. In actual networking environments, you can configure some servers and the network devices attached to the router as authentication-free users.

Authentication-free user information contains the IP address of the user and the interface on the router to which the user is connected. Only the user whose information fully matches the authentication-free user information can be allowed to access the Internet without authentication.

II. Free IP addresses

Free IP addresses are the IP addresses which users can access without limitation. A free IP address can be the IP address of a DNS server, or the IP address of a free website provided by an Internet service provider (ISP).

3.2 Basic Portal Configuration

3.2.1 Configuration Prerequisites

Before performing portal configuration, make sure:

- The portal-enabled Ethernet interface is configured with a legal IP address.
- The portal server and the RADIUS server are installed and configured properly.
- With re-DHCP authentication, the router is configured as a DHCP relay, and the DHCP server is installed and configured properly.

If the portal server, RADIUS server, and DHCP server employ CAMS, refer to *Comprehensive Access Management Server Portal User Manual* for information about CAMS installation and configuration.

3.2.2 Basic Portal Configuration Tasks

The following table describes the basic portal configuration tasks.

Table 3-1 Basic portal configuration tasks

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set the portal service type to normal	**portal service-type normal**	Optional. The default portal service type is normal portal mode.
Configure a portal server	**portal server** *server-name* { **ip** *ip-address* | **key** *key-string* | **port** *port* | **url** *url-string* } *	Required. By default, no portal server is configured. When a portal server is configured, by default, *key-string* is huawei, *port* is 50100, and *url-string* is the IP address string prefixed with http://.
Configure the portal operating mode	**portal method** { **direct** | **redhcp** }	Optional. The default portal operating mode is direct authentication. For an application supporting portal authentication for non-directly connected network segments, you can configure direct authentication only.
Configure authentication network segments	**portal auth-network** *ip-address net-mask* **interface** *interface-type interface-num*	Required
Enable fast portal authentication	**portal fast-authentication server** *server-name* **user-name** *name* **password** *password*	Optional.

To do…	Use the command…	Remarks
Enter interface view	**interface** *interface-type interface-num*	Required
Enable portal authentication on an interface	**portal** *server-name*	Required
Display portal configuration information and statistics	**display portal** [**acm statistics** | **auth-network** [**auth-interface** *interface-type interface-num*] | **free-user** | **free-ip** | **interface** [*interface-type interface-num*] | **server** [*server-name*] | **server statistics** | **tcp-cheat statistics**]	Available for use in any view
Clear portal-related statistics	**reset portal** { **acm** | **server** | **tcp-cheat** } **statistics**	Available for use in user view

Use the corresponding **undo** command to remove the configuration.

⚠ **Caution:**

- For an application supporting portal authentication for non-directly connected network segments, you can configure direct authentication only.
- When configuring a portal server for the first time, you must specify its IP address.
- To modify the parameters of a portal server which is referenced by an interface, you must first remove the reference.
- Whenever there are users, regardless the states of the users, you are strongly recommended not to configure the **undo portal** command. Instead, you can perform configuration on the RADIUS server to force the users to log out.
- When configuring the RADIUS scheme, you must configure the server type as portal.
- The portal server and the router must be configured with either fast authentication or normal authentication concurrently. Otherwise, the user will not be successfully authenticated or will be able to access the Internet without being authenticated.

3.2.3 Direct Authentication Configuration Example

I. Network requirements

- Configure the router to enable portal authentication. Set the portal operating mode to direct authentication and the portal server name to newp.
- The router uses the RADIUS server to implement authentication and accounting.
- Before passing the portal authentication, the user can only access the portal server. After passing the portal authentication, the user can access the Internet.

II. Network diagram

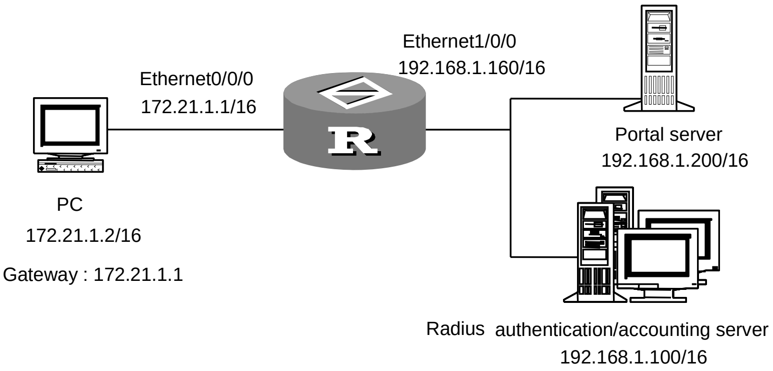


Figure 3-2 Network diagram for direct authentication

III. Configuration procedure

1) Configure a RADIUS scheme

# Enter system view, create a RADIUS scheme named portal and enter its view.

```
<3Com> system-view
[3Com] radius scheme portal
```

# Configure the server type of the RADIUS scheme as portal. Note that you must configure it as portal.

```
[3Com-radius-portal] server-type portal
```

# Configure the primary authentication server, the primary accounting server, and communication key for the RADIUS scheme.

```
[3Com-radius-portal] primary authentication 192.168.1.100
[3Com-radius-portal] primary accounting 192.168.1.100
[3Com-radius-portal] key accounting hello
[3Com-radius-portal] key authentication hello
[3Com-radius-portal] user-name-format without-domain
[3Com-radius-portal] quit
```

2) Configure ISP domain

# Create an ISP domain named portal and enter its view.

```
[3Com] domain portal
```

# Configure the ISP domain to use the RADIUS scheme named portal.

```
[3Com-isp-portal] radius-scheme portal
[3Com-isp-portal] quit
```

# Configure the default ISP domain as portal (optional).

```
[3Com] domain default enable portal
```

3) Configure portal authentication

# Configure the portal server with a name of newp, an IP address of 192.168.1.200, a key of huawei, a port of 50100, and a URL of http://192.168.1.200/portal.

```
[3Com] portal server newp ip 192.168.1.200 key huawei port 50100 url
http://192.168.1.200/portal
```

# Configure the portal operating mode as direct authentication.

```
[3Com] portal method direct
```

4) Enable portal authentication on the Ethernet interface connected to the user PC

# Enable portal authentication on interface ethernet0/0/0.

```
[3Com] interface ethernet0/0/0
[3Com-ethernet0/0/0] ip address 172.21.1.1 255.255.0.0
[3Com-ethernet0/0/0] portal newp
[3Com-ethernet0/0/0] quit
```

5) Configure interface ethernet1/0/0

```
[3Com] interface ethernet 1/0/0
[3Com-ethernet1/0/0] ip address 192.168.1.160 255.255.0.0
```

For normal portal authentication, the above configurations are enough. A user can now launch a web browser, enter the user name and password, and then access the Internet after successful portal authentication.

For fast portal authentication, you still need to perform the following configuration:

# Specify to perform fast portal authentication with user name fast and password 123.

```
[3Com] portal fast-authentication server newp user-name fast password 123
```

Note that the user name of fast and the password of 123 must be also configured on the RADIUS server. After completing the above configurations, the user can launch a web browser and access the Internet directly, without having to enter the user name and password.

3.2.4 Portal Authentication Across Layer 3 Devices Configuration Example

I. Network requirements

Router A supports portal authentication, while Router B does not. The PC of the user connects to Router A through Router B.

- Configure Router A to enable portal authentication. Set the portal operating mode to direct authentication and the name of the portal server to newp.
- Router A counts on the RADIUS server for authentication and accounting.
- Before passing the authentication, the PC can only access the portal server. After passing the authentication, the PC can access the Internet.

II. Network diagram

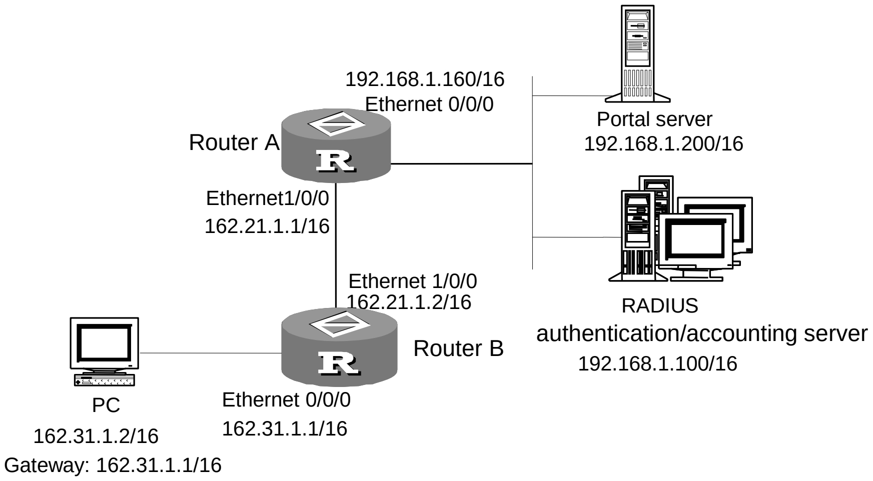


Figure 3-3 Network diagram for portal authentication across layer 3 devices

III. Configuration procedure

Note:

The following describes only the configurations for portal authentication across layer 3 devices. For configurations of the RADIUS scheme and ISP domain, refer to section 3.2.3 "Direct Authentication Configuration Example".

1) Configure Router A

# Enter system view, configure the portal server with a name of newp, an IP address of 192.168.1.200, a key of huawei, a port of 50100, and a URL of http://192.168.1.200/portal.

```
<3Com> system-view
[3Com] portal server newp ip 192.168.1.200 key huawei port 50100 url
http://192.168.1.200/portal
```

# Configure the portal operating mode as direct authentication.

```
[3Com] portal method direct
[3Com] portal auth-network 162.31.0.0 255.255.0.0 ethernet1/0/0
```

# Enable portal authentication on interface ethernet1/0/0.

```
[3Com] interface ethernet 1/0/0
[3Com-Ethernet 1/0/0] ip address 162.21.1.1 255.255.0.0
[3Com-Ethernet 1/0/0] portal newp
[3Com-Ethernet 1/0/0] quit
```

# Configure a route to segment 162.31.0.0/16.

```
[3Com] ip route-static 162.31.0.0 16 162.21.0.0
```

2) On Router B, configure a default route to segment 192.168.0.0/16, specifying the next hop as 162.21.0.0. The detailed configurations are not described here.

3.2.5 Re-DHCP Authentication Configuration Example

I. Network requirements

- Configure portal authentication on the router, and set the portal operating mode to re-DHCP authentication.
- The name of the portal server is newp.
- The router counts on the RADIUS server for authentication and accounting.
- Before passing the portal authentication, the IP address used by the user is a private address obtained from a DHCP server. After passing the portal authentication, the user obtains a public address and can access the Internet.

II. Network diagram

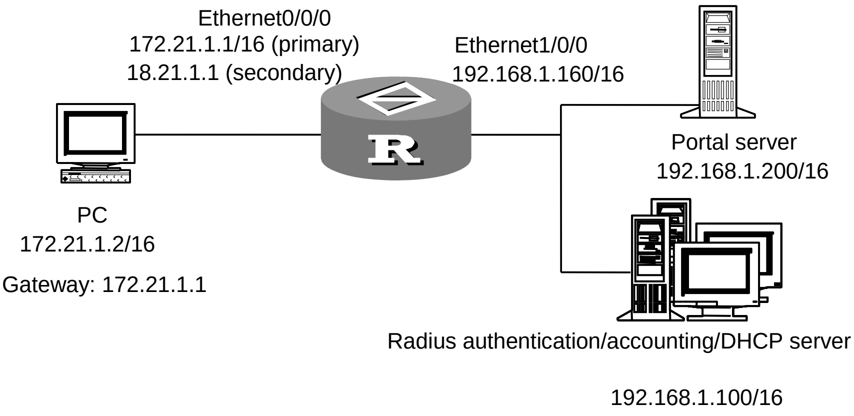


Figure 3-4 Network diagram for Re-DHCP authentication

III. Configuration procedure

Note:

- The following describes only the configurations related to re-DHCP authentication. For configurations of the RADIUS scheme and ISP domain, refer to section 3.2.3 “Direct Authentication Configuration Example”.
- For re-DHCP authentication, the DHCP server must support portal authentication, and you must create both a public address pool and a private address pool, which are 172.21.0.0/16 and 18.21.0.0/16 respectively. The detailed configurations are not described here.
- For re-DHCP authentication, you must configure the router as a DHCP relay instead of a DHCP server, and configure the portal-enabled interface with a primary IP address and a secondary IP address for use on public and private networks respectively.

# Enter system view and set the portal operating mode to re-DHCP authentication.

```
<3Com> system-view
[3Com] portal method redhcp
```

# Configure the portal server with a name of newp, an IP address of 192.168.1.200, a key of huawei, a port of 50100, and a URL of http://192.168.1.200/portal.

```
[3Com] portal server newp ip 192.168.1.200 key huawei port 50100 url http://192.168.1.200/portal
[3Com] portal auth-network 18.21.0.0 255.255.0.0 ethernet 0/0/0
```

# configure the portal-enabled interface with a primary IP address and a secondary IP address for use on public and private networks respectively.

```
[3Com] interface ethernet0/0/0
[3Com-ethernet0/0/0] dhcp select relay
[3Com-ethernet0/0/0] ip relay address 192.168.1.100
[3Com-ethernet0/0/0] ip address 172.21.1.1 255.255.0.0
[3Com-ethernet0/0/0] ip address 18.21.1.1 255.255.0.0 sub
```

# Enable portal authentication on interface ethernet0/0/0.

```
[3Com-ethernet0/0/0] portal newp
```

3.3 Authentication-Free User and Free IP address Configuration

3.3.1 Configuration Prerequisites

Before performing authentication-free user and free IP address configuration, determine the users to be configured as the authentication-free ones and the servers to be configured with free IP addresses.

3.3.2 Authentication-Free User and Free IP Address Configuration Tasks

The following table describes authentication-free user and free IP address configuration tasks. These configurations are optional.

Table 3-2 Authentication-free user and free IP address configuration

No.	To do…	Use the command…	Remarks
1	Enter system view	**system-view**	—
2	Configure a free IP address	**portal free-ip** *ip-address* **interface** *interface-type interface-num*	The system supports up to eight free IP addresses, including the IP address of the portal server.
3	Configure an authentication-free user	**portal free-user ip** *ip-address* **interface** *interface-type interface-num*	Up to 32 authentication-free users can be configured.
4	Display configuration information about authentication-free users and free IP addresses	**display portal** [**free-ip** | **free-user**]	Available in any view

Use the corresponding **undo** command to remove a configuration.

⚠ **Caution:**

- To enable portal authentication on an interface, be sure you have configured authentication-free users and free IP addresses.
- In re-DHCP authentication mode, the IP address of an authentication-free user and the primary IP address of the interface must be on the same network segment. In direct authentication mode, the IP address of an authentication-free user and the IP address of the interface must be on the same network segment.

3.3.3 Authentication-Free User and Free IP Configuration Example

I. Network requirements

- Configure portal authentication on the router. Set the portal operating mode to direct authentication and the name of the portal server to newp.
- Before passing the authentication, the user can access Server 1, an internal server.

- Server 2 can access the Internet without authentication.

II. Network diagram

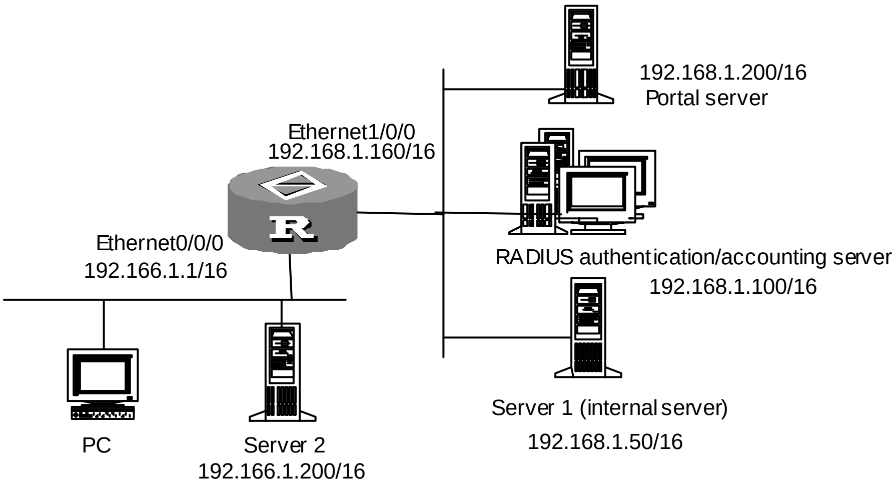


Figure 3-5 Network diagram for authentication-free users and free IP addresses

III. Configuration procedure

Note:

The following describes only the configurations related to authentication-free users and free IP addresses. For configurations of the RADIUS scheme and ISP domain, refer to section 3.2.3 "Direct Authentication Configuration Example".

# Configure the portal server with a name of newp, an IP address of 192.168.1.200, a key of huawei, a port of 50100, and a URL of http://192.168.1.200/portal.

```
[3Com] portal server newp ip 192.168.1.200 key huawei port 50100 url
http://192.168.1.200/portal
```

# Configure the portal operating mode as direct authentication.

```
[3Com] portal method direct
[3Com] portal auth-network 192.166.1.1 255.255.0.0 ethernet 0/0/0
```

# Configure Server 2 as an authentication-free user.

```
[3Com] portal free-user ip 192.166.1.200 interface ethernet 0/0/0
```

# Configure the IP address of Server 1 as a free IP address.

```
[3Com] portal free-ip 192.168.1.50 interface ethernet 0/0/0
```

Enable portal authentication on interface ethernet0/0/0.

```
[3Com] interface ethernet0/0/0
[3Com-ethernet0/0/0] ip address 192.166.1.1 255.255.0.0
[3Com-ethernet0/0/0] portal newp
[3Com-ethernet0/0/0] quit
```

Chapter 4 EAD Configuration

4.1 Introduction to EAD

On an enterprise network that implements host-level attack defense, every user has to install antivirus software, kill virus, and update virus database themselves. This is both inefficient and not good for integrated management. In addition, it may expose the network to security hazards, for example, when a user fails to patch or upgrade software.

Endpoint admission defense (EAD) is an attack defense solution developed based on Huawei comprehensive access management server (CAMS) system. Different from traditional defense ideas, it centralizes security policy deployment, and controls endpoint admission by evaluating the security compliance of endpoints and dynamically controlling their access rights. This enhances the active defense ability of endpoints, and prevents virus and worms from spreading on the network.

EAD requires the cooperation between security client, antivirus client, security cooperation device (such as a router), portal server, and third-party server (such as patch server and antivirus server). It provides the following functions:

- Check the security compliance and defense ability of endpoints, ensuring that the operating system (OS) has been patched, antivirus software and virus database have been updated, and no virus is present. An endpoint can access the network only when it is compliant with the security policy of the enterprise. In conjunction with identity authentication techniques, EAD ensures that only those legitimate and trusted endpoints can access the network.
- Isolate “dangerous” and “vulnerable” endpoints. EAD achieves this by granting only limited access rights to endpoints incompliant with the security policy of the enterprise. For example, you may allow infected endpoints and endpoints whose system patches and virus databases are not up to date to access only antivirus server, patch server, and the like for system repair.
- Forcibly repair system patches and upgrade antivirus software. After an endpoint is isolated, EAD can automatically remind the user to update software patch/virus database, or update software automatically in conjunction with the antivirus or patch server so that the endpoint can meet the security policy.

- Management and control. EAD provides a user management platform incorporating access policy, security policy, service policy, and security event monitoring. It can help the network administrator to customize network policies based on user identity. Moreover, in conjunction with the security policy server and the security client, EAD can implement mandatory security configuration and security event monitoring for endpoints.

The EAD solution for routers incorporates portal+. Portal+ is an enhancement to portal. Different from portal where forcible authentication is supported only for HTTP requests, portal+ can cooperate with the EAD client to provide security authentication in addition to access authentication.

4.1.1 Application of EAD

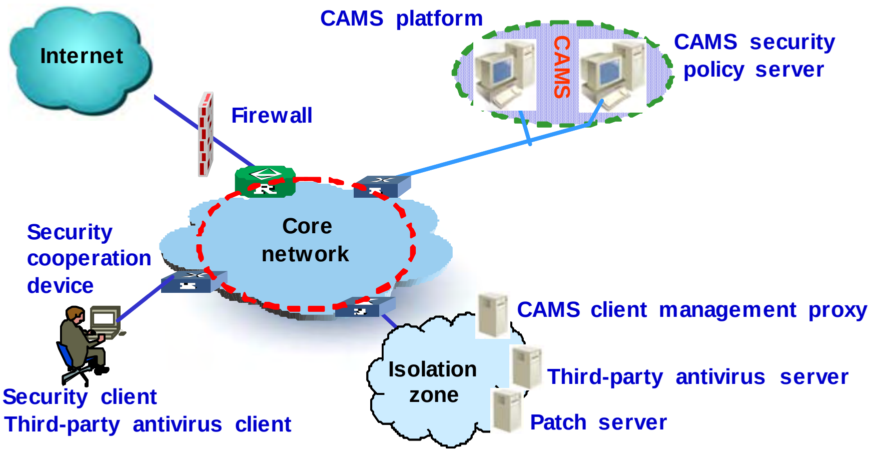

Internet
CAMS platform
CAMS
CAMS security policy server
Firewall
Core network
Security cooperation device
CAMS client management proxy
Isolation zone
Third-party antivirus server
Patch server
Security client
Third-party antivirus client

Figure 4-1 Network diagram for EAD combined with portal authentication

Portal authentication-combined EAD involves five types of devices; they are described in the following subsections.

II. Security client

Security client is installed on endpoints for endpoint authentication, security assess, and security policy enforcement. It functions to:

- Provide portal authentication. In conjunction with a security cooperation device, for example, a router, it can control endpoint admission.
- Check the security compliance of endpoints by checking OS version, completeness of system patches, and other information. In conjunction with the

antivirus client, it can check antivirus software version, virus database version, and virus scan/kill history.

- Implement security policies. It can receive the security policy issued by the security policy server and force it upon endpoints.
- Monitor system security status in real time and regularly report security events to the security policy server.

III. Security cooperation device

In this manual, security cooperation devices are routers that can do the following:

- Force the endpoint users attempting to access the network to accept identity authentication and security evaluation.
- Isolate non-compliant endpoints. A security cooperation device can isolate endpoints or remove isolation online when receiving the isolation or isolation removal command issued by the security policy server.

IV. Security policy server

In an EAD solution, the security policy server is the management and control center. It functions to:

- Manage security policies. The security policy server defines a set of policies used for endpoint admission control, covering aspects such as endpoint security evaluation criteria, endpoint recovery method, and isolation criteria.
- Manage users. The security policy server can provide identity-specific differentiated security configuration and network service class.
- Control security cooperation. The security policy server can evaluate the security reports of endpoints, command the security cooperation device to isolate endpoints or to remove isolation, and issue security policies to endpoints.
- Audit log. The security policy server can collect and log the security events reported by security clients for the administrator to trace and monitor network security.

V. Security client manager proxy

The security client and the security policy server communicate through the security client manager proxy.

VI. RADIUS server

RADIUS server authenticates identities of endpoint users.

VII. Portal server

A portal server provides portal authentication. To work with EAD, a portal server must support portal+.

Note:

In Figure 4-1, the security policy server and the RADIUS server are provided by the CAMS platform, and the portal server is provided by the CAMS portal service component.

VIII. Third-party server

In an EAD solution, the third-party server could be an antivirus or patch server providing the virus database update or patch update service to endpoint users.

4.1.2 Basic EAD Procedures

The endpoint authentication process of EAD is divided into two phases: identity authentication and security authentication.

I. Identity authentication phase

In the identify authentication phase, AAA RADIUS authentication is implemented through portal+, where user identity is verified by verifying username and password. This phase involves the following steps:

An unauthenticated endpoint sends an IP packet to the router.

The router checks the received packet and finds out that it is sent from an unauthenticated IP address. Then, the router sends back a mandatory authentication request carrying the IP address and port number of a portal server.

After receiving the authentication request, the client obtains the user name and password and initiates an authentication request to the portal server.

1) After receiving the authentication request, the portal server interacts with the RADIUS server to complete AAA authentication following the same authentication procedure adopted by portal.

After an endpoint user passes identity authentication, it is placed in an isolation zone and can access the update resources in the isolation zone.

II. Security authentication phase

In the security authentication phase, the security policy server evaluates the security compliance of endpoints based on reported security information. This phase involves the following steps:

1) After an endpoint user passes identity authentication, the security policy server issues the IP address and port number of a security client manager proxy and an isolation ACL to the router. According to the isolation ACL, the router places the endpoint user in the isolation zone.
2) The router notifies the portal server of the identity authentication success, carrying the IP address and port number of the security client manager proxy in the notification.
3) The portal server notifies the security client of the identity authentication success, carrying the IP address and port number of the security client manager proxy in the notification.
4) The security client interacts with the security policy server through the security client manager proxy, and as required completes virus database and patch check/update and security authentication.
5) After the endpoint passes security authentication, the security policy server issues a security ACL to the router to reassign an access right to the endpoint user and to remove isolation.

If the endpoint user passes security authentication, it can access all network resources; if not, it can access only the update resources in the isolation zone.

4.2 EAD Configuration

4.2.1 Configuration Prerequisites

Complete necessary AAA and RADIUS configurations.

4.2.2 Configuring EAD

Table 4-1 Configure EAD

To do…	Use the command…	Remarks
Enter system view	**system-view**	—
Set the portal service type to portal+	**portal service-type plus**	Required The default portal service type is normal portal mode.

To do…	Use the command…	Remarks
Specify a portal server	**portal server** *server-name* { **ip** *ip-address* | **key** *key-string* | **port** *port* | **url** *url-string* } *	Required By default, no portal server is specified. When configuring a portal server, the *key-string* argument defaults to huawei, the *port* argument defaults to 50100, and the *url-string* argument defaults to the character string of *ip-address*.
Configure the operating mode of portal	**portal method** { **direct** | **redhcp** }	Optional The default portal operating mode is direct authentication. For an application supporting portal authentication for non-directly connected network segments, you can configure direct authentication only.
Configure an authentication network segment	**portal auth-network** *network-address net-mask* **interface** *interface-type interface-num*	Required
Create a resource name	**portal resource** *resource-name*	Optional The default resource name is huawei.
Add an IP address to update resources	**portal update-resource ip** *ip-address* [**mask** *mask*]	Required Normally, patch server, antivirus server, security client manager proxy are added to update resources.
Add an update-resource ID	**portal update-resource-id** *number*	Required You are recommended to configure the update-resource ID the same as the isolation ACL configured on the security policy server for the router
Add an all-resource ID	**portal all-resource-id** *number*	Required This ID must be the same as the security ACL configured on the security policy server for the router.
Enter interface view	**interface** *interface-type interface-number*	Required
Assign an IP address to the interface	**ip address** *ip-address mask*	Required

To do…	Use the command…	Remarks
Configure the IP address of the interface connected to the CAMS server	**portal upload-ip** *ip-address*	Required This command must be configured on the interface enabled with portal authentication.
Enable portal authentication on the interface	**portal** *server-name*	Required
Exit to system view	**quit**	—
Enter RADIUS scheme view	**radius scheme** *radius-scheme-name*	Required
Set the server type to portal	**server-type portal**	Required
Configure the IP address of security policy server	**security-policy-server** *ip-address*	Optional
Display configuration information and statistics about portal	**display portal** [**acm statistics** | **auth-network** [**auth-interface** *interface-type interface-num*] | **free-user** | **free-ip** | **interface** [*interface-type interface-num*] | **server** [*server-name*] | | **server statistics** | **tcp-cheap statistics|** **update-resource**]	Execute the command in any view.

Note:

- Enable portal authentication only after completing the portal+ authentication configuration.
- Neither authentication-free users nor devices with free IP addresses are to be isolated.
- You need to configure the **security-policy-server** command only when RADIUS, portal, and security policy servers are not co-located.
- For EAD, you may configure portal to operate in direct authentication mode or re-DHCP authentication mode while the portal authentication mode must be set to normal.

4.3 Portal Authentication-Combined EAD Configuration Example

I. Network requirements

The following figure presents a scenario, where

- A security policy server, a RADIUS server, and a portal server are co-located on a CAMS server with IP address 10.110.91.146/24.
- A patch and antivirus server with IP address 10.22.2.2/24 is located in an isolation zone.
- A security client manager proxy is present with IP address 10.22.2.1/24.
- The update-resource ID is 10 and all-resource ID is 20.
- A PC (an endpoint) is located on the network segment 172.21.1.2/16.

Configure the router to provide EAD, requiring that:

- The PC could only access the antivirus server after passing identity authentication and before passing security authentication.
- The PC could access other network resources after passing security authentication.

II. Network diagram

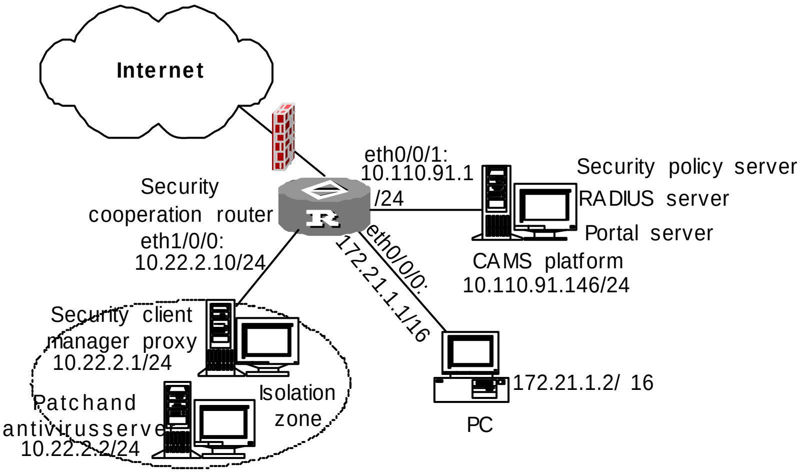


Figure 4-2 Network diagram for EAD combined with portal authentication

III. Configuration procedure

1) Configure the security cooperation router

# Set the portal service type to portal+.

```
<3Com> system-view
[3Com] portal service-type plus
```

# Configure information on the portal server, setting its name to newp, IP address to 10.110.91.146, key to huawei, port number to 50100, and URL to http://10.110.91.146 /portal.

```
[3Com] portal server newp ip 10.110.91.146 key huawei port 50100 url
http://10.110.91.146 /portal
```

# Set the portal operating mode to direct authentication.

```
[3Com] portal method direct
[3Com] portal auth-network 172.21.0.0 255.255.0.0 ethernet 0/0/0
```

# Configure IP addresses of update resources.

```
[3Com] portal update-resource ip 10.22.1.1
[3Com] portal update-resource ip 10.22.2.1
```

# Configure the update-resource ID and all-resource ID.

```
[3Com] portal update-resource-id 10
[3Com] portal all-resource-id 20
```

# Assign an IP address to interface Ethernet 0/0/1.

```
[3Com] interface ethernet0/0/1
[3Com-ethernet0/0/1] ip address 10.110.91.1 255.255.255.0
[3Com-ethernet0/0/1] quit
```

# Enable portal authentication on interface Ethernet 0/0/0 and configure the IP address of the interface connected to the CAMS server.

```
[3Com] interface ethernet0/0/0
[3Com-ethernet0/0/0] ip address 172.21.1.1 255.255.0.0
[3Com-ethernet0/0/0] portal upload-ip 10.110.91.1
[3Com-ethernet0/0/0] portal newp
[3Com-ethernet0/0/0] quit
```

# Configure interface Ethernet 1/0/0.

```
[3Com] interface ethernet1/0/0
[3Com-ethernet1/0/0] ip address 10.22.2.10 255.255.255.0
[3Com-ethernet1/0/0] quit
```

# Create a RADIUS scheme.

```
[3Com] radius scheme system
```

# Set the server type to portal.

```
[3Com-radius-system] server-type portal
```

2) Configure the security policy server

Do the following on the security policy server:

- Define software names, software patches, virus database version, antivirus engine, and so on.
- Set the IP address of antivirus and patch server to 10.22.1.1/24.
- Set the IP address of security client manager proxy to 10.22.2.1/24.
- Set isolation ACL to 10 and security ACL to 20.

Note:

- The configuration of AAA and RADIUS is beyond the scope of this example. For their configuration, refer to Chapter 2 “AAA and RADIUS/HWTACACS Protocol Configuration.”
- The configuration of RADIUS Server and security policy server is beyond the scope of this example. For their configuration, refer to *CAMS Platform User Manual* and *CAMS EAD Security Policy Component User Manual*.

Chapter 5 ACL Configuration

5.1 Introduction to ACL

5.1.1 ACL Overview

In order to filter data packets, a series of rules need to be configured on the router to decide which data packets can pass. These rules are defined by ACL (Access Control List), which are a series of sequential rules consisting of **permit | deny** statements. The rules are described by source address, destination address and port number of data packets. ACL classifies data packets through these router interface applied rules, by which the router decides which packets can be received and which should be rejected.

5.1.2 Classification of ACL

According to application purpose, ACL falls into four groups:

- Basic ACL
- Advanced ACL
- Interface-based ACL
- MAC-based ACL

The application purpose of ACL is specified by the range of the number. Interface-based ACL ranges from 1000 to 1999; basic ACL ranges from 2000 to 2999; advanced ACL ranges from 3000 to 3999; and MAC-based ACL ranges from 4000 to 4999.

5.1.3 Match order of ACL

An access control rule may consist of several **permit | deny** statements, each statement specifying different packet ranges. In this case, match order problem exists on matching a packet and access control rule.

There are two kinds of match orders:

- Configuration sequence: match ACL rules according to their configuration order.
- Automatic sequencing: follow the principle of “depth priority”.

“Depth priority” rule puts the statement that specifies the smallest packet range into first place. This can be realized by comparing address wildcard. The smaller the wildcard is, the smaller the specified host range. For example, 129.102.1.1 0.0.0.0 specifies a host: 129.102.1.1, while 129.102.1.1 0.0.255.255 specifies a network segment: from 129.102.1.1 to 129.102.255.255. Obviously, the former is put first in access control rule. The detailed standard is: for statements of basic access control rule, directly compare their source address wildcards. If the same wildcard is shared, arrange them according to configuration sequence. For interface-based access control rules, put the rule configured with “any” behind, and arrange others according to configuration sequence. For advance access control rules, compare their source address wildcards first. If they are the same, compare their destination address wildcards. If they are also the same, compare their ranges of port number. Put those with smaller ranges before others. If the ranges of port number are still the same, arrange then according to configuration sequence.

The **display acl** command can be used to verify which rule takes effect first. Upon the display, the rule that is listed first takes effect first.

5.1.4 ACL Creation

An ACL is virtually a series of rule lists that consist of **permit | deny** statements. Several rule lists constitute an ACL. Before configuring the rule of ACL, you need to create an ACL first.

The following command can be used to create an ACL:

acl number *acl-number* [**match-order** { **config | auto** }]

The following command can be used to delete an ACL:

undo acl { **number** *acl-number* **| all** }

Parameter description:

- **number** *acl-number*: Specify a number-typed ACL.
- *acl-number*: Number of ACL. An interface-based ACL takes a value in the range 1000 to 1999, a number-based basic ACL in the range 2000 to 2999, a number-based advanced ACL in the range 3000 to 3999, and a MAC-based ACL in the range 4000 to 4999.
- **match-order config**: Specify to match rules according to configuration sequence of the user.
- **match-order auto**: Specify to match rules by system automatic sequencing, namely in “depth priority” sequence.
- **all**: Delete all configured ACL.

By default, the match order is configuration sequence of the user, namely “**config**” is in use. Once the user specifies the match order of a certain ACL, he can never change it, unless he deletes all the contents in the ACL and specifies its match order again.

ACL view can be entered after an ACL is created. ACL view is classified according to the application purpose of ACL. For example, advanced ACL view can be entered by creating a number-typed ACL numbered 3000. The following is the router prompt:

```
[3Com-acl-adv-3000]
```

After entering the ACL view, you can configure ACL rules. The rules of different ACLs are different. The detailed configuration method of each ACL rule will be introduced respectively in the following sections.

5.1.5 Basic ACL

Basic ACL can only adopt source address information to serve as element for defining ACL rule. A basic ACL can be created and basic ACL view be entered by the above-mentioned ACL command. In basic ACL view, the rule of basic ACL can be created.

The following command can be used to define a basic ACL rule:

rule [*rule-id*] { **permit | deny | comment** *text* } [**source** *sour-addr sour-wildcard* **| any**] [**time-range** *time-name*] [**logging**] [**fragment**] [**vpn-instance** *vpn-instance-name*]

Parameter description:

- *rule-id*: Optional parameter, number of ACL rule, ranging from 0 to 65534. After the number is specified, if the ACL rule related to the number has existed, a newly defined rule may be used to overwrite the old definition, just as editing an existing ACL rule. If the ACL rule related to the number does not exist, use the specified number to create a new rule. When the number is not specified, it indicates to add a new rule. In this case, the system will assign a number automatically for the ACL rule and add the new rule.
- **permit**: Permit qualified data packet.
- **deny**: Discard qualified data packet.
- **comment** *text*: Specifies a comment for each rule.
- **source**: Optional parameter, used to specify source address information of ACL rule. If it is not specified, it indicates any source address of the packet matches.
- *source-addr*: Source address of data packet, in dotted decimal. Or, “**any**” may be used to represent source address 0.0.0.0, with wildcard being 255.255.255.255.
- *source-wildcard*: Wildcard of source address, in dotted decimal.
- **time-range**: Optional parameter, used to specify effective time range of ACL.
- *time-name*: Name of ACL effective time range.
- **logging**: Optional parameter, indicating whether to log qualified data packet. The log content includes sequence number of access control rule, data packet passed or discarded and the number of data packets.
- **fragment**: Optional parameter, used to specify whether the rule is only valid for non-first-fragment. When this parameter is included, it indicates the rule is only valid for non-first-fragment.
- **vpn-instance**: Optional parameter specifying the vpn-instance to which the packets belong. If it is not specified, the ACL rule will be valid for the packets in all the vpn-instances. If it is specified, the ACL rule will be valid only for the specified vpn-instance.

For existing ACL rule, if edit is performed with specified ACL rule number, the rest part will not be affected. For example:

First configure an ACL rule:

rule 1 deny source 1.1.1.1 0

Then edit the ACL rule:

rule 1 deny logging

And then, the ACL rule becomes:

rule 1 deny source 1.1.1.1 0 logging

The following command can be used to delete a basic ACL rule:

undo rule *rule-id* [**comment** *text*] [**source**] [**time-range**] [**logging**] [**fragment**] [**vpn-instance** *vpn-instance-name*]

Parameter description:

- *rule-id*: Number of ACL rule, which should be an existing ACL rule number. If there is no parameter followed, the entire ACL rule will be deleted. Otherwise, only part of information related to the ACL rule will be deleted.
- **comment** *text*: Specifies a comment for each rule.
- **source**: Optional parameter. Only the source address information setting of ACL rule with corresponding number will be deleted.
- **time-range**: Optional parameter. Only the specific effective time range setting of ACL rule with corresponding number will be deleted.
- **logging**: Optional parameter. Only the logging qualified packet setting of ACL rule with corresponding number will be deleted.
- **fragment**: Optional parameter. Only the validation setting solely for non-first-fragment of ACL rule with corresponding number will be deleted.
- **vpn-instance**: Optional parameter. If it has been specified, the deletion operation will delete only the settings involved the vpn-instance in the ACL rule with the specified number.

5.1.6 Advanced ACL

Advanced ACL can define rules by using such contents of data packet as source address information, destination address information, IP carried protocol type and protocol oriented feature (for example, source port and destination port of TCP, type and code of ICMP). Advance ACL can be used to define more accurate, diversified and flexible rules than basic ACL.

An advanced ACL can be created and advanced ACL view be entered by the previously mentioned ACL command. In advance ACL view, the rules of advanced ACL can be created.

The following command can be used to define an advanced ACL rule:

rule [*rule-id*] { **permit** | **deny** | **comment** *text* } *protocol* **source** [*sour-addr sour-wildcard* | **any**] **destination** [*dest-addr dest-mask* | **any**] [**soucre-port** *operator port1* [*port2*]] [**destination-port** *operator port1* [*port2*]] [**icmp-type** { *icmp-message* |*icmp-type icmp-code*}] [**dscp** *dscp*] [**precedence** *precedence*] [**tos** *tos*] [**time-range** *time-name*] [**logging**] [**fragment**] [**vpn-instance**]

Parameter description:

- *rule-id*: Optional parameter, number of ACL rule, ranging from 0 to 65534. After the number is specified, if the ACL rule related to the number has existed, a newly defined rule may be used to overwrite the old definition, just as editing an existing ACL rule. If the ACL rule related to the number does not exist, use the specified number to create a new rule. When the number is not specified, it indicates to add a new rule. In this case, the system will assign a number automatically for the ACL rule and add the new rule.
- **deny**: Discard qualified data packet.
- **permit**: Permit qualified data packet.
- **comment** *text*: Specifies a comment for each rule.
- *protocol*: IP carried protocol type represented by name or number. The number range is from 1 to 255. The name can be gre, icmp, igmp, ip, ipinip, ospf, tcp, and udp.
- **source**: Optional parameter, used to specify source address information of ACL rule. If it is not configured, it indicates any source address of the packet matches.
- *source-addr*: Source address of data packet, in dotted decimal. Or, "**any**" may be used to represent source address 0.0.0.0, with wildcard being 255.255.255.255.
- *source-wildcard*: Wildcard of source address, in dotted decimal.
- **destination**: Optional parameter, used to specify destination address information of ACL rule. If it is not configured, it indicates any destination address of the packet matches.
- *dest-addr*: Destination address of data packet, in dotted decimal. Or, "**any**" may be used to represent destination address 0.0.0.0, with wildcard being 255.255.255.255.
- *dest-wildcard*: Destination address wildcard, in dotted decimal. Or, "**any**" may be used to represent destination address 0.0.0.0, with wildcard being 255.255.255.255.
- **icmp-type**: Optional parameter, used to specify type of ICMP packet and message code information, only valid when the packet protocol is ICMP. If it is not configured, it indicates any type of ICMP packet matches.
- *icmp-type*: ICMP packet can be filtered according to the message type of ICMP. It is a number ranging from 0 to 255.
- *icmp-code*: ICMP packet filtered according to ICMP message type can also be filtered according to message code. It is a number ranging from 0 to 255.
- *icmp-message*: ICMP packet can be filtered according to name of ICMP type or name of ICMP code.
- **source-port**: Optional parameter, used to specify source port information of UDP or TCP message, only valid when the specified protocol number is TCP or UDP. If it is not specified, it indicates any source port information of TCP/UDP packet matches.

- **destination-port**: Optional parameter, used to specify destination port information of UDP or TCP packet, only valid when the protocol number specified by the rule is TCP or UDP. If it is not specified, it indicates any destination port information of TCP/UDP packet matches.
- *operator*: Optional parameter. The port number operator, name and meaning of source/destination address are compared as follows: lt (lower than), gt (greater than), eq (equal to), neq (not equal to) and range (between). Only “range” needs two port numbers as operator, others only need one port number as operator
- *port1, port2*: Optional parameter, port number of TCP or UDP, represented by name or number, with the number ranging from 0 to 65535.
- **dscp** *dscp*: Specifies a DSCP field (the DS byte in IP packets).
- **precedence**: Optional parameter, by which data packets can be filtered. A number ranging from 0 to 7 or a name.
- **tos** *tos*: Type of service value, an optional parameter by which data packets can be filtered.This number uses the second bit to the fifth bit in the ToS field, from right to left. As shown in the following figure, the *tos* argument in an ACL ranges from 0 to 15, indicating the real range of 0 to 30.

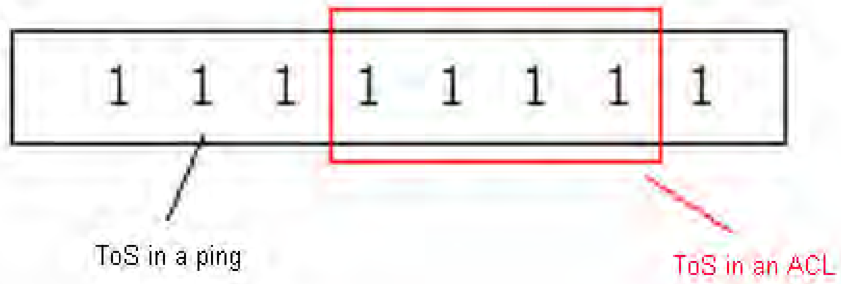


Figure 5-1 ToS defined in an ACL

When testing the ToS setting, 1 for example, in an ACL with the **ping -tos** command, you must set the *-tos* argument to 2, that is, twice of the ToS setting in the ACL.

- **logging**: Optional parameter, indicating whether to log qualified data packet. The log contents include sequence number of ACL, data packet passed/discarded, upper layer protocol type over IP, source/destination address, source/destination port number, and the number of data packets.
- **time-range** *time-name*: The ACL rule is valid in the time range.
- **fragment**: Used to specify whether the rule is only valid for non-first-fragment. When this parameter is included, it indicates the rule is only valid for non-first-fragment.
- **vpn-instance**: Optional, specifies a vpn-instance. If it is not specified, the ACL rule is invalid for packets in all vpn-instances. If it is specified, the ACL rule is valid only for the specified vpn-instance.

For existing ACL rule, if edit is performed with specified ACL rule number, the rest part will not be affected. For example:

First configure an ACL rule:

rule 1 deny ip source 1.1.1.1 0

Then edit the ACL rule:

rule 1 deny ip destination 2.2.2.1 0

And then, the ACL rule becomes:

rule 1 deny ip source 1.1.1.1 0 destination 2.2.2.1 0

The following command can be used to delete an advanced ACL rule:

undo rule *rule-id* [**comment** *text*] [**source**] [**destination**] [**source-port**] [**destination-port**] [**icmp-type**] [**dscp**] [**precedence**] [**tos**] [**time-range**] [**logging**] [**fragment**] [**vpn-instance** *vpn-instance-name*]

Parameter description:

- *rule-id*: Number of ACL rule, which should be an existing ACL rule number. If there is no parameter followed, the entire ACL rule will be deleted. Otherwise, only part of information related to the ACL rule will be deleted.
- **comment** *text*: Specifies a comment for each rule.
- **source**: Optional parameter. Only the source address information setting of ACL rule with corresponding number will be deleted.
- **destination**: Optional parameter. Only the destination address information setting of ACL rule with corresponding number will be deleted.
- **source-port**: Optional parameter. Only source port information setting of ACL rule with corresponding number will be deleted. It is only valid when the protocol number of the rule is TCP or UDP.
- **destination-port**: Optional parameter. Only the destination port information setting of ACL rule with corresponding number will be deleted. It is only valid when the protocol number of the rule is TCP or UDP.
- **icmp-type**: Optional parameter. Only ICMP type and message code information setting of ACL rule with corresponding number will be deleted. It is only valid when the protocol number of the rule is ICMP.
- **dscp** *dscp*: Specifies a DSCP value. For IP packets, it is a DS value.
- **precedence**: Optional parameter. Only the precedence setting of ACL rule with corresponding number will be deleted.
- **tos**: Optional parameter. Only the tos setting of ACL rule with corresponding number will be deleted.
- **time-range**: Optional parameter. Only the specific effective time range setting of ACL rule with corresponding number will be deleted.
- **logging**: Optional parameter. Only the logging qualified packet setting of ACL rule with corresponding number will be deleted.

- **fragment**: Optional parameter. Only the validation setting solely for non-first-fragment of ACL rule with corresponding number will be deleted.
- **vpn-instance**: Optional parameter. If it has been specified, the deletion operation will delete only the settings involved the vpn-instance in the ACL rule with the specified number.

Only TCP and UDP protocols need to specify port range. The supported operators and grammar are listed below.

Table 5-1 Operator meaning of advanced ACL

Operator and grammar	Meaning
eq portnumber	Equal to port number
gt portnumber	Greater than port number
lt portnumber	Lower than port number
neq portnumber	Not equal to port number
range portnumber1 portnumber2	Between portnumber1 and portnumber2

When specifying *portnumber*, part of common port numbers can use mnemonics to substitute actual numbers. The supported mnemonics are shown in the table below.

Table 5-2 Port number mnemonics

Protocol	Mnemonics	Meaning and actual value
TCP	Bgp	Border Gateway Protocol (179)
	Chargen	Character generator (19)
	Cmd	Remote commands (rcmd, 514)
	Daytime	Daytime (13)
	Discard	Discard (9)
	Domain	Domain Name Service (53)
	Echo	Echo (7)
	Exec	Exec (rsh, 512)
	Finger	Finger (79)
	Ftp	File Transfer Protocol (21)
	Ftp-data	FTP data connections (20)
	Gopher	Gopher (70)
	Hostname	NIC hostname server (101)
	Irc	Internet Relay Chat (194)
	Klogin	Kerberos login (543)
	Kshell	Kerberos shell (544)
	Login	Login (rlogin, 513)
	Lpd	Printer service (515)
	Nntp	Network News Transport Protocol (119)
	Pop2	Post Office Protocol v2 (109)
	Pop3	Post Office Protocol v3 (110)
	Smtp	Simple Mail Transport Protocol (25)
	Sunrpc	Sun Remote Procedure Call (111)
	Syslog	Syslog (514)
	Tacacs	TAC Access Control System (49)
	Talk	Talk (517)
	Telnet	Telnet (23)
	Time	Time (37)
	Uucp	Unix-to-Unix Copy Program (540)
	Whois	Nicname (43)
	Www	World Wide Web (HTTP, 80)

Protocol	Mnemonics	Meaning and actual value
UDP	biff	Mail notify (512)
	bootpc	Bootstrap Protocol Client (68)
	bootps	Bootstrap Protocol Server (67)
	discard	Discard (9)
	dns	Domain Name Service (53)
	dnsix	DNSIX Security Attribute Token Map (90)
	echo	Echo (7)
	mobilip-ag	MobileIP-Agent (434)
	mobilip-mn	MobilIP-MN (435)
	nameserver	Host Name Server (42)
	netbios-dgm	NETBIOS Datagram Service (138)
	netbios-ns	NETBIOS Name Service (137)
	netbios-ssn	NETBIOS Session Service (139)
	ntp	Network Time Protocol (123)
	rip	Routing Information Protocol (520)
	snmp	SNMP (161)
	snmptrap	SNMPTRAP (162)
	sunrpc	SUN Remote Procedure Call (111)
	syslog	Syslog (514)
	tacacs-ds	TACACS-Database Service (65)
	talk	Talk (517)
	tftp	Trivial File Transfer (69)
	time	Time (37)
	who	Who(513)
	Xdmcp	X Display Manager Control Protocol (177)

For ICMP, ICMP packet type can be specified. The default is all ICMP packets. When specifying ICMP packet type, it can be a number (ranging from 0 to 255) or a mnemonic.

Table 5-3 Mnemonics of ICMP packet type

Mnemonic	Meaning
echo	Type=8, Code=0
echo-reply	Type=0, Code=0
fragmentneed-DFset	Type=3, Code=4
host-redirect	Type=5, Code=1
host-tos-redirect	Type=5, Code=3
host-unreachable	Type=3, Code=1
information-reply	Type=16,Code=0
information-request	Type=15,Code=0
net-redirect	Type=5, Code=0
net-tos-redirect	Type=5, Code=2
net-unreachable	Type=3, Code=0
parameter-problem	Type=12,Code=0
port-unreachable	Type=3, Code=3
protocol-unreachable	Type=3, Code=2
reassembly-timeout	Type=11,Code=1
source-quench	Type=4, Code=0
source-route-failed	Type=3, Code=5
timestamp-reply	Type=14,Code=0
timestamp-request	Type=13,Code=0
ttl-exceeded	Type=11,Code=0

The user can add appropriate access rules by configuring firewall. IP packets passing the router will be checked through packet filtering and the packets that the user does not want them to pass the router will be ruled out. Thus, network security is protected.

5.1.7 Interface-based ACL

Interface-based ACL is a kind of special ACL, which specifies rules according to packet-receiving interface.

An interface-based ACL can be created and interface-based ACL view be entered by the previously mentioned ACL command. In interface-based ACL view, the rules of interface-based ACL can be created.

The following command can be used to define an interface-based ACL rule:

rule [*rule-id*] { **permit** | **deny** | **comment** *text* } **interface** { *interface-type interface-number* | **any** } [**time-range** *time-name*] [**logging**]

Parameter description:

- *rule-id*: Optional. ACL rule number, ranging from 0 to 65534. After the number is specified, if the ACL rule related to the number has existed, a newly defined rule may be used to overwrite the old definition, just as editing an existing ACL rule. If the ACL rule related to the number does not exist, use the specified number to create a new rule. When the number is not specified, it indicates to add a new rule. In this case, the system will assign a number automatically for the ACL rule and add the new rule.

- **deny**: Discard qualified data packet.
- **permit**: Permit qualified data packet.
- **comment** *text*: Specifies a comment for each rule.
- **interface** *interface-type interface-number*: Specifies the interface information of the packets. If no interface is specified, all interfaces can be matched. **any** represents all interfaces.
- **logging**: Optional parameter, indicating whether to log qualified packet. Log contents include sequence number of ACL rule, packet permitted or discarded and the number of data packets.
- **time-range** *time-name*: Optional, specifies the time range in which the rule is valid.

The following command can be used to delete an interface-based ACL rule:

undo rule *rule-id* [**comment** *text*] [**logging | time-range**]*

Parameter description:

- *rule-id*: Number of ACL rule, which must be an existing ACL rule number.
- **comment** *text*: Specifies a comment for each rule.
- **logging**: Optional, indicating whether to log matched packets. The log contents include sequence number of ACL rule, packets passed or discarded, upper layer protocol type over IP, source/destination address, source/destination port number, and number of packets.
- **time-range**: Optional, specifies the time range in which the rule is valid.

5.1.8 MAC-Based ACL

MAC-based ACLs are numbered in the range 4000 to 4999.

You can use the following command to configure a MAC-based ACL rule:

rule [*rule-id*] { **deny | permit | comment** *text* } [**type** *type-code type-mask* | **lsap** *lsap-code lsap-mask*]] [**source-mac** *sour-addr sour-mask*] [**dest-mac** *dest-addr dest-mask*]

The parameters are described as follows:

- *rule-id* represents a rule number.
- **deny**: Discard qualified data packet.
- **permit**: Permit qualified data packet.
- **comment** *text*: Specifies a comment for each rule.
- *type-code* is a hexadecimal number in the format of xxxx, used for matching the protocol type of the transmitted packets.

- *type-mask* represents the protocol type mask. For type-code values, refer to the chapter that discusses bridge configuration in the link layer protocol part of this manual.
- *lsap-code* is a hexadecimal number in the format of xxxx, used for matching the encapsulation format of bridged packet on an interface. *lsap-wildcard* represents the wildcard (mask) of protocol type.
- *sour-addr* represents the source MAC address of a data frame in the format of xxxx-xxxx-xxxx. *sour-mask* represents the mask of the source MAC address.
- *dest-addr* represents the destination MAC address in the format of xxxx-xxxx-xxxx. *dest-mask* represents the mask of the destination MAC address.

The following command can be used to delete a MAC-based ACL rule:

undo rule *rule-id* [**comment** *text*]

The parameters are described as follows:

- *rule-id*: ACL rule number, which must exist already.
- **comment** *text*: Specifies a comment for each rule.

5.1.9 ACL Supporting Fragment

Traditional packet filtering does not process all IP packet fragments. Rather, it only performs matching processing on the first fragment and releases all the follow-up fragments. Thus, security dormant trouble exists, which makes attackers able to construct follow-up segments to realize traffic attack.

Packet filtering of 3Com router provides fragment filtering function, including: performing Layer3 (IP Layer) matching filtering on all fragments; at the same time, providing two kinds of matching, normal matching and exact matching, for ACL rule entries containing extension information (such as TCP/UDP port number and ICMP type). Normal matching is the matching of Layer3 information and it omits non-Layer3 information. Exact matching matches all ACL entries, which requires firewall should record the state of first fragment so as to obtain complete matching information of follow-up fragments. The default function mode is normal matching.

The keyword **fragment** is used in the configuration entry of ACL rule to identify that the ACL rule is only valid for non-first fragments. For non-fragments and first fragment, this rule is omitted. In contrast, the configuration rule entry not containing this keyword is valid for all packets.

For example:

```
[3Com-basic-2000] rule deny source 202.101.1.0 0.0.0.255 fragment
[3Com-basic-2000] rule permit source 202.101.2.0 0.0.0.255
[3Com-adv-3001] rule permit ip destination 171.16.23.1 0 fragment
[3Com-adv-3001] rule deny ip destination 171.16.23.2 0
```

In above rule entries, all entries are valid for non-first fragments. The first and the third entries are omitted for non-fragments and first fragment, only valid for non-first fragments.

5.2 Configuring an ACL

ACL configuration includes:

- Configure basic ACL
- Configure advanced ACL
- Configure interface-based ACL
- Configure MAC-based ACL
- Delete ACL

5.2.1 Configuring an Basic ACL

Perform the following configuration.

Table 5-4 Configure basic ACL

Operation	Command
Create a basic ACL in system view.	**acl number** *acl-number* [**match-order** { **config** | **auto** }]
Configure/delete an ACL rule in basic ACL view.	**rule** [*rule-id*] { **permit** | **deny** } **source** [*source-addr source-wildcard* | **any**] [**time-range** *time-name*] [**logging**] [**fragment**] [**vpn-instance** *vpn-instance-name*] **undo rule** *rule-id* [**source**] [**time-range**] [**logging**] [**vpn-instance** *vpn-instance-name*] [**fragment**]

For detailed introduction to parameters, refer to basic ACL.

5.2.2 Configuring an Advanced ACL

Perform the following configuration.

Table 5-5 Configure advanced ACL

Operation	Command
Create an advanced ACL in system view.	**acl number** *acl-number* [**match-order** { **config** | **auto** }]

Operation	Command
Configure/delete an ACL rule in advanced ACL view.	**rule** [*rule-id*] { **permit | deny** } *protocol* **source** [*source-addr source-wildcard* | **any**] **destination** [*dest-addr dest-mask* | **any**] [**sourer-port** *operator port1* [*port2*]] [**destination-port** *operator port1* [*port2*]] [**icmp-type** {*icmp-type icmp-code*| *icmp-message*}] [**precedence** *precedence*] [**tos** *tos*] [**time-range** *time-name*] [**logging**] [**fragment**] [**vpn-instance** *vpn-instance-name*] **undo rule** *rule-id* [**source**] [**destination**] [**source-port**] [**destination-port**] [**icmp-type**] [**precedence**] [**tos**] [**time-range**] [**logging**] [**fragment**] [**vpn-instance** *vpn-instance-name*]

5.2.3 Configuring an Interface-based ACL

Perform the following configuration.

Table 5-6 Configure an interface-based ACL

Operation	Command
Create an interface-based ACL in system view.	**acl number** *acl-number* [**match-order** { **config | auto** }]
Configure/delete an ACL rule in interface-based ACL view.	**rule** { **permit | deny** } [**interface** *type number*] [**time-range** *time-name*] [**logging**] **undo rule** *rule-id* [**time-range | logging**]*

You can specify an interface by specifying its type and number or all interfaces by specifying the **any** keyword.

5.2.4 Configuring a MAC-Based ACL

Perform the following configuration.

Table 5-7 Configure a MAC-based ACL

Operation	Command
Create a MAC-based ACL in system view.	**acl number** *acl-number* [**match-order** { **config | auto** }]

Operation	Command
Configure/delete an ACL rule in MAC-based ACL view.	**rule** [*rule-id*] { **deny** | **permit** } [**type** *type-code type-mask* | **lsap** *lsap-code lsap-mask*]] [**source-mac** *sour-addr sour-wildcard*] [**dest-mac** *dest-addr dest-mask*] **undo rule** *rule-id*

5.2.5 Deleting an ACL

Perform the following configuration in system view.

Table 5-8 Delete an ACL

Operation	Command
Delete ACL	**undo acl** { **number** *acl-number* | **all** }

5.3 Configuring Time Range

Time range configuration includes:

- Create a time range

5.3.1 Creating/Deleting a Time Range

The configuration task is used to create a time range or many time ranges with the same name.

Perform the following configuration in system view.

Table 5-9 Configure time range

Operation	Command
Create a time range	**time-range** *time-name* [*start-time* **to** *end-time*] [*days*] [**from** *time1 date1*] [**to** *time2 date2*]
Delete a time range.	**undo time-range** *time-name* [*start-time* **to** *end-time*] [*days*] [**from** *time1 date1*] [**to** *time2 date2*]

5.4 Displaying and Debugging ACL

After the above configuration, execute the **display** command in all views to display the running of the ACL configuration, and to verify the effect of the configuration. Execute the **reset** command in user view to rest ACL counters.

Table 5-10 Display and debug ACL

Operation	Command
Display the configured ACL rules.	**display acl** { **all** | *acl-number* }
Display information on time ranges.	**display time-range** { **all** | *time-name* }
Reset ACL counters.	**reset acl counter** { **all** | *acl-number* }

5.5 Typical Configuration Examples of ACL

Refer to the typical configuration examples in the part about packet filter.

Chapter 6 Firewall Configuration

6.1 Introduction to Firewall

In building construction, firewall is designed to prevent fire spreading from one part of the building to another part. Network firewall serves to the similar purpose: to prevent the Internet danger from spreading to your internal network.

On the one hand, firewall prohibits unauthorized or unauthenticated access from the Internet to the protected network. On the other hand, firewall permits internal network subscribers to Web access the Internet or send/receive E-mails. Firewall can also serve as an authority control gateway for accessing the Internet, for example, to permit specific person in an organization to access the Internet. Many firewalls now still bear some other attributes, such as subscriber identification, information security (encryption) processing and so on.

In addition to protecting Internet connection, a firewall can protect mainframes and important resources (such as data) on your network as well. All accesses to the protected data should pass the firewall, even for internal access from inside the organization.

When subscribers of external networks access internal network resources, they pass the firewall, so do internal network subscribers who access external network resources. In this case, firewall plays a role like a “guard” who discards data packets that should be prohibited.

In V 2.41, firewall mainly refers to ACL-based packet filter (referred to as ACL/packet filter throughout this manual), application specific packet filter (ASPF, also known as stateful firewall), and NAT. For more information about NAT, refer to the “Network Protocol” part in this manual. The following sections in this chapter mainly introduce ACL/packet filter and stateful firewall.

6.1.1 ACL/Packet Filter

I. ACL/Packet filter overview

The application of ACL/packet filter on the router endows the router with packet filter function. ACL/packet filter filters IP packets. For data packet that should be forwarded by the router, first obtain the header information of the packet, including upper layer protocol number over IP Layer, source address, destination address, source port and destination port of the packet, then compare with the configured ACL rule. Decide whether to forward or discard the packet according to the comparison result.

II. Packet filter supporting fragment filtering

ACL/packet filter on 3Com router supports testing and filtering of fragments. Packet filter tests packet type (non-fragment packet, first fragment or non-first fragment), obtains such information as Layer3 (IP Layer) information about the packet (basic ACL rule and advanced ACL rule not containing information except Layer3) and non-Layer3 information (advanced ACL rule containing non-Layer3 information) for matching, and obtains configured ACL rule.

For advanced ACL rule that has configured exact matching filtering, packet filter needs to record the non-Layer3 information of each first fragment. When the follow-up fragments arrive, the saved information will be used to perform full matching on each matching condition of ACL rule.

After exact matching is used for filtering, the implementation efficiency of packet filter will be slightly reduced. The more the matching entries are configured, the more the efficiency is reduced. Threshold can be configured to limit the maximum processing number of firewall.

For definitions of normal matching and exact matching, refer to the part about configuring ACL.

6.1.2 Application Specific Packet Filter

ACL/packet filter is a static firewall with the following problems:

- Some security policies are unable to foresee multi-channel application protocols such as FTP and H.323.
- It is unable for detecting some attacks such as TCP SYN, Java applet, and ActiveX, from the application layer.

Therefore, the concept of status firewall -- ASPF was brought forth. Application specific packet filter (ASPF) is packet filtering oriented to the application and transport layers, namely status based packet filtering. The application layer protocol detections include FTP, HTTP, SMTP, RTSP, and H.323 (Q.931, H.245, and RTP/RTCP) ones. The transport layer protocol detection contains general TCP/UDP detection.

ASPF is able to perform the primary functions as follows:

- Check application layer protocol information, such as the protocol type of a packet and port number. In addition, it monitors the connection-based application layer protocol status. ASPF maintains the information of each connection and dynamically decides whether to permit a data packet into the internal network for malicious-intrusion prevention.
- Detect the transport layer protocol information, that is, general TCP and UDP protocol detection. It can also decide whether to permit a TCP/UDP packet into the internal network.

ASPF implements the following additional functions:

- It can both filer packets based on connection status and detect packet contents at the application layer. Java Blocking to distrusted sites protects the network from malicious Java Applet.
- It enhances the session logging function and can log all the connection information including time, source address, destination address, the port in use, and the number of transmitted bytes.
- It supports Port to Application Map (PAM) and allows user-defined application protocol to use non-general port.

On the network edge, ASPF cooperates with common static firewall to provide comprehensive and practical security policy for intranets.

I. Basic Concepts

- Java blocking

Java Blocking blocks the java applet transferred by HTTP protocol. When Java Blocking configured, ASPF will block and filter out the request commands sent by users who attempt to obtain the Java applet-included programs from web pages.

- Port to application mapping

Application layer protocols use some (well-known) port numbers pre-defined by the system for communication. PAM (Port to Application Mapping) permits subscribers to define a set of new port numbers other than port numbers pre-defined by the system for different applications. PAM provides some mechanism to maintain and use port configuration information defined by subscribers.

PAM supports two kinds of mapping mechanisms: general port mapping and ACL-based host port mapping. General port mapping is to establish mapping relationship between user-defined port numbers and application layer protocols. For example, map 8080 port as HTTP protocol so that all TCP packets with destination port of 8080 could be regarded as HTTP packets. Host mapping is to establish mapping relationship between user-defined port numbers and application protocols for packets to/from some specific hosts. For example, map the TCP packets using the port 8080 and destined to the network segment 10.110.0.0 to HTTP packets. The range of hosts is specified by basic ACL.

- Single-channel protocol/multi-channel protocol

Single-channel protocol: Only one channel is available for data interaction from the establishment of a session to the end. Such protocols include SMTP and HTTP.

Multi-channel protocol: The interaction of the control information and the transfer of data are achieved in different channels. They can be FTP and RTSP.

- Internal interface and external interface

If a router connects an internal network and the Internet and deploys ASPF to protect the server of the internal network, the interface on the router connecting with the internal network is an internal interface while the one connecting with Internet is an external interface.

When ASPF is applied to the outbound direction of an external interface on the router, a temporary channel can be opened on the firewall for the returned packets of internal network users who access the Internet.

II. Fundamentals of application protocol layer detection

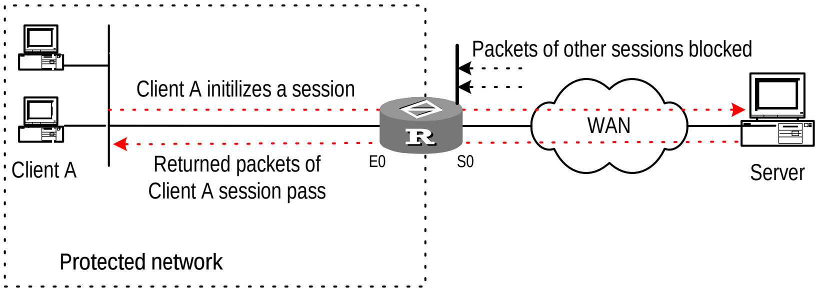


Figure 6-1 Fundamentals of application protocol layer detection

As shown in the above figure, generally a static ACL is needed on the router to allow a host of the internal network to access the external network and to prohibit a host of the external network to access internal network. However, a static ACL will filter out the returned packets after the user initiates a connection, so the connection cannot be established. When a router is configured with application layer protocol detection, ASPF is able to detect every session on application layer and create a status table and a temporary access control list (TACL). The status table is created once the first packet is detected and is used in maintaining the status of a session at a certain time detecting the session status transition is correct. The entry of a TACL is created together with a status entry and will be deleted after a session terminates. It seems like the permit entry in an extended ACL to match all the returned packets in a session. This functions like that a temporary channel is created at the external interface of the firewall for some returned packets.

Take FTP detection for example to illustrate the process of a multi-channel application layer protocol detection.

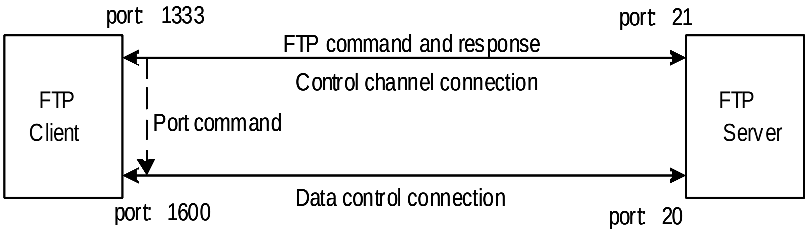


Figure 6-2 FTP detection process

Following is how an FTP connection is set up:

Suppose that an FTP Client initiates an FTP control channel connection from its port 1333 to the port 21 of FTP Server. After negotiation, Server initiates a data channel connection from its port 20 to the port 1600 of Client. The timeout or end of a data transfer makes a connection deleted.

Following is how FTP detection operates since an FTP connection is set up till it is disconnected:

1) Check the IP packet sent from the egress interface to the outside and acknowledges it is an FTP packet based on TCP.
2) Check the port number, acknowledge it as a control connection to create a TACL and status table for returned packets.
3) Check the FTP control connection packets, makes FTP instruction resolution, and updates the status table according to the instructions. If there are data channel establish instructions, then it creates the TACL for other data links. It does not detect the status of data links.
4) A match detection is performed on returned packets according to protocol type and then ASPF decides if to pass the packets after referring to the status table and TACL of the protocol.
5) The status table and TACL are cleared along with the deletion of an FTP connection.

The detection of single-channel application layer protocols, such as SMTP and HTTP, is rather simple. A TACL is created and cleared together with the connection.

III. Fundamentals of transport protocol layer detection

Here the transport layer protocol detection refers to TCP/UDP detection. Different from the application layer protocol detection, the transport layer protocol detects the packet information of transport layer, such as source address, destination address and port number. The TCP/UDP detection requires that the packets returned back to the external interface of ASPF match exactly the packets sent out it, that is, the source address, destination address and port number are right. Otherwise, the returned packets will be blocked. Therefore, you cannot establish a connection for the multi-channel application layer protocols such as FTP and .H.323, if you just configure TCP detection, but not application layer detection.

6.2 Configuring Packet Filter

Packet filter configuration includes:

- Enable or Disable Firewall
- Set the Default Filtering Mode of Firewall
- Enable Packet Filter Fragment Inspection
- Configure High/Low Threshold of Fragment Inspection
- Apply ACL on the Interface

6.2.1 Enabling or Disabling Firewall

Perform the following configuration in system view.

Table 6-1 Enable or disable firewall

Operation	Command
Enable firewall	**firewall enable**
Disable firewall	**undo firewall enable**

By default, firewall is disabled.

6.2.2 Setting the Default Filtering Mode of Firewall

To set the default filtering mode of firewall means when there is no appropriate rule to judge whether the user packet can pass, the policy adopted by the firewall is to permit the packet to pass or not.

Perform the following configuration in system view.

Table 6-2 Set the default filtering mode of firewall

Operation	Command
Set the default filtering mode as permitting the packet to pass	**firewall default permit**
Set the default filtering mode as denying the packet to pass	**firewall default deny**

When firewall is enabled, the default is to permit the packet to pass.

6.2.3 Applying ACL on the Interface

When applying access rule on the interface, the time range filtering principle is followed at the same time. Moreover, access rule can be specified respectively for transmitting and receiving packets on the interface.

Perform the following configuration in interface view.

Table 6-3 Apply ACL on the interface

Operation	Command
Specify the rule of filtering transmitting and receiving packets in the interface	**firewall packet-filter** *acl-number* { **inbound** | **outbound** } [**match-fragments** { **normally** | **exactly** }]
Remove the rule of filtering transmitting and receiving packets in the interface	**undo firewall packet-filter** *acl-number* { **inbound** | **outbound** }

You can only use the parameter **outbound** for interface-based ACL (ACL 1000 to 1999).

The **match-fragments** keyword can be applied to advanced ACLs only. For information about how to configure packet filter to filter fragments, refer to section 6.2.4 "Configuring Packet Filter to Filter Fragments".

The standard matching is used by default.

6.2.4 Configuring Packet Filter to Filter Fragments

The following are the configuration tasks for filtering fragments based on source address and/or time range information:

- Configure a basic ACL
- Apply the basic ACL on the interface

The following are the configuration tasks for filtering fragments based on layer 4 information:

- Configure an advanced ACL
- Enable packet filter fragment inspection
- Configure the upper/lower threshold of fragment inspection (optional)
- Apply the advanced ACL on the interface

I. Configuring an ACL

To filter non-first fragments only, you must specify the **fragment** keyword in the **rule** command used for configuring a basic or advanced ACL.

🕮 **Note:**

The matching of non-first-fragments depends on how the first fragment is processed. Only when the first fragment of a packet is “permitted” by the ACL, does the router records the extension information of the packet. If the first fragment of a packet is “denied” by the ACL, the router does not record any information about the packet. Therefore, the extension information in the ACL affects non-first-fragments only when the first fragment is “permitted”.

II. Enabling packet filter fragment inspection

This command is required for exact matching. Only when fragment inspection is enabled, does the packet filter records the status of the fragments and performs exact matching based on extension information in the advance ACL.

Perform the following configuration in system view.

Table 6-4 Enable fragment inspection

Operation	Command
Enable fragment inspection	**firewall fragments-inspect**
Disable fragment inspection	**undo firewall fragments-inspect**

🕮 **Note:**

If you want the router to filter fragments based on only layer 3 information, you do not need to enable the fragment inspection.

III. Configuring upper/lower threshold of fragment inspection (optional)

Perform the following configuration in system view.

Table 6-5 Configure upper/lower threshold of fragment inspection

Operation	Command
Specify number of upper/lower threshold fragment state records	**firewall fragments-inspect** { **high** | **low** } { **default** | *number* }
Restore the default number of upper/lower threshold fragment state records	**undo firewall fragments-inspect** { **high** | **low** }

The default number of upper threshold fragment state records is 2000. The default number of lower threshold fragment state records is 1500.

IV. Applying ACL on the interface

To filter fragments based on layer 3 information or time range, you can configure the router to perform standard matching. To filter fragments based on port information, you must configure the router to perform exact matching; otherwise, the port matching rule does not take effect.

Table 6-6 Apply ACL on the interface

Operation	Command
Specify the rule of filtering transmitting and receiving packets in the interface	**firewall packet-filter** *acl-number* { **inbound** | **outbound** } [**match-fragments** { **normally** | **exactly** }]
Remove the rule of filtering transmitting and receiving packets in the interface	**undo firewall packet-filter** *acl-number* { **inbound** | **outbound** }

The standard matching is used by default.

6.2.5 Displaying and Debugging Packet Filter

After the above configuration, execute **display** command in all views to display the running of the packet filter configuration, and to verify the effect of the configuration.

Execute **debugging** command in user view to debug the packet filter.

Table 6-7 Display and debug firewall

Operation	Command
Display statistics about firewall of the interface	**display firewall-statistics** { **all** | **interface** *type number* | **fragments-inspect** }
Enable firewall packet filtering debugging (in user view)	**debugging firewall** { **all** | **eff** | **icmp** | **packet** { **permitted** | **denied** } | **tcp** | **udp** | **fragments-inspect** | **others** } [**interface** *type number*]
Disable firewall packet filtering debugging (in user view)	**undo debugging firewall** { **all** | **eff** | **icmp** | **packet** { **permitted** | **denied** } | **tcp** | **udp** | **fragments-inspect** | **others** } [**interface** *type number*]

6.2.6 Typical Configuration Examples of Packet Filter

I. Network requirements

The following example of configuring firewall in a company explains firewall configuration.

The company accesses the internet through the interface Serial1/0/0 on a 3Com router. It provides WWW, FTP and Telnet services externally. The internal subnet of the company is 129.38.1.0, the internal FTP server address is 129.38.1.1, internal Telnet server address is 129.38.1.2, internal WWW server address is 129.38.1.3 and company external address is 202.38.160.1. Address translation is configured on the router so that internal PCs could access the Internet and external PCs could access internal server. The following requirements are aimed to be satisfied through configuration firewall:

- Only specific subscribers on external network can access the internal server.
- Only specific hosts on the internal network can access external network.

Suppose the IP address of the specific external subscriber is 202.39.2.3.

II. Network diagram

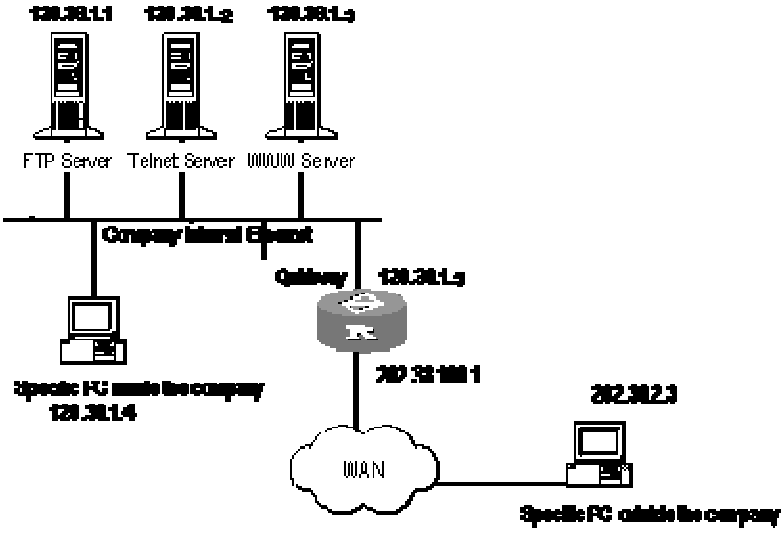


Figure 6-3 Network diagram of packet filter configuration example

III. Configuration procedure

# Enable firewall.

```
[3Com] firewall enable
```

# Set the default firewall filtering mode as permitting packet to pass.

```
[3Com] firewall default permit
```

# Create ACL 3001.

```
[3Com] acl number 3001
```

# Configuration rule permits specific host to access external network and permits internal server to access external network.

```
[3Com-acl-adv-3001] rule permit ip source 129.38.1.4 0
[3Com-acl-adv-3001] rule permit ip source 129.38.1.1 0
[3Com-acl-adv-3001] rule permit ip source 129.38.1.2 0
[3Com-acl-adv-3001] rule permit ip source 129.38.1.3 0
[3Com-acl-adv-3001] rule deny ip
```

# Create ACL 3002.

```
[3Com] acl number 3002
```

# Configuration rule permits specific user to access internal server from external network.

```
[3Com-acl-adv-3002] rule permit tcp source 202.39.2.3 0 destination 202.38.160.1 0
```

# Configuration rule permits specific user to obtain data from external network (only packets with ports bigger than 1024 are permitted.)

```
[3Com-acl-adv-3002] rule permit tcp destination 202.38.160.10 0 destination-port gt 1024
```

# Act the rule 3001 on inbound packet from the interface Ethernet0/0/0.

```
[3Com-Ethernet0/0/0] firewall packet-filter 3001 inbound
```

# Act the rule 3002 on inbound packet from the interface Serial1/0/0.

```
[3Com-Serial1/0/0] firewall packet-filter 3002 inbound
```

6.3 Configuring ASPF

ASPF configuration includes:

- Enable firewall
- Configure ACL
- Define an ASPF policy
- Apply the ASPF policy on specified interfaces

6.3.1 Enabling Firewall

This configuration task is the same as the configuration of packet filter.

6.3.2 Configuring ACL

To protect internal network, access control list should be configured on the router and applied to external interface, permitting the internal hosts access external network and prohibiting external hosts from accessing internal network.

Table 6-8 Configure ACL

Operation	Command
Configure ACL (in ACL view)	**rule deny**
Apply ACL to external interface (in interface view)	**firewall packet-filter** *acl-num* **inbound**

6.3.3 Defining an ASPF Policy

Define an ASPF policy according to the following steps:

- Create an ASPF policy
- Configure aging-time value
- Configure application layer protocol detection
- Configure general TCP or UDP detection

I. Creating an ASPF policy

Perform the following configuration in system view.

Table 6-9 Create an ASPF policy

Operation	Command
Create an ASPF policy and enter its view	**aspf-policy** *aspf-policy-number*
Delete the created ASPF policy	**undo aspf-policy** *aspf-policy-number*

The *aspf-policy-number* argument ranges from 1 to 99.

II. Configuring aging-time value

Perform the following configuration in ASPF policy view.

Table 6-10 Configure aging-time value

Operation	Command
Configure aging-time value	**aging-time** { **syn** | **fin** | **tcp** | **udp** } *seconds*
Restore the default aging-time value	**undo aging-time** { **syn** | **fin** | **tcp** | **udp** }

This task is used to configure waiting timeout value in SYN state and FIN state of TCP, free timeout value of TCP and UDP session entries. The default timeout time of syn, fin, tcp and udp are 30s, 5s, 3600s and 30s respectively.

III. Configuring application layer protocol detection

Perform the following configuration in ASPF policy view.

Table 6-11 Configure application layer protocol detection

Operation	Command
Configure ASPF detection for application layer protocol	**detect** *protocol* [**aging-time** *seconds*]
Delete the configured application protocol detection	**undo detect** *protocol*

The application protocol can be **ftp**, **http**, **h323**, **smtp**, **rtsp**, and the transport layer protocol can be **tcp** or **udp**.

The default timeout time of the application protocol is 3600 seconds. The default TCP timeout time is 3600 seconds and the default UDP timeout time is 30 seconds.

When the *protocol* argument is set to **http**, Java blocking can be configured as follows.

Table 6-12 Configure Java blocking detection

Operation	Command
Configure Java blocking detection	**detect http** [**java-blocking** *acl-number*] [**aging-time** *seconds*]
Delete the configured ASPF detection rule	**undo detect http**

IV. Configuring generic TCP and UDP protocol detection

Perform the following configuration in ASPF policy view.

Table 6-13 Configure general TCP and UDP protocol detection

Operation	Command
Configure general TCP detection	**detect tcp** [**aging-time** *seconds*]
Configure general UDP detection	**detect udp** [**aging-time** *seconds*]
Delete general TCP detection	**undo detect tcp**
Delete general UDP detection	**undo detect udp**

The TCP-based default timeout time is 3600 seconds and the UDP-based timeout time is 30 seconds.

You are recommended to use the application layer detection together with TCP/UDP detection, for a configuration of TCP/UDP detection without application layer protocol might cause packet return failures.

Note:

For Telnet applications, just configure generic TCP detection to implement ASPF function.

6.3.4 Applying ASPF Policy on Specified Interface

The interface stream detection will take effect only after applying the pre-defined ASPF policy on the external interface.

Perform the following configuration in interface view.

Table 6-14 Apply ASPF policy on specified interface

Operation	Command
Configure ASPF detection policy in specified interface	**firewall aspf** *aspf-policy-number* { **inbound** | **outbound** }
Delete the ASPF detection policy applied in the interface	**undo firewall aspf** *aspf-policy-number* { **inbound** | **outbound** }

As ASPF saves and maintains application layer protocol status based on interface, you must ensure that the originating and response packets for a connection are sent out and received on the same interface.

6.3.5 Configuring a Port Mapping Entry

Perform the following configuration in system view.

Table 6-15 Configure PAM

Operation	Command
Configure the generic PAM function.	**port-mapping** *application-name* **port** *port-number*
Delete the user-configured generic PAM.	**undo port-mapping** *application-name* **port** *port-number*
Configure PAM for a host.	**port-mapping** *application-name* **port** *port-number* **acl** *acl-number*

Operation	Command
Delete the user-configured PAM of a host	**undo port-mapping** *application-name* **port** *port-number* **acl** *acl-number*

The range of hosts in the host-specific PAM is specified using a basic ACL.

6.3.6 Displaying and Debugging ASPF

After the above configuration, execute **display** command in all views to display the running of the ASPF configuration, and to verify the effect of the configuration. Execute **debugging** command in user view for the debugging of ASPF.

Table 6-16 Display and debug ASPF

Operation	Command
Display all ASPF configurations	**display aspf all**
Display information about the interfaces where ASPF policies and ACLs are applied	**display aspf interface**
Display the configuration of a specific ASPF policy	**display aspf policy** *aspf-policy-number*
Display sessions currently traced and inspected by ASPF	**display aspf session** [**verbose**]
Display port mapping information.	**display port-mapping** [*application-name* | **port** *port-number*]
Enable ASPF debugging	**debugging aspf** { **all** | **verbose** | **events** | **ftp** | **h323** | **http** | **rtsp** | **session** | **smtp** | **tcp** | **timers** | **udp** }
Disable ASPF debugging	**undo debugging aspf** { **all** | **verbose** | **events** | **ftp** | **h323** | **http** | **rtsp** | **session** | **smtp** | **tcp** | **timers** | **udp** }

6.3.7 ASPF Configuration Example

I. Network requirements

Configure an ASPF policy on the firewall to detect the FTP and HTTP traffic passing the firewall. Requirement: If the packet is a returned packet of FTP and HTTP connections initiated by internal network subscribers, permit it to pass the firewall and enter the internal network. For other packets, deny them. In addition, this detection policy can filter out Java Applets in HTTP packets from the server 2.2.2.11. This example can be applied in the case when local user needs to access remote network service.

II. Network diagram

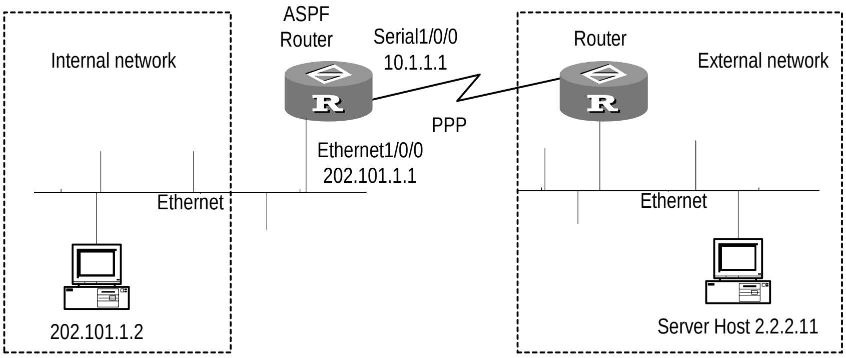


Figure 6-4 Network diagram of ASPF configuration example

III. Configuration procedure

# Enable firewall.

```
[3Com] firewall enable
```

# Configure ACL 3111 to refuse all TCP and UDP traffic to enter internal network. ASPF will create a temporary ACL for traffic that is permitted to pass.

```
[3Com] acl number 3111
[3Com-acl-adv-3111] rule deny ip
```

# Create ASPF policy, with a policy number of 1. The policy detects two protocols on application layer, FTP and FTTP, and defines the timeout time of the two protocols in case of no actions as 3000 seconds.

```
[3Com] aspf-policy 1
[3Com-aspf-policy-1] detect ftp aging-time 3000
[3Com-aspf-policy-1] detect http aging-time 3000
[3Com-aspf-policy-1] detect http java-blocking 2001
```

# Configure ACL 2001 to filter Java Applets from the site 2.2.2.11.

```
[3Com] acl number 2001
[3Com-acl-basic-2001] rule deny source 2.2.2.11 0
[3Com-acl-basic-2001] rule permit
```

# Apply the ASPF policy on the interface.

```
[3Com-Serial1/0/0] firewall aspf 1 outbound
```

# Apply ACL 3111 on the interface.

```
[3Com-Serial1/0/0] firewall packet-filter 3111 inbound
```

Chapter 7 IPSec Configuration

7.1 IPSec Overview

7.1.1 IPSec

IP Security (IPSec) protocol family is a series of protocols defined by IETF. It provides high quality, interoperable and cryptology-based security for IP data packets. The two sides of communication perform encryption and data source authentication on IP layer to assure confidentiality, data integrity, data origin authentication and anti-replay for packets when they are being transmitted on networks.

Note:

Confidentiality is to encrypt a client data and then transmit it in cipher text.

Data integrity is to authenticate the received data so as to determine whether the packet has been modified.

Data origin authentication is to authenticate the data source to make sure that the data is sent from a real sender.

Anti-replay is to prevent some malicious client from repeatedly sending a data packet. In other words, the receiver will deny old or repeated data packets.

IPSec implements the above aims via Authentication Header (AH) security protocol and Encapsulating Security Payload (ESP) security protocol. Moreover, Internet Key Exchange (IKE) provides auto-negotiation key exchange and Security Association (SA) setup and maintenance services for IPSec so as to simplify the use and management of IPSec.

- AH mainly provides data source authentication, data integrity authentication and anti-replay. However, it cannot encrypt the packet.
- ESP provides encryption function besides the above functions that AH provides. However, its data integrity authentication does not include IP header.

Note:

AH and ESP can be used either independently or corporately. There are two types of working modes for AH and ESP: transport mode and tunnel mode, which will be introduced later.

- IKE is to negotiate the cryptographic algorithm applied in AH and ESP and to put the necessary key in the algorithm to the proper place.

Note:

IPSec policy and algorithm can also be negotiated manually. So IKE negotiation is not necessary. The comparison of these two negotiation modes will be introduced later.

7.1.2 IPSec Basic Concepts

I. Security association

IPSec provides security communication between two ends, which are called as IPSec peers.

IPSec allows systems, network subscribers or administrators to control granularity of security services between peers. For instance, IPSec policies of some group prescribe that data flow from some subnet should be protected over AH and ESP and be encrypted over Triple Data Encryption Standard (3DES) simultaneously. Moreover, the policies prescribe that data flow from another site should be protected over ESP only and be encrypted via DES only. IPSec can provide security protection in various levels for different data flows based on SA.

SA is essential to IPSec. It is the standard for some elements of communication peers. For example, it determines which protocol should be applied (AH, ESP or both) as well as the working mode (transport mode or tunnel mode), encryption algorithm (DES and 3DES), shared protecting key in some stream, and SA lifetime.

As SAs are unidirectional, at least two SAs are needed to protect data flow from two directions in a bi-directional communication. Moreover, if both AH and ESP are applied to protect data flow between peers, still two SAs are needed for AH and ESP respectively.

SA is identified by a triplet uniquely, including Security Parameter Index (SPI), destination IP address and security protocol ID (AH or ESP). SPI is a 32-bit number generated for uniquely identifying SA. It is transmitted in AH/ESP header.

SA has duration. It is calculated as follows:

- Time-based duration is to update SA at a specific interval;
- Traffic-based duration is to update SA after certain data (bytes) transmission.

II. Working mode of IPSec protocol

IPSec protocol falls into two working modes: transport mode and tunnel mode. They are specified in SA.

In the transport mode, AH/ESP is inserted after the IP header but before all transmission layer protocols or all other IPSec protocols. In the tunnel mode, AH/ESP is inserted before the original IP header but after the new header. The data encapsulation format for various protocols (taking the transmission protocol TCP as an example) in the transmission/tunnel mode is shown in the following figure:

Mode Protocol	transport	tunnel
AH	IP Header AH TCP Header data	new IP Header AH raw IP Header TCP Header data
ESP	IP Header ESP TCP Header data ESP Tail ESP Auth data	new IP Header ESP raw IP Header TCP Header data ESP Tail ESP Auth data
AH-ESP	IP Header AH ESP TCP Header data ESP Tail ESP Auth data	new IP Header AH ESP raw P Header TCP Header data ESP Tail ESP Auth data

Figure 7-1 Data encapsulation format for security protocols

The tunnel mode is safer than the transport mode. It can authenticate and encrypt original IP data packets completely. Moreover, it can hide the client IP address via the IPSec peer IP address. On the other hand, the tunnel mode occupies more bandwidth than the transport mode because it has an extra IP header. Therefore, you can select a proper mode according to the practical need on security or performance.

III. Authentication algorithm and encryption algorithm

1) Authentication algorithm

Both AH and ESP can authenticate integrity for an IP packet so as to determine whether the packet is modified. The authentication algorithm is implemented via hybrid function. The hybrid function is a kind of algorithm that does not limit the length of inputting messages and outputs messages in a certain length. The output message is called as message summary. IPSec peers calculate the packet via the hybrid function respectively. If they get identical summaries, the packet is integrated and not modified.

Generally speaking, there are two types of IPSec authentication algorithms.

- MD5: Input a message in any length and generate a 128-bit message summary.
- SHA-1: Input a message less than 2^{64}-bit and generate a 160-bit message summary.

Because the SHA-1 summary is longer than that of MD5, SHA-1 is safer than MD5.

2) Encryption algorithm

ESP can encrypt IP packets so that the contents of the packets will not let out during the transmission. Encryption algorithm is implemented by encrypting or decrypting data with identical key via symmetric key system. V 2.41 implements three types of encryption algorithm.

- DES(Data Encryption Standard): Encrypt a 64-bit clear text via a 56-bit key.
- 3DES(Triple DES): Encrypt a clear text via three 56-bit keys (168 bits key).
- AES (Advanced Encryption Standard): 128-bit/192-bit/256-bit AES algorithm can be implemented on V 2.41.

IV. Negotiation mode

There are two negotiation modes to establish SA: manual mode (**manual**) and IKE auto-negotiation mode (**isakmp**). The former is a bit complex because all information about SA has to be configured manually. Moreover, it does not support some advanced features of IPSec, such as key update timer. However, its advantage is that it can implement IPSec independent of IKE. The latter one is much easier because SA can be established and maintained by IKE auto-negotiation as long as security policies of IKE negotiation are configured.

Manual mode is feasible in the case of few peer devices or in a small-sized static environment. For medium/big-sized dynamic environment, IKE auto-negotiation mode is recommended.

7.1.3 Overview of Encryption Card

IPSec may use ESP or AH protocol to process packets. For high security purpose, complicated encryption/decryption/authentication algorithms are often used. The IPSec on a router uses many CPU resources for encryption/decryption algorithm, so the overall performance may be degraded. To solve this problem, you can insert an encryption card for a modularized router, on which IPSec operations are processed by hardware. This can improve IPSec processing efficiency, as well as overall performance of a router.

1) Encryption/decryption process on the encryption card: The router sends data to be encrypted or decrypted to the encryption card. The card runs encryption/decryption operations and add/delete encryption headers to/from data, and then sends the processed data back to the router for forwarding.
2) The encryption card processes data flows: A modularized router can support up to four encryption cards for concurrent data processing. The host software distributes data with different security requirements to the encryption cards, which are specified in the SA proposal, for processing. The same card can process data flows defined with different security policies, but the data flows of a type only can be processed by the same card.
3) For the IPSec SA implemented by the encryption card, if the card is faulty, backup function is enabled on the card and the selected encryption/authentication algorithms for the SA are supported by the IPSec module on V 2.41 platform, IPSec shall be implemented by the IPSec module on V 2.41 platform. But you cannot use one encryption card as the backup to another card.

Note:

The encryption card and the IPSec module of V 2.41 adopt the same data processing mechanism. They differ in the sense that the former implements hardware encryption while the latter implements software encryption. In addition, the encryption card supports fast forwarding but the IPSec module does not.

7.1.4 Introduction to IPSec DPD

IPSec dead peer detection (IPSec DPD) is a function that allows on-demand IKE peer liveliness detection on IPSec/IKE tunnels.

The idea of DPD is that when an IKE peer receives no packets from its peer for a specified period, a DPD query is triggered. The IKE peer sends a query to its peer detecting the liveliness asking for proof of liveliness.

Compared with other keepalive mechanisms available with IPSec, DPD generates less traffic, but allows more prompt detection and quicker tunnel recovery.

You may use DPD in the solution where ISAKMP SAs are established between addresses of a router and VRRP standby group. This allows the established security tunnel to recover automatically and quickly when failover occurs in the VRRP standby group, preventing communication from being interrupted. DPD thus broadens the application scope of IPSec and improves its robustness.

DPD is implemented in compliance with RFC3706 and RFC2408.

I. Concepts

1) DPD data structure

A DPD data structure, or a DPD structure, contains DPD query parameters, such as interval-time timer and time_out timer. A DPD structure can be referenced by multiple IKE peers. Thus, you need not to configure one DPD structure for each interface.

2) Timers

IPSec DPD uses the following two timers to control sending and receipt of DPD packets:

Interval-time: specifies the idle interval for triggering a DPD query. If an IKE peer receives no IPSec packet from its peer when this timer times out, DPD query is triggered.

Time_out: specifies the time waiting for a DPD acknowledgement.

II. Operating Mechanism

The following describes how DPD operates after being enabled:

- At the sender side

An IKE peer does not receive IPSec packets from its peer when interval-time timer expires and now, it wants to send IPSec packets to its peer. Before that, the IKE peer sends a DPD query to its peer for proof of liveliness. At the same time, a time_out timer is started. If no acknowledgement is received upon expiration of this timer, DPD records one failure event. When the number of failure events reaches three, the involved ISAKMP SAs and IPSec SAs are deleted.

The same applies to the IPSec SAs set up between a router and the virtual address of a VRRP standby group: when the failure count reaches three, the security tunnel between them is deleted. The setup of this security tunnel is triggered only when a packet matching the IPSec policy is present.

The failover duration depends on the setting of time_out timer. A shorter timer setting means a shorter communication interruption period but increased overheads.

You are recommended to use the default setting in normal cases.

- At the responder end

The peer of the sender sends an acknowledgement after receiving the query.

7.1.5 Introduction to IPSec Mutli-Instance

Currently, IPSec provides the multi-instance function on the VPN-instance associated interfaces between PEs and CEs. That is, a PE is connected to different CEs using different interfaces, so that the CEs of different VPNs can establish IPSec tunnels with the PE respectively. This makes the networking more flexible.

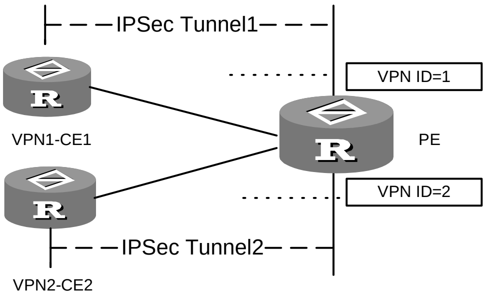


Figure 7-2 Network diagram for IPSec multi-instance

Packets are processed as follows:

- When the PE needs to forward an IP packet to a CE, it first identifies the VPN the packet belongs to according to the VPN ID in the packet. Then, it looks up the corresponding VPN routing table and according to the matched entry, forwards the packet to the outbound interface. If the outbound interface is configured with the **ipsec policy** command and this packet matches the ACL, this packet is encrypted and sent to the CE.
- When the PE receives the IPSec packet, it decrypts the packet first (this step is skipped for non-IPSec packets). The PE identifies the VPN the packet belongs to

according to the VPN ID in the packet. Then, it looks up the corresponding VPN routing table and according to the matched entry to identify whether the destination of this packet is a local host or not. If the packet is intended for the local host, it is forwarded to the IP layer or a CE that belongs to the same VPN. If the packet is not intended for the local host, it is labeled according to the matched entry in the VPN routing table.

7.1.6 IPSec on V 2.41

V 2.41 implements the said aspects of IPSec.

Via IPSec, peers (here refer to the router where V 2.41 locates as well as its peer) can perform various security protections (authentication, encryption or both) on different data flows, which are differentiated based on ACL. Security protection elements, such as security protocol, authentication algorithm, encryption algorithm and operation mode, are defined in IPSec proposal. The association between data flows and IPSec proposal (namely, apply a certain protection on a certain data flow) together with SA negotiation mode, peer IP address configuration (i.e., the start/end of protection path), the required key as well as the duration of SA are defined in IPSec policies. Finally, IPSec policies are applied on router interfaces. This is the process of IPSec configuration.

Following is the detailed description:

1) Defining data flows to be protected

A data flow is an aggregation of a series of traffics, regulated by source address/mask, destination address/mask, number of protocol over IP, source port number and destination port number. An ACL rule defines a data flow, that is, traffic that matches an ACL rule is a data flow logically. A data flow can be a single TCP connection between two hosts or all traffics between two subnets. IPSec can apply different security protections on different data flows. So the first step of IPSec configuration is to define data flows.

2) Defining IPSec proposal

IPSec proposal prescribes security protocol, authentication algorithm and encryption algorithm as well as operation mode (namely, the packet encapsulation mode) for data flows to be protected.

AH and ESP supported by V 2.41 can be used either independently or corporately. AH supports MD5 and SHA-1 authentication algorithms. ESP supports MD5 and SHA-1 authentication algorithms as well as DES, 3DES, and AES encryption algorithms. Working mode supported by V 2.41 includes transport mode and tunnel mode.

As for a data flow, peers should be configured with identical protocol, algorithm and working mode. Moreover, if IPSec is applied on two security gateways (such as between V 2.41 routers), the tunnel mode is recommended so as to hide the real source and destination addresses.

Therefore, you should define an IPSec proposal based on requirements so that you can associate it with data flows.

3) Defining IPSec policy or IPSec policy group

IPSec policy specifies a certain IPSec proposal for a certain data flow. An IPSec policy is defined by “name” and “sequence number” uniquely. It falls into two types, manual IPSec policy and IKE negotiation IPSec policy. The former one is to configure parameters such as key, and SPI as well as IP addresses of two ends in the tunnel mode manually. As for the latter one, these parameters are automatically generated by IKE negotiation.

An IPSec policy group is an aggregation of IPSec policies with identical name but different sequence numbers. In an IPSec policy group, the smaller the sequence number is, the higher the priority is.

4) Applying IPSec policies on an interface

Apply all IPSec policies in a group on an interface so as to perform different security protections on different data flows passing the interface.

7.2 IPSec Configuration

I. Configuring IPSec

1) Configure ACL
2) Configure a security proposal

- Create a security proposal (IPSec proposal or card SA proposal)
- Specify the encryption card used in the card SA proposal (only applies to encryption cards)
- Select security protocol
- Select security algorithm
- Select packet encapsulation mode

3) Create security policy (manually or by using IKE)

For manual mode:

- Create security policy
- Import security proposal into security policy
- Import ACL into security policy
- Configure starting and end points for tunnel
- Configure SPI for SA
- Configure SA keys

For IKE mode:

- Create security policy using IKE
- Import card SA proposal into security policy
- Import ACL into security policy
- Import IKE peer into security policy

- Configure SA duration (optional)
- Configure PFS feature for negotiation

A security policy can reference an IPSec proposal or card SA proposal as needed.

4) Configure security policy template (optional)
5) Apply security policy on the interface
6) Disable next-payload field checking (optional)

II. Configuring the encryption card (optional)

1) Enable encryption card
2) Enable the IPSec module to back up the encryption card
3) Configure the fast forwarding function of the encryption card
4) Configure the simple network management operations for the encryption card

7.2.1 Defining ACL

IPSec uses advanced ACLs to discriminate which packets needs protection and which do not. The role of ACL in IPSec is different from what introduced in firewalls. Normally, ACL is used for determining which data can be permitted and which must be denied on which interface. ACL in IPSec, however, is used by IPSec to determine which packet needs security protection and which does not. For this reason, ACL applied in IPSec is in fact encryption ACL. Packets permitted by ACL will be in protection, while packets denied by ACL will not be protected. An encryption ACL can apply on both input interfaces and output interfaces.

For more information about that, see section 1.4.3 II. “ACL.”

Encryption ACLs defined at the local and peer routers must be in consistency (i.e., they can mirror each other), thus allowing either side to decrypt the data encrypted at the other side. For example,

Local end:

acl number 3101

rule 1 permit ip source 173.1.1.1 0.255.255.255 destination 173.2.2.2 0.255.255.255

Peer end:

acl number 3101

rule 1 permit ip source 173.2.2.2 0.255.255.255 destination 173.1.1.1 0.255.255.255

Note:

- IPSec protects the data flow permitted in the ACL, therefore, the users are recommended to configure the ACL accurately, that is, configure permit only to the data flow needing IPSec protection so as to avoid the excessive use of the key word **any**.
- Configure the ACLs of local and peer ends as the mirror of each other to avoid decryption failures.
- When you set up an IPSec tunnel only through IKE, the initiator of the tunnel performs two ACL match operations while the receiver performs only one ACL match operation. They set up an IPSec tunnel after the IKE negotiation completes. At the initiator side, ACL matches may increase as the match operation is done on each packet. At the receiver side, however, packets are matched with the IPSec tunnel and therefore the number of acl matches does not change.
- For releases of V 2.41 and releases of V 2.411.7, different traffic matching approaches are adopted when implementing IPSec:

For V 2.411.7, V 2.41 Release 0010 and its earlier releases, only one IPSec SA pair is set up for all rules in an ACL. The **display ipsec tunnel** command is not supported.

For releases later than V 2.41 Release 0010, an IPSec SA pair and an IPSec tunnel are set up for each rule on an ACL.

To set up IPSec SAs between two routers installed with software versions using different traffic matching approaches, you must configure multiple ACLs on both of them, each including only one rule.

Executing the **display acl all** command will display all the ACLs, including all the extended IP ACLs regardless whether they are for communications filtering or for encryption. Simply speaking, the system does not discriminate the extended ACLs for these two purposes in the output information of this command.

7.2.2 Defining an IPSec Proposal

An IPSec proposal saves the particular security protocol and the encryption/authentication algorithms applied in IPSec, intending for providing security parameters for IPSec to make SA negotiation. To ensure the success of a negotiation, the two ends involved in the negotiation must use the same IPSec proposal.

Perform the following tasks to configure a security proposal.

- Create an IPSec or card SA proposal
- Specify the encryption card in the card SA proposal (only applied when an encryption card is involved)
- Select a security protocol
- Select a security algorithms
- Set the mode adopted by the security protocol in IP datagram encapsulation

I. Creating an IPSec or card SA proposal

An IPSec proposal is a set of security protocol, algorithms and packet encapsulation format used to implement IPSec protection. An IPSec policy can determine the adopted security protocol, algorithms, and encapsulation mode by referencing one or more IPSec proposals. Before an IPSec proposal is referenced by IPSec policy, this IPSec proposal must be established. Up to 50 IPSec proposals can be configured.

You are allowed to modify an IPSec proposal, but such modifications cannot take effect at all if the modified proposal is applied to an SA that has been setup between the two sides after negotiation – unless you execute the **reset ipsec sa** (or **reset encrypt-card sa**) command to reset the SA. New security proposals can only apply to new SAs.

Perform the following configuration in system view.

Table 7-1 Configure an IPSec proposal

Operation	Command
Create an IPSec proposal and access the IPSec proposal view (for IPSec module)	**ipsec proposal** *proposal-name*
Delete the IPSec proposal (for IPSec module)	**undo ipsec proposal** *proposal-name*
Create a card SA proposal and access its view (for encryption cards only)	**ipsec card-proposal** *proposal-name*
Delete the card SA proposal (for encryption card)	**undo ipsec card-proposal** *proposal-name*

By default, no card SA proposal is configured.

II. Specifying the encryption card to be used by a security proposal

When an encryption card is used, you must specify its slot number in card SA proposal view. Each modular router can accommodate up to four encryption cards; each can be assigned to multiple encryption card security proposals.

Perform the following configuration in card SA proposal view.

Table 7-2 Assign an encryption card to the card SA proposal

Operation	Command
Assign an encryption card to the card SA proposal	**use encrypt-card** [*slot-id*]
Remove the configuration	**undo use encrypt-card** [*slot-id*]

By default, no encryption card is used in the card SA proposal.

III. Selecting packet encapsulation mode

You MUST specify encapsulation mode in a security proposal. In addition, the same encapsulation mode MUST be adopted at the two ends of a security tunnel.

Perform the following configurations in IPSec proposal or card SA proposal view.

Table 7-3 Select a packet encapsulation mode

Operation	Command
Set the IP datagram encapsulation mode adopted by the security protocol.	**encapsulation-mode** { **transport** | **tunnel** }
Restore the default encapsulation mode.	**undo encapsulation-mode**

Normally, tunnel mode is always adopted between two security GWs (routers). Transport mode is always preferred, however, with respect to the communication between two hosts or between a host and a security GW (for example, in the network management communication between a GW workstation and a router, the security GW is the receiving host relative to the GW data).

By default, tunnel mode is adopted.

IV. Selecting security protocol

The security protocol needs specifying in the IPSec proposal and by far AH and ESP are the only two options. You are allowed to use AH, ESP, or both, but the choice must be the same as that at the remote end of the security tunnel.

Perform the following configuration in the IPSec proposal or card SA proposal view.

Table 7-4 Select security protocol

Operation	Command
Configure security protocol used by IPSec proposal	**transform** { **ah** | **ah-esp** | **esp** }
Restore default security protocol	**undo transform**

By default, **esp** (defined by RFC 2406) applies.

V. Selecting security algorithm

Different security protocols may use different authentication and encryption algorithms. Currently AH supports the MD5 and SHA-1 authentication algorithms, while ESP supports the MD5 and SHA-1 authentication algorithms and the DES, 3DES and AES encryption algorithms.

Perform the following configuration in the IPSec proposal or card SA proposal view.

Table 7-5 Select security algorithm

Operation	Command
Configure encryption algorithm used by ESP	**esp encryption-algorithm** { **3des | des | aes** [**128 | 192 | 256**] }
Configure undo packet encrypting for ESP	**undo esp encryption-algorithm**
Configure authentication method used by ESP	**esp authentication-algorithm** { **md5 | sha1** }
Configure undo packet authentication for ESP	**undo esp authentication-algorithm**
Configure authentication method used by AH protocol	**ah authentication-algorithm** { **md5 | sha1** }
Restore AH protocol default authentication method	**undo ah authentication-algorithm**

ESP will allow encryption and authentication process for packet at the same time, or encryption only or process authentication only. Attention, **undo esp authentication-algorithm** command will not restore authentication method to the default, but configure authentication method as null, i.e., undo authentication-method. When encryption algorithm is null, **undo esp authentication-algorithm** command is invalid. AH protocol has no encrypting function and can only perform authentication for packets. **undo ah authentication-algorithm** command is used to restore AH protocol default authentication method as **md5**. On both ends of security tunnel, the IPSec proposals referenced by IPSec policy must be configured with the same authentication method and encryption algorithm.

ESP protocol supports three types of encryption algorithms: **des**, **3des** and **aes**, and two authentication algorithms: **hmac-md5** and **hmac-sha1**.

AH protocol supports two types of authentication algorithms: **hmac-md5** and **hmac-sha1**.

By default, encryption algorithm used by ESP is **des** and authentication method used is **md5**. Authentication method used by AH protocol is **md5**.

🕮 **Note:**

Only when the desired security protocol is selected with the **transform** command, can security algorithm be configured. For example, if you can select ESP, you can only configure those security algorithms particular to ESP, excluding those for AH.

7.2.3 Creating IPSec Policies

IPSec policies each specify an IPSec proposal for a certain data flow. They fall into two types, manual IPSec policy and IKE negotiation IPSec policy. The former one is to configure parameters such as key, SPI and SA duration as well as IP addresses of two ends in the tunnel mode manually. As for the latter one, these parameters are automatically generated by IKE negotiation.

🕮 **Note:**

This section introduces configurations about IPSec policy in detail, including manual configuration and IKE negotiation configuration. Configuration for one mode will be followed by a special description. Otherwise, the configuration should be performed in both manual mode and IKE negotiation mode.

I. Manually creating an IPSec policy

1) Manually creating an IPSec policy

You are not allowed to modify the negotiation mode of an IPSec policy that has been created. For example: If **manual** IPSec policy is established, it cannot be revised into **isakmp** mode, and you have to delete this IPSec policy before establishing a new one.

Perform the following configuration in system view.

Table 7-6 Establish IPSec policy

Operation	Command
Manually create an IPSec policy for an SA.	**ipsec policy** *policy-name seq-number* **manual**
Modify the IPSec policy of the SA.	**ipsec policy** *policy-name seq-number* **manual**
Delete the IPSec policy	**undo ipsec policy** *policy-name* [*seq-number*]

IPSec policies with the same name and different sequence numbers can compose an IPSec policy group. In one IPSec policy group, up to 100 IPSec policies can be configured. However, the maximum number of all IPSec policies in all IPSec policy groups is 100. In an IPSec policy group, the smaller the sequence number is, the higher the priority will be.

By default, there is no IPSec policy.

2) Referencing IPSec proposal in IPSec policy

IPSec policy will specify security protocol algorithm and packet encapsulation format by referencing IPSec proposal. Before an IPSec proposal is referenced, this IPSec proposal must be configured.

Perform the following configuration in system view.

Table 7-7 Use IPSec proposal in IPSec policy

Operation	Command
Configure IPSec proposal referenced by IPSec policy	**proposal** *proposal-name1* [*proposal-name2...proposal-name6*]
Remove IPSec proposal referenced by IPSec policy	**undo proposal** [*proposal-name*]

The Security Association can be established through **manual** mode. One IPSec policy can reference only one IPSec proposal. If IPSec proposal has been configured, the former IPSec proposal must be removed so as to configure new IPSec proposal. On both ends of security tunnel, IPSec proposals referenced by the IPSec policy must be configured by using the same security protocol, algorithm and packet encapsulation mode.

3) Configuring ACL referenced by IPSec policy

IPSec policy will reference ACL. IPSec will specify which packet needs security protection and which does not according to the rules in this ACL. Packets permitted by ACL will be in protection, while packets denied by ACL will not be protected.

Perform the following configuration in IPSec policy view.

Table 7-8 Configure access control list referenced by IPSec policy

Operation	Command
Configure access control list referenced by IPSec policy	**security acl** *acl-number*
Remove access control list referenced by IPSec policy	**undo security acl**

One IPSec policy can reference only one ACL. If the IPSec policy has referenced more than one ACL, only the last one takes effect. In this ACL, only one rule takes effect to protect packets matching the ACL first. For subsequent packets matching other rules, no protection is provided.

4) Configuring tunnel start/end point

Generally, tunnels applying IPSec policies are called “security tunnels”. A security tunnel is set up between the local and the peer GWs. To ensure the success in security tunnel setup, you must configure correct local and peer addresses.

Perform the following configuration in IPSec policy view.

Table 7-9 Configure tunnel start/end point

Operation	Command
Configure local address in the IPSec policy	**tunnel local** *ip-address*
Delete the local address configured in the IPSec policy	**undo tunnel local** *ip-address*
Configure peer address in the IPSec policy.	**tunnel remote** *ip-address*
Delete the peer address configured in the IPSec policy.	**undo tunnel remote** *ip-address*

With respect to an IPSec policy set up manually, only if both local and peer addresses are correctly configured, can a security tunnel be set up. As ISAKMP SA can automatically obtain local and peer addresses, it does not require the configuration of local or peer address.

5) Configuring SA SPI

This configuration task only applies to a manually created IPSec policy. Use the following command to configure SA SPI for manually creating an SA. An **isakmp**-mode IPSec policy does not need manual configuration and IKE will automatically negotiate SPI and create SA.

Perform the following configuration in IPSec policy view.

Table 7-10 Configure an SA SPI

Operation	Command
Configure an SA SPI.	**sa spi** { **inbound** | **outbound** } { **ah** | **esp** } *spi-number*
Delete the SA SPI.	**undo sa spi** { **inbound** | **outbound** } { **ah** | **esp** }

When configuring an SA for the system, you must set the parameters in the **inbound** and **outbound** directions separately.

The SA parameters set at both ends of the security tunnel must be fully matched. The SPI and key in the inbound SA at the local must be the same as those in the outbound SA at the remote. Likewise, the SA SPI and key in the outbound SA at the local must be the same as those in the inbound SA at the remote.

6) Configuring key for SA

This configuration is used only for **manua**l mode IPSec policy. Security association key can be input manually by using the following commands. (For **isakmp** negotiation IPSec policy, manual configuration for key is not required. IKE will automatically negotiate security association key.)

Perform the following configuration in IPSec policy view.

Table 7-11 Configure key used by security association

Operation	Command
Configure AH protocol authentication key (input in hex form)	**sa authentication-hex** { **inbound** | **outbound** } { **ah** | **esp** } *hex-key*
Configure protocol authentication key (input in character string)	**sa string-key** { **inbound** | **outbound** } { **ah** | **esp** } *string-key*
Configure ESP encryption key (input in hex form)	**sa encryption-hex** { **inbound** | **outbound** } **esp** *hex-key*

Delete configured security association parameter	**undo sa string-key** { **inbound** | **outbound** } { **ah** | **esp** }
	undo sa authentication-hex { **inbound** | **outbound** } { **ah** | **esp** }
	undo encryption-hex { **inbound** | **outbound** } **esp**

On both ends of security tunnel, configured Security Association parameters must be consistent. Security association SPI and shared secret input on local end must be the same as peer output Security Association SPI and shared secret. Security association SPI and shared secret output on local end must the same as those input on peer end.

For the character string key and hex string key, the last configured one will be adopted. On both ends of security tunnel, shared secret should be input in the same form. If shared secret is input in character string on one end and in hex on the other end, the security tunnel cannot be correctly established.

II. Creating an IPSec Policy by using IKE

Following are the configuration tasks for creating an IPSec policy by using IKE.

- Create IPSec policy by using IKE
- Reference an IPSec proposal in the IPSec policy
- Configure ACL referenced by the IPSec policy
- Reference an IKE peer in the IPSec policy
- Configure the lifetime of an SA (optional)
- Configure the PFS feature in negotiation (optional)

1) Creating an IPSec policy by using IKE

Perform the following configurations in system view.

Table 7-12 Create an IPSec policy

Operation	Command
Create an IPSec policy by using IKE and access the IPSec policy view.	**ipsec policy** *policy-name seq-number* **isakmp**

Operation	Command
Dynamically create an IPSec policy by using IKE and an IPSec policy template.	**ipsec policy** *policy-name seq-number* **isakmp** [**template** *template-name*]
Modify an IPSec policy that has been established by using IKE negotiation	**ipsec policy** *policy-name seq-number* **isakmp**
Delete the specified IPSec policy.	**undo ipsec policy** policy-name [*seq-number*]

If you want to create a dynamic IPSec policy by making use of an IPSec policy template, you must first define the policy template. For more information about defining a policy template, see "Section 7.2.4 Configuring IPSec Policy Template".

2) Referencing an IPSec proposal in the IPSec policy

An IPSec proposal is referenced in an IPSec policy to specify IPSec protocol, algorithms, and packet encapsulation mode. Before an IPSec proposal can be referenced, it must have been created.

Perform the following configurations in IPSec policy view.

Table 7-13 Reference an IPSec proposal in the IPSec policy

Operation	Command
Reference an IPSec proposal in the IPSec policy.	**proposal** *proposal-name1* [*proposal-name2... proposal-name6*]
Remove the IPSec proposal referenced by the IPSec policy.	**undo proposal**

In the event of manually creating SA, each IPSec policy can reference only one IPSec proposal. If an IPSec proposal has been referenced, it must be removed before the configuration of a new IPSec proposal is allowed. At both ends of a security tunnel, IPSec proposals referenced by the IPSec policy must adopt the same security protocol, algorithms and packet encapsulation mode.

3) Referencing ACL in the IPSec policy

IPSec policy will reference an ACL to specify which packet needs security protection and which does not according to the rules in this access control list. Packets permitted by ACL will be in protection, while packets denied by ACL will not be protected.

Perform the following configuration in IPSec policy view.

Table 7-14 Reference ACL in the IPSec policy

Operation	Command
Reference an ACL in the IPSec policy	**security acl** *acl-number*
Remove the ACL referenced by the IPSec policy	**undo security acl**

One IPSec policy can reference only one access control list. If the IPSec policy has referenced more than one ACLs, only the one configured last is valid.

In the event of setting up an SA by making use of IKE (**isakmp**) negotiation, each IPSec policy can reference up to six IPSec proposals. When making an IKE negotiation, the systems at the two ends of the security tunnel will look up the configured IPSec proposals for a match. If no match is found, the setup attempt of SA will fail and the packets requiring protection will be dropped.

4) Referencing an IKE peer in the IPSec policy

In IKE negotiation mode, these parameters such as peer, SPI and key can be obtained through negotiation, so you only need to associate IPSec policy with IKE peer.

Perform the following configurations in IPSec policy view.

Table 7-15 Reference an ACL in the IPSec policy

Operation	Command
Reference an IKE peer in the IPSec policy.	**ike peer** *peer-name*
Remove the referenced IKE peer from the IPSec policy.	**undo ike peer** *peer-name*

Note:

This section only discusses importing IKE peer for IPSec, but in practice other parameters also need to be configured in IKE Peer view, including IKE negotiation mode, ID type, NAT traversal, shared key, peer IP address, peer name etc. Refer to the next chapter for such details.

5) Configuring SA duration (lifetime) (optional)

a. Configuring global SA lifetime

All the SAs that have not been configured separately with a lifetime in IPSec policy view adopt the global lifetime. In the SA negotiation via IKE, the lifetime configured at the local or at the peer will be adopted, whichever is smaller.

There are two types of lifetime: “time-based" lifetime and “traffic-based” lifetime. The expiration of either type of lifetime will render an SA useless. Before it goes invalid, IKE will negotiate to set up a new SA for IPSec. Thus, when the old SA becomes fully invalid, a new one is available.

Perform the following configurations in system view.

Table 7-16 Configure a global SA lifetime

Operation	Command
Configure a global SA lifetime.	**ipsec sa global-duration** { **traffic-based** *kilobytes* **|** **time-based** *seconds* }
Restore the default global SA lifetime.	**undo ipsec sa global-duration** { **traffic-based** **|** **time-based** }

Changing the configured global lifetime does not affect the IPSec policies that have separate lifetimes or the SAs that have been set up. The changed global lifetime will apply to the IKE negotiation initiated later.

Lifetime is not significant to manually established SAs but **isakmp** mode SAs. In other words, a manually established SA will maintain permanently.

b. Configuring SA lifetime in IPSec policy view

You can configure a separate SA lifetime for an IPSec policy. If such a lifetime is not available, the global SA lifetime will apply.

In the SA negotiation via IKE, the lifetime configured at the local or at the peer will be adopted, whichever is smaller.

Perform the following configurations in IPSec policy view.

Table 7-17 Configure an SA lifetime

Operation	Command
Configure an SA lifetime for the IPSec policy.	**sa duration** { **traffic-based** *kilobytes* **|** **time-based** *seconds* }
Adopt the configured global SA lifetime.	**undo sa duration** { **traffic-based** **|** **time-based** }

Changing the configured global lifetime does not affect the SAs that have been set up. The changed global lifetime will apply to the IKE negotiation initiated later.

6) Configuring the PFS feature in negotiation (optional)

Perfect Forward Secrecy (PFS) is a security feature. With it, keys are not derivative, so the compromise of a key will not threaten the security of other keys. This feature is implemented by adding the process of key exchange in the stage-2 negotiation of IKE. Perform the following configuration in IPSec policy view.

Table 7-18 Set the PFS feature used in negotiation

Operation	Command
Configure the PFS feature used in negotiation.	**pfs** { **dh-group1** | **dh-group2** | **dh-group5** | **dh-group14** }
Disable PFS in negotiation.	**undo pfs**

When IKE initiates a negotiation by using an IPSec policy configured with the PFS feature, it will make a key exchange operation. In the event that the local adopts PFS, the peer must also adopt PFS. The local and the peer must specify the same Diffie-Hellman (DH) group; otherwise, the negotiation between them will fail.

1024-bit DH group (**group2**) provides a security level higher than 768-bit DH group (**group1**), but it needs longer time for calculation.

The four keywords, **group1**, **group2**, **group5**, and **group14**, each can provide a higher security level than the former does but at the price of calculation time.

By default, no PFS feature is configured.

7.2.4 Configuring IPSec Policy Template

In the IKE approach, you may create a security policy by referencing an IPSec policy template as an alternative to directly configuring one in IPSec policy view. Before doing that, you need to configure a set of security polies in the template.

The configuration of IPSec policy template is similar to common IPSec policy: first, you need create a policy template; then, template parameters can be specified.

Perform the following configuration in system view.

Table 7-19 Configure IPSec policy template

Operation	Command
Create/Modify IPSec policy template	**ipsec policy-template** *template-name seq-number*
Delete an IPSec policy template	**undo ipsec policy-template** *template-name* [*seq-number*]

Using IPSec policy-template command, you will enter the IPSec policy template view, in which you can specify the policy template related parameters.

🕮 **Note:**

The parameters configurable in an IPSec policy template are the same as those of IPSec policy, but most are optional. Only IPSec proposal is mandatory. However, it should be noted that the proposal parameters are required while other parameters are optional. In IKE negotiation, if IPSec policy template is used for policy matching, the configured parameters must be matched and the parameters not configured use those of the initiation side.

After the configuration of policy template, the following command must be executed to apply the policy template just defined.

Table 7-20 Reference IPSec policy template

Operation	Command
Reference an IPSec policy template	**ipsec policy** *policy-name seq-number* **template** *template-name*

The view of the IPSec policy that has referenced IPSec policy template does not support policy configuration and modification, which can only be implemented in IPSec policy template view.

⚠ **Caution:**

- The policy of IPSec policy template cannot initiate the negotiation of security association, but is can response a negotiation.
- The number of an IPSec policy configured by referencing an IPSec policy template must be greater than that of an IPSec policy not configured in that way. Otherwise, the responding party cannot find a match and the negotiation fails.

7.2.5 Applying IPSec Policy Group to Interface

In order to validate a defined SA, you must apply an IPSec policy group at the interface (logical or physical) where the outgoing data or incoming data needs encryption or decryption. Data encryption on the interface will be made based on the IPSec policy group and in conjunction with the peer router. Deleting the IPSec policy group from the interface will disable the protection function of IPSec on the interface.

Perform the following configuration in the interface view.

Table 7-21 Use IPSec policy group

Operation	Command
Use the IPSec policy group	**ipsec policy** *policy-name*
Remove the IPSec policy group in use	**undo ipsec policy** [*policy-name*]

An interface can only use one IPSec policy group. Only ISAKMP IPSec policy group can be used on more than one interface. A manually configured IPSec policy group can only be used on one interface.

When packet transmitted from an interface, each IPSec policy in the IPSec policy group will be searched according to sequence numbers in ascending order. If an access control list referenced by the IPSec policy permits a packet, the packet will be processed by this IPSec policy. If the packet is not permitted, keep on searching the next IPSec policy. If the packet is not permitted by any access control list referenced by the IPSec policy, it will be directly transmitted (IPSec does not protect the packet).

Huawei's IPSec policy implementation can not only apply on practical physical ports such as serial ports and Ethernet ports, but also on virtual interfaces such as Tunnel and Virtual Template. In this way, IPSec can be applied on tunnels like GRE and L2TP according to the practical networking requirement.

7.2.6 Disabling Next-Payload Field Checking

An IKE negotiation packet comprises multiple payloads; the next-payload field is in the generic header of the last payload. According to the protocol, this field should be set to 0. It however may vary by vendor. For compatibility sake, you can use the **ike next-payload check disabled** command to ignore this field during IPSec negotiation.

Table 7-22 Disable the router to check the next-payload field

Operation	Command
Disable the router to check the next-payload field in the last payload of the IKE negotiation packet during IPSec negotiation	**ike next-payload check disabled**
Remove the default	**undo ike next-payload check disabled**

By default, the router checks the next-payload field in the last payload of the IKE negotiation packet during IPSec negotiation.

7.2.7 Configuring the Encryption Card (Optional)

The basic configurations of an encryption card are the same as those of IPSec; refer to the previous sections.

The following are the optional configurations for the encryption card.

I. Entering encryption card interface view and enabling the card

When a router is fitted with multiple encryption cards, you may use the **undo shutdown** and **shutdown** commands to enable or disable them. The **undo shutdown** command can reset and initialize an encryption card that is disabled.

Before you can shut down/enable the encryption card in a specified slot, you must use the **interface encrypt** command to enter the view of the encryption card.

Perform the following configuration in system view.

Table 7-23 Enter encryption card interface view

Operation	Command
Enter encryption card interface view	**interface encrypt** [*slot-id*]

Perform the following configuration in system view.

Table 7-24 Enable or shut down the encryption card

Operation	Command
Turn up the encryption card	**undo shutdown**
Shut down the encryption card	**shutdown**

By default, all the fitted encryption cards are up.

II. Enabling IPSec module backup function

For the IPSec SA implemented by the encryption card, if the card is normal, IPSec is processed by the card. If the card fails, backup function is enabled on the card and the selected encryption/authentication algorithms for the SA are supported by the IPSec module on V 2.41 platform, IPSec shall be implemented by the IPSec module on V 2.41 platform. In the event that the selected algorithms are not supported by the IPSec module, the system drops packets.

Perform the following configuration in system view.

Table 7-25 Configure IPSec module backup function

Operation	Command
Enable IPSec module backup function	**encrypt-card backuped**

Operation	Command
Disable IPSec module backup function	**undo encrypt-card backuped**

By default, IPSec module backup function is disabled.

III. Configuring the fast forwarding function of the encryption card

For the packets that have the same [SourIP, SourPort, DestIP, DestPort, Prot] quintuple, the router creates a fast forwarding entry when it receives the first packet. Then, the subsequent packets, rather than processed packet by packet, are sent directly to the encryption card, where they are sent to the destination after being encrypted or decrypted. This is how the fast forwarding function of the encryption card expedites packet processing.

Perform the following configuration in system view.

Table 7-26 Configure the fast forwarding function of the encryption card

Operation	Command
Enable the fast forwarding function of the encryption card	**encrypt-card fast-switch**
Disable the fast forwarding function of the encryption card	**undo encrypt-card fast-switch**

By default, the fast forwarding function of the encryption card is disabled.

IV. Setting Simple network management configuration on encryption cards

You can manage the encryption cards on the router remotely by using SNMP. With the NM function on the router, you can query the card status and monitor trap information, which includes information about card rebooting, status transition and packet loss processing.

Perform the following configuration in system view.

Table 7-27 Configure trap function on Encryption card

Operation	Command
Enable trap function on Encryption card	**snmp-agent trap enable encrypt-card**
Disable trap function on Encryption card	**undo snmp-agent trap enable encrypt-card**

By default, the trap function is not enabled on the encryption card.

7.2.8 Configuring IPSec DPD

I. Creating a DPD structure

Perform the following configuration in system view.

Table 7-28 Create a DPD structure and enter its view

Operation	Command
Create a DPD structure and enter its view	**ike dpd** *dpd-name*
Delete the specified DPD structure	**undo ike dpd** *dpd-name*

If a DPD structure has been referenced by an IKE peer, it cannot be deleted.

II. Configuring timers

Perform the following configuration in DPD structure view.

Table 7-29 Configure timers

Operation	Command
Configure the interval for triggering a DPD query	**interval-time** *seconds*
Restore the default interval for triggering a DPD query	**undo interval-time**
Configure the time waiting for a DPD acknowledgment	**time-out** *seconds*
Restore the default time waiting for a DPD acknowledgment	**undo time-out**

By default, the interval for triggering a DPD query is 10 seconds, and the time waiting for a DPD acknowledgment is five seconds.

III. Specifying a DPD structure for an IKE peer

Perform the following configuration in IKE peer view.

Table 7-30 Specify a DPD structure for an IKE peer

Operation	Command
Specify a DPD structure for the IKE peer	**dpd** *dpd-name*
Remove the referenced DPD structure	**undo dpd**

7.3 Displaying and Debugging IPSec

7.3.1 Displaying and Debugging over IPSec Module on V 2.41 Platform

I. Displaying and debugging IPSec configuration

After the above configuration, execute **display** command in any view to display the running of the IPSec configuration, and to verify the effect of the configuration.

Execute **debugging** command in user view for the debugging of IPSec configuration.

Table 7-31 Display and debug IPSec

Operation	Command
Display Security Association related information	**display ipsec sa** [**brief** | **remote** *ip-address* | **policy** *policy-name* [*seq-number*] | **duration**]
Display statistical information on IPSec processed packet	**display ipsec statistics**
Display IPSec proposal	**display ipsec proposal** [*proposal-name*]
Display IPSec policy	**display ipsec policy** [**brief** | **name** *policy-name* [*seq-number*]]
Display IPSec policy template	**display ipsec policy-template** [**brief** | **name** *policy-name* [*seq-number*]]
Display information about the specified or all DPD structures	**display ike dpd** [*dpd-name*]
Enable IPSec debugging function	**debugging ipsec** { **all** | **sa** | **packet** [**policy** *policy-name* [*seq-number*] | **parameters** *ip-address protocol spi-number*] | **misc** }
Disable IPSec debugging function	**undo debugging ipsec** { **all** | **sa** | **packet** [**policy** *policy-name* [*seq-number*] | **parameters** *ip-address protocol spi-number*] | **misc** }
Enable IKE DPD debugging	**debugging ike dpd**
Disable IKE DPD debugging	**undo debugging ike dpd**

II. Clearing IPSec packet statistical information

This command clears IPSec packet statistical information. All statistical information is set to zero.

Perform the following configuration in the user view.

Table 7-32 Clear IPSec packet statistics

Operation	Command
Clear IPSec packet statistical information	**reset ipsec statistics**

III. Deleting SA

The configuration is used to delete the established SA (either manually or through IKE negotiation). If no parameter is specified, all the SAs will be deleted.

Perform the following configuration in user view.

Table 7-33 Delete SA

Operation	Command
Delete SA	**reset ipsec sa** [**remote** *ip-address* **|** **policy** *policy-name* [*seq-number*] **|** **parameters** *dest-address protocol spi*]

If a packet re-triggers IKE negotiation after an SA set up through IKE negotiation is deleted, IKE will reestablish an SA through negotiation.

If an SA set up manually is deleted, the system will automatically set up a new SA according to the parameter manually set up.

The keyword **parameters** will take effect only after the *spi* of the outbound SA is defined. Because SAs appear in pairs, the inbound SA will also be deleted after the outbound SA is deleted.

7.3.2 Displaying and Debugging Encryption Card Information

I. Displaying and debugging IPSec information on encryption cards

You can view the IPSec configurations, including SA information, statistics, log, interface information and IPSec module backup function, on the encryption card using **display** commands.

Execute the **debugging** command in user view for the debugging of IPSec configuration.

Table 7-34 Display and debug encryption card configuration

Operation	Command
Display SA information on the encryption card	**display encrypt-card sa** [*slot-id*]
Display statistics on the encryption card	**display encrypt-card statistics** [*slot-id*]

Operation	Command
Display system logging information on the encryption card	**display encrypt-card syslog** [*slot-id*]
Display interface information on the encryption card	**display interface encrypt** [*slot-id*]
Display information about the fast forwarding cache for the encryption cards	**display encrypt-card fast-switch**
Enable to information, packet, SA, command, error and other message debugging on the encryption card	**debugging encrypt-card** { { **all** | **command** | **error** | **misc** | **packet** | **sa** } [*slot-id*]
Disable to information, packet, SA, command, error and other message debugging on the encryption card	**undo debugging encrypt-card** { { **all** | **command** | **error** | **misc** | **packet** | **sa}** [*slot-id*]
Enable V 2.41 test software debugging on the encryption card	**debugging encrypt-card host** { **all** | **packet** | **sa** | **command** | **error** | **misc** } [*slot-id*]
Disable V 2.41 test software debugging on the encryption card	**undo debugging encrypt-card host** { **all** | **packet** | **sa** | **command** | **error** | **misc** } [*slot-id*]

II. Clearing statistics on encryption card

If no slot ID is specified in the command, the statistics of all the encryption cards on the router shall be cleared.

Perform the following configuration in the user view.

Table 7-35 Clear statistics on encryption card(s)

Operation	Command
Clear statistics on encryption card	**reset counters interface encrypt** [*slot-id*]

III. Deleting SA on encryption card

If no slot ID is specified in the command, the established SAs (either manually or through IKE negotiation) of all the encryption cards on the router shall be deleted.

Perform the following configuration in user view.

Table 7-36 Delete SA

Operation	Command
Delete SAs on the encryption card	**reset encrypt-card sa** [*slot-id*]

IV. Clearing packet statistics on encryption card

You can reset all counters on the encryption card, including those for data packets, byte counting, lost packets, failed authentication, faulty SAs, invalid SA proposals, invalid protocols, and so on.

Perform the following configuration in user view.

Table 7-37 Clear packet statistics on encryption card

Operation	Command
Clear packet statistics on encryption card	**reset encrypt-card statistics** [*slot-id*]

V. Clearing system log on encryption card

You can clear the system log, which records all key operations to it, on the encryption card.

Perform the following configuration in user view.

Table 7-38 Clear system log on encryption card

Operation	Command
Clear system log on encryption card	**reset encrypt-card syslog** [*slot-id*]

7.4 Typical IPSec Configuration Examples

7.4.1 Establishing Security Association Manually

I. Network requirements

A security tunnel will be configured between Router A and Router B. Data flow security protection will be setup between sub-network (10.1.1.x) represented by PC A and sub-network (10.1.2.x) represented by PC B. Security protocol used is ESP and encryption algorithm is DES. The authentication method is SHA1-HMAC-96.

II. Network diagram

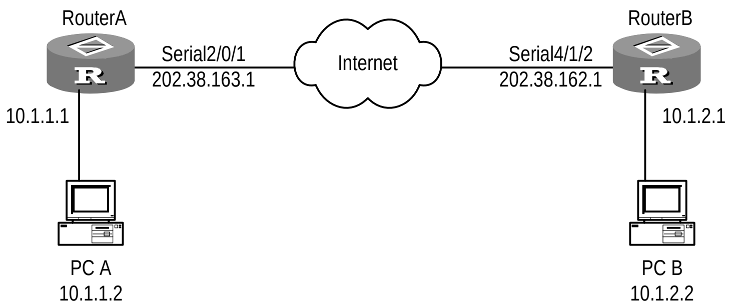


Figure 7-3 Diagram for IPSec configuration

III. Configuration procedure

1) Router A will be configured as follows:

# Configure an access control list, defining data flow from sub-network 10.1.1.x to sub-network 10.1.2.x.

```
[3Com] acl number 3101
[3Com-acl-adv-3101] rule permit ip source 10.1.1.0 0.0.0.255 destination
10.1.2.0 0.0.0.255
[3Com-acl-adv-3101] rule deny ip source any destination any
```

# Configure the static route to PC B.

```
[3Com] ip route-static 10.1.2.0 255.255.255.0 202.38.162.1
```

# Establish IPSec proposal, and the name is tran1.

```
[3Com] ipsec proposal tran1
```

# Packet encapsulation format is tunnel mode.

```
[3Com-ipsec-proposal-tran1] encapsulation-mode tunnel
```

# Security protocol is ESP.

```
[3Com-ipsec-proposal-tran1] transform esp
```

# Select algorithm.

```
[3Com-ipsec-proposal-tran1] esp encryption-algorithm des
[3Com-ipsec-proposal-tran1] esp authentication-algorithm sha1
```

# Return to system view.

```
[3Com-ipsec-proposal-tran1] quit
```

# Establish an IPSec policy and negotiation mode is manual.

```
[3Com] ipsec policy map1 10 manual
```

# Reference access control list.

```
[3Com-ipsec-policy-manual-map1-10] security acl 3101
```

# Reference the IPSec proposal.

```
[3Com-ipsec-policy-manual-map1-10] proposal tran1
```

# Configure the peer address.

```
[3Com-ipsec-policy-manual-map1-10] tunnel remote 202.38.162.1
```

# Configure local end address.

```
[3Com-ipsec-policy-manual-map1-10] tunnel local 202.38.163.1
```

# Configure SPI.

```
[3Com-ipsec-policy-manual-map1-10] sa spi outbound esp 12345
[3Com-ipsec-policy-manual-map1-10] sa spi inbound esp 54321
```

# Configure shared secret.

```
[3Com-ipsec-policy-manual-map1-10] sa string-key outbound esp abcdefg
[3Com-ipsec-policy-manual-map1-10] sa string-key inbound esp gfedcba
```

# Return to system view.

```
[3Com-ipsec-policy-manual-map1-10] quit
```

# Enter serial interface view.

```
[3Com] interface serial 2/0/1
```

# Configure serial interface IP address.

```
[3Com-Serial2/0/1] ip address 202.38.163.1 255.0.0.0
```

# On serial interface, use IPSec policy group.

```
[3Com-Serial2/0/1] ipsec policy map1
```

2) Router B will be configured as follows:

# Configure an access control list, specifying data flow from sub-network 10.1.2.x to sub-network 10.1.1.x.

```
[3Com] acl number 3101
[3Com-acl-adv-3101] rule permit ip source 10.1.2.0 0.0.0.255 destination
10.1.1.0 0.0.0.255
[3Com-acl-adv-101] rule deny ip source any destination any
```

# Configure the static route to PC A.

```
[3Com] ip route-static 10.1.1.0 255.255.255.0 202.38.163.1
```

# Establish IPSec proposal with the name tran1.

```
[3Com] ipsec proposal tran1
```

# Set packet encapsulation mode to tunnel mode.

```
[3Com-ipsec-proposal-tran1] encapsulation-mode tunnel
```

# Security protocol is ESP protocol.

```
[3Com-ipsec-proposal-tran1] transform esp
```

# Select algorithm.

```
[3Com-ipsec-proposal-tran1] esp encryption-algorithm des
[3Com-ipsec-proposal-tran1] esp authentication-algorithm sha1
```

# Return to system view.

```
[3Com-ipsec-proposal-tran1] quit
```

# Establish an IPSec policy with negotiation mode as manual.

```
[3Com] ipsec policy use1 10 manual
```

# Reference access control list.

```
[3Com-ipsec-policyl-manual-use1-10] security acl 3101
```

# Reference the IPSec proposal.

```
[3Com-ipsec-policyl-manual-use1-10] proposal tran1
```

# Configure peer address.

```
[3Com-ipsec-policyl-manual-use1-10] tunnel remote 202.38.163.1
```

# Configure local end address.

```
[3Com-ipsec-policyl-manual-use1-10] tunnel local 202.38.162.1
```

# Configure SPI.

```
[3Com-ipsec-policyl-manual-use1-10] sa spi outbound esp 54321
[3Com-ipsec-policyl-manual-use1-10] sa spi inbound esp 12345
```

# Configure key.

```
[3Com-ipsec-policyl-manual-use1-10] sa string-key outbound esp gfedcba
[3Com-ipsec-policyl-manual-use1-10] sa string-key inbound esp abcdefg
```

# Return to system view.

```
[3Com-ipsec-policyl-manual-use1-10] quit
```

# Enter serial interface view.

```
[3Com] interface serial 4/1/2
```

# Configure serial interface IP address.

```
[3Com-Serial4/1/2] ip address 202.38.162.1 255.0.0.0
```

# Use IPSec policy group on serial interface,.

```
[3Com-Serial4/1/2] ipsec policy use1
```

When the above configuration is completed, the security tunnel between Router A and Router B is established. The data flow between sub-network 10.1.1.x and sub-network 10.1.2.x will be encrypted before being transmitted

7.4.2 Establishing Security Association in isakmp Mode

I. Network requirements

As displayed in above figure, a security tunnel is configured between Router A and Router B. Data flow security protection will be setup between sub-network (10.1.1.x) represented by PC A and sub-network (10.1.2.x) represented by PC B. Security protocol used is ESP and encryption algorithm is DES. The authentication method is SHA1-HMAC-96.

II. Network diagram

See Figure 7-3.

III. Configuration procedure

1) Configure Router A

# Configure an access control list, specifying data flow from sub-network 10.1.1.x to sub-network 10.1.2.x.

```
[3Com] acl number 3101
[3Com-acl-adv-3101] rule permit ip source 10.1.1.0 0.0.0.255 destination
10.1.2.0 0.0.0.255
[3Com-acl-adv-3101] rule deny ip source any destination any
```

# Configure static route to PC B.

```
[3Com] ip route-static 10.1.2.0 255.255.255.0 202.38.162.1
```

# Establish IPSec proposal with the name tran1.

```
[3Com] ipsec proposal tran1
```

# Packet encapsulation format is tunnel mode.

```
[3Com-ipsec-proposal-tran1] encapsulation-mode tunnel
```

# Security protocol is ESP.

```
[3Com-ipsec-proposal-tran1] transform esp
```

# Select algorithms.

```
[3Com-ipsec-proposal-tran1] esp encryption-algorithm des
[3Com-ipsec-proposal-tran1] esp authentication-algorithm sha1
```

# Return to system view.

```
[3Com-ipsec-proposal-tran1] quit
```

# Configure an IKE peer.

```
[3Com] ike peer peer
[3Com-ike-peer-peer] pre-shared-key abcde
[3Com-ike-peer-peer] remote-address 202.38.162.1
```

# Establish an IPSec policy, and negotiation is isakmp.

```
[3Com] ipsec policy map1 10 isakmp
```

# Reference IPSec proposal.

```
[3Com-ipsec-policy-isakmp-map1-10] proposal tran1
```

# Reference access control list.

```
[3Com-ipsec-policy-isakmp-map1-10] security acl 3101
```

# Reference the IKE peer.

```
[3Com-ipsec-policy-isakmp-map1-10] ike peer peer
```

# Return to system view.

```
[3Com-ipsec-policy-isakmp-map1-10] quit
```

# Enter serial interface view.

```
[3Com] interface serial 2/0/1
```

# Configure serial interface IP address.

```
[3Com-Serial2/0/1] ip address 202.38.163.1 255.0.0.0
```

# Apply IPSec policy group on serial interface.

```
[3Com-Serial2/0/1] ipsec policy map1
```

# Return to system view.

```
[3Com-Serial2/0/1] quit
```

2) Configure Router B

# Configure an access control list, specifying data flow from sub network10.1.2.x to sub-network 10.1.1.x.

```
[3Com] acl number 3101
[3Com-acl-adv-3101] rule permit ip source 10.1.2.0 0.0.0.255 destination
10.1.1.0 0.0.0.255
[3Com-acl-adv-3101] rule deny ip source any source any
```

# Configure the static route to PC A.

```
[3Com] ip route-static 10.1.1.0 255.255.255.0 202.38.163.1
```

# Establish IPSec proposal, and the name is tran1.

```
[3Com] ipsec proposal tran1
```

# Packet encapsulation format is tunnel mode.

```
[3Com-ipsec-proposal-tran1] encapsulation-mode tunnel
```

# Security protocol is ESP.

```
[3Com-ipsec-proposal-tran1] transform esp
```

# Select algorithms.

```
[3Com-ipsec-proposal-tran1] esp encryption-algorithm des
[3Com-ipsec-proposal-tran1] esp authentication-algorithm sha1
```

# Return to system view.

```
[3Com-ipsec-proposal-tran1] quit
```

# Configure an IKE peer.

```
[3Com] ike peer peer
[3Com-ike-peer-peer] pre-shared-key abcde
[3Com-ike-peer-peer] remote-address 202.38.163.1
```

# Establish an IPSec policy, and negotiation mode is isakmp.

```
[3Com] ipsec policy use1 10 isakmp
```

# Reference access control list.

```
[3Com-ipsec-policy-isakmp-use1-10] security acl 3101
```

# Reference IPSec proposal.

```
[3Com-ipsec-policy-isakmp-use1-10] proposal tran1
```

# Reference the IKE peer.

```
[3Com-ipsec-policy-isakmp-map1-10] ike peer peer
```

# Return to system view.

```
[3Com-ipsec-policy-isakmp-use1-10] quit
```

# Enter serial interface view.

```
[3Com] interface serial 4/1/2
```

# Configure serial interface IP address.

```
[3Com-Serial4/1/2] ip address 202.38.162.1 255.0.0.0
```

# Use IPSec policy group on serial interface.

```
[3Com-Serial4/1/2] ipsec policy use1
```

# Return to system view.

```
[3Com-Serial4/1/2] quit
```

After above configuration is finished, if there is packet transmitted between Router A and Router B, IKE will be triggered for negotiation to establish Security Association. When the IKE negotiation succeeds and Security Association is established, data flow will be encrypted before transmission between sub-network 10.1.1.x and sub-network 10.1.2.x.

7.4.3 Implementing Encryption/Decryption and Authentication on Encryption Card

I. Network requirements

A security tunnel will be configured between Router A and Router B. Data flow security protection will be setup between sub-network (10.1.1.0/24) represented by PC A and sub-network (10.1.2.0/24) represented by PC B. Manually create SAs, choose ESP protocol, DES encryption algorithm and SHA1-HMAC-96 authentication algorithm.

II. Network diagram

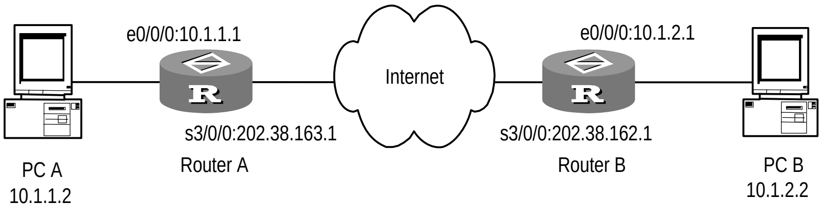


Figure 7-4 Network diagram for creating SAs over encryption card

III. Configuration procedure

1) Configure Router A

# Configure an access control list, defining data flow from sub-network 10.1.1.0/24 to sub-network 10.1.2.0/24.

```
[Router] acl 3001
[Router-acl-3001] rule permit ip source 10.1.1.0 0.0.0.255 destination
10.1.2.0 0.0.0.255
[Router-acl-3001] rule deny ip source any destination any
[Router-acl-3001] quit
```

# Create SA proposal “trans1”.

```
[Router] ipsec card-proposal tran1
```

# Specify SA proposal trans1 to use the encryption card on the slot 1/0/0.

```
[Router-ipsec-card-proposal-tran1] use encrypt-card 1/0/0
```

# Packet encapsulation format is tunnel mode.

```
[Router-ipsec-card-proposal-tran1] encapsulation-mode tunnel
```

# Security protocol is ESP.

```
[Router-ipsec-proposal-tran1] transform esp
```

# Select algorithm.

```
[Router-ipsec-proposal-tran1] esp encryption-algorithm des
[Router-ipsec-proposal-tran1] esp authentication-algorithm sha1-hmac-96
```

# Return to system view.

```
[Router-ipsec-proposal-tran1] quit
```

# Establish a security policy and negotiation mode is manual.

```
[Router] ipsec policy policy1 10 manual
```

# Reference access control list.

```
[Router-ipsec-policy-policy1-10] security acl 3001
```

# Configure the peer address.

```
[Router-ipsec-policy-policy1-10] tunnel remote 202.38.162.1
```

# Configure local end address.

```
[Router-ipsec-policy-policy1-10] tunnel local 202.38.163.1
```

# Reference SA proposal.

```
[Router-ipsec-policy-policy1-10] proposal tran1
```

# Configure SPI.

```
[Router-ipsec-policy-policy1-10] sa outbound esp spi 12345
[Router-ipsec-policy-policy1-10] sa inbound esp spi 54321
```

# Configure shared secret.

```
[Router-ipsec-policy-policy1-10] sa outbound esp string-key abcdefg
[Router-ipsec-policy-policy1-10] sa inbound esp string-key gfedcba
```

# Return to system view.

```
[Router-ipsec-policy-policy1-10] quit
```

# Enter Ethernet interface view; configure IP address.

```
[Router] interface Ethernet0/0/0
[Router-Ethernet0/0/0] ip address 10.1.1.1 255.255.255.0
```

# Enter serial interface view; configure IP address.

```
[Router-Ethernet0/0/0] interface serial 3/0/0
[Router-Serial3/0/0] ip address 202.38.163.1 255.255.255.0
```

# Apply the security policy set to the serial interface.

```
[Router-Serial3/0/0] ipsec policy policy1
[Router-Serial3/0/0] quit
```

# Return to system view, configure a static route to the segment 10.1.2.0/24.

```
[Router] ip route-static 10.1.2.0 255.255.255.0 202.38.162.1
```

2) Router B will be configured as follows:

# Configure an access control list, specifying data flow from sub-network 10.1.2.0/24 to sub-network 10.1.1.0/24.

```
[Router] acl 3000
[Router-acl-3000] rule permit ip source 10.1.2.0 0.0.0.255 destination
10.1.1.0 0.0.0.255
[Router-acl-3000] rule deny ip source any destination any
[Router-acl-3000] quit
```

# Create the SA proposal named trans1.

```
[Router] ipsec card-proposal tran1
```

# Specify SA proposal trans1 to use the encryption card on the slot 1/0/0.

```
[Router-ipsec-card-proposal-tran1] use encrypt-card 1/0/0
```

# Packet encapsulation format is tunnel mode.

```
[Router-ipsec-card-proposal-tran1] encapsulation-mode tunnel
```

# Security protocol is ESP.

```
[Router-ipsec-card-proposal-tran1] transform esp
```

# Select algorithms.

```
[Router-ipsec-card-proposal-tran1] esp encryption-algorithm des
[Router-ipsec-card-proposal-tran1]      esp      authentication-algorithm
sha1-hmac-96
```

# Return to system view.

```
[Router-ipsec-card-proposal-tran1] quit
```

# Establish a security policy and negotiation mode is manual.

```
[Router] ipsec policy map1 10 manual
```

# Reference access control list.

```
[Router-ipsec-policy-map1-10] security acl 3000
```

# Configure the peer address.

```
[Router-ipsec-policy-map1-10] tunnel remote 202.38.163.1
```

# Configure local end address.

```
[Router-ipsec-policy-map1-10] tunnel local 202.38.162.1
```

# Reference SA proposal.

```
[Router-ipsec-policy-map1-10] proposal tran1
```

# Configure SPI.

```
[Router-ipsec-policy-map1-10] sa outbound esp spi 54321
[Router-ipsec-policy-map1-10] sa inbound esp spi 12345
```

# Configure shared secret.

```
[Router-ipsec-policy-map1-10] sa outbound esp string-key gfedcba
[Router-ipsec-policy-map1-10] sa inbound esp string-key abcdefg
```

# Return to system view.

```
[Router-ipsec-policy-map1-10] quit
```

# Enter Ethernet interface view; configure IP address.

```
[Router] interface Ethernet0/0/0
[Router-Ethernet0/0/0] ip address 10.1.2.1 255.255.255.0
```

# Enter serial interface view, configure IP address.

```
[Router-Ethernet0/0/0] interface serial 3/0/0
```

```
[Router-Serial3/0/0] ip address 202.38.162.1 255.255.255.0
```

# Apply the security policy set on the serial interface.

```
[Router-Serial0/0/0] ipsec policy map1
[Router-Serial3/0/0] quit
```

# Configure a static route to the segment 10.1.1.0/24.

```
[Router] ip route-static 10.1.1.0 255.255.255.0 202.38.163.1
```

7.4.4 Setting Up SAs Between a Router and a VRRP Standby Group

I. Network requirements

As shown in the following diagram, the headquarters uses the VRRP standby group formed by Router A and Router B as its default gateway. Router E sets up IPSec SAs with the virtual address of this VRRP standby group to protect data transmitted between the headquarters and the branch.

Router C and Router D are access routers of operators. They are not discussed here.

II. Network diagram

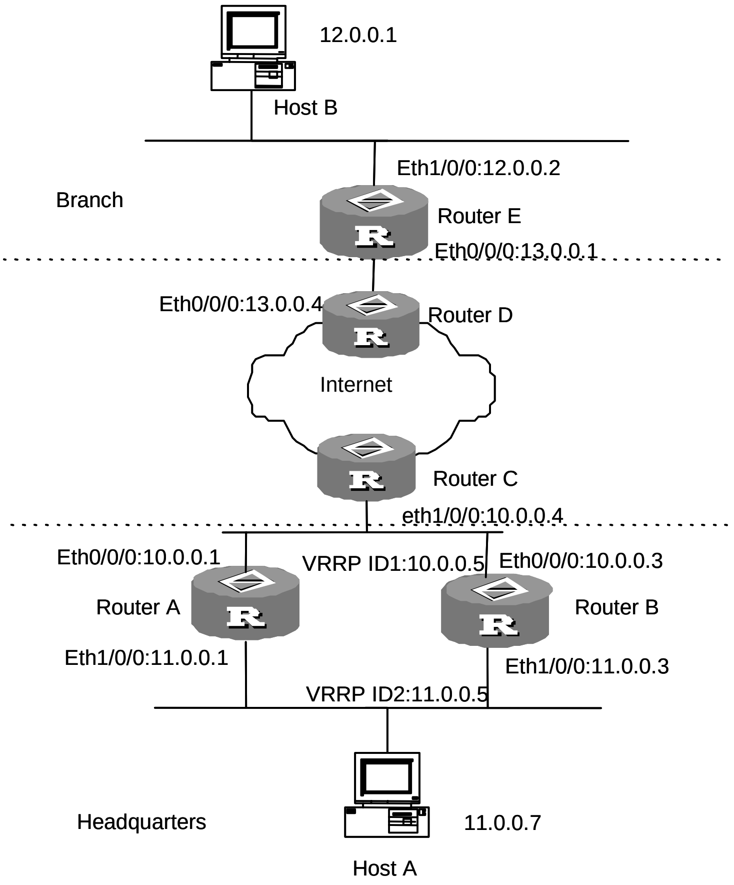


Figure 7-5 Set up SAs between a router and a virtual address of a VRRP backup group

III. Configuration procedure

1) Configure Router A

# Configure Router A as the master in a VRRP group.

```
<3Com> system
[3Com] vrrp ping-enable
[3Com] interface ethernet0/0/0
[3Com-Ethernet0/0/0] ip address 10.0.0.1 255.255.255.0
[3Com-Ethernet0/0/0] vrrp vrid 1 virtual-ip 10.0.0.5
[3Com-Ethernet0/0/0] vrrp vrid 1 priority 120
[3Com-Ethernet0/0/0] vrrp vrid 1 preempt-mode timer delay 5
[3Com-Ethernet0/0/0] interface ethernet1/0/0
[3Com-Ethernet1/0/0] ip address 11.0.0.1 255.255.255.0
[3Com-Ethernet1/0/0] vrrp vrid 2 virtual-ip 11.0.0.5
[3Com-Ethernet1/0/0] vrrp vrid 2 priority 120
[3Com-Ethernet1/0/0] vrrp vrid 2 preempt-mode timer delay 5
[3Com-Ethernet1/0/0] quit
```

# Configure the data flow protected by IPSec.

```
[3Com] acl number 3101
[3Com-acl-adv-3101] rule 0 permit ip source 11.0.0.0 0.0.0.255 destination
12.0.0.0 0.0.0.255
[3Com-acl-adv-3101] rule deny ip source any destination any
[3Com-acl-adv-3101] quit
```

# Configure a static route to host B.

```
[3Com] ip route-static 0.0.0.0 0.0.0.0 10.0.0.4 preference 60
```

# Configure IPSec DPD.

```
[3Com] ike dpd dpd1
[3Com-ike-dpd-dpd1] interval_time 10
[3Com-ike-dpd-dpd1] time_out 5
[3Com-ike-dpd-dpd1] quit
```

# Create a security proposal named tran1 (the contents are omitted).

```
[3Com] ipsec proposal tran1
```

#Configure an IKE peer.

```
[3Com] ike peer peer
[3Com-ike-peer-peer] pre-shared-key abcde
[3Com-ike-peer-peer] remote-address 13.0.0.1
[3Com-ike-peer-peer] local-address 10.0.0.5
[3Com-ike-peer-peer] dpd dpd1
[3Com-ike-peer-peer] quit
```

# Create a security policy, setting negotiation mode to ISAKMP.

```
[3Com] ipsec policy map1 10 isakmp
[3Com-ipsec-policy-isakmp-map1-10] proposal tran1
[3Com-ipsec-policy-isakmp-map1-10] security acl 3101
[3Com-ipsec-policy-isakmp-map1-10] ike-peer peer
[3Com-ipsec-policy-isakmp-map1-10] quit
```

# Apply an IPSec policy group to the interface.

```
[3Com] interface ethernet 0/0/0
[3Com-ethernet 0/0/0] ipsec policy map1
[3Com-ethernet 0/0/0] quit
```

2) Configure Router B

# Configure Router B as a slave in the VRRP standby group. It uses the default priority 100, lower than that of Router A.

```
<3Com> system
[3Com] vrrp ping-enable
[3Com] interface ethernet 0/0/0
[3Com-Ethernet 0/0/0] ip address 10.0.0.3 255.255.255.0
[3Com-Ethernet 0/0/0] vrrp vrid 1 virtual-ip 10.0.0.5
[3Com-Ethernet 0/0/0] interface ethernet 1/0/0
[3Com-Ethernet1/0/0] ip address 11.0.0.3 255.255.255.0
[3Com-Ethernet1/0/0] vrrp vrid 2 virtual-ip 11.0.0.5
[3Com-Ethernet1/0/0] quit
```

# Configure the data flow protected by IPSec.

```
[3Com] acl number 3101
[3Com-acl-adv-3101] rule 0 permit ip source 11.0.0.0 0.0.0.255 destination
12.0.0.0 0.0.0.255
[3Com-acl-adv-3101] rule deny ip source any destination any
[3Com-acl-adv-3101] quit
```

# Configure a static route to host B.

```
[3Com] ip route-static 0.0.0.0 0.0.0.0 10.0.0.4 preference 60
```

# Configure IPSec DPD.

```
[3Com] ike dpd dpd1
[3Com-ike-dpd-dpd1] interval_time 10
[3Com-ike-dpd-dpd1] time_out 5
[3Com-ike-dpd-dpd1] quit
```

#Create a security proposal named tran1 (the contents are omitted).

```
[3Com] ipsec proposal tran1
```

# Configure an IKE peer.

```
[3Com] ike peer peer
[3Com-ike-peer-peer] pre-shared-key abcde
```

```
[3Com-ike-peer-peer] remote-address 13.0.0.1
[3Com-ike-peer-peer] local-address 10.0.0.5
[3Com-ike-peer-peer] dpd dpd1
[3Com-ike-peer-peer] quit
```

# Create an IPSec policy, setting negotiation mode to ISAKMP.

```
[3Com] ipsec policy map1 10 isakmp
[3Com-ipsec-policy-isakmp-map1-10] proposal tran1
[3Com-ipsec-policy-isakmp-map1-10] security acl 3101
[3Com-ipsec-policy-isakmp-map1-10] ike-peer peer
[3Com-ipsec-policy-isakmp-map1-10] quit
```

# Apply a security policy group to the interface.

```
[3Com] interface ethernet 0/0/0
[3Com-Ethernet0/0/0] ipsec policy map1
[3Com-Ethernet0/0/0] quit
```

3) Configure Router E

# Configure the data flow protected by IPSec.

```
[3Com] acl number 3101
[3Com-acl-adv-3101] rule 0 permit ip source 12.0.0.0 0.0.0.255 destination
11.0.0.0 0.0.0.255
[3Com-acl-adv-3101] rule deny ip source any destination any
[3Com-acl-adv-3101] quit
```

# Configure a static route to host A.

```
[3Com] ip route-static 0.0.0.0 0.0.0.0 13.0.0.4 preference 60
```

# Configure IPSec DPD.

```
[3Com] ike dpd dpd1
[3Com-ike-dpd-dpd1] interval_time 10
[3Com-ike-dpd-dpd1] time_out 5
[3Com-ike-dpd-dpd1] quit
```

# Create a security proposal named tran1 (the content is omitted).

```
[3Com] ipsec proposal tran1
```

# Configure an IKE peer.

```
[3Com] ike peer peer
[3Com-ike-peer-peer] pre-shared-key abcde
[3Com-ike-peer-peer] remote-address 10.0.0.5
[3Com-ike-peer-peer] local-address 13.0.0.1
[3Com-ike-peer-peer] dpd dpd1
[3Com-ike-peer-peer] quit
```

# Create a security policy, setting negotiation mode to ISAKMP.

```
[3Com] ipsec policy map1 10 isakmp
[3Com-ipsec-policy-isakmp-map1-10] proposal tran1
[3Com-ipsec-policy-isakmp-map1-10] security acl 3101
[3Com-ipsec-policy-isakmp-map1-10] ike-peer peer
[3Com-ipsec-policy-isakmp-map1-10] quit
```

# Apply an IPSec policy group to the interface.

```
[3Com] interface ethernet 0/0/0
[3Com-Ethernet 0/0/0] ip address 13.0.0.1 255.0.0.0
[3Com-Ethernet 0/0/0] ipsec policy map1
[3Com-Ethernet 0/0/0] quit
```

# Configure an Ethernet interface.

```
[3Com] interface ethernet 1/0/0
[3Com-Ethernet1/0/0] ip address 12.0.0.2 255.255.255.0
```

Execute the **ping -c 500 11.0.0.7** command on host B to ping PC A, and then execute the **display ike sa** and **display ipsec sa** commands on Router A and Router E respectively to display established SAs.

Execute the **shutdown** command on interface Ethernet 0/0/0 on Router A. Then execute the **debugging ike dpd** command on Router E. You may find out that a DPD query is sent three times, but no acknowledgement is received. Then, all SAs on the involved peer are deleted, while failover is happening in the VRRP standby group. About 10 seconds later, the security tunnel is recovered. The following debugging information is displayed:

```
<3Com> debugging ike dpd
```

(SAs are deleted after three DPD query attempts are failed.)

```
RouterE IKE/8/DEBUG:REQUEST(send dpd request): send a message (seqno:-12903966)
RouterE IKE/8/DEBUG:REQUEST: wait for response timeout
RouterE IKE/8/DEBUG:REQUEST(send dpd request): send a message (seqno:-1917909230
RouterE IKE/8/DEBUG:REQUEST: wait for response timeout
RouterE IKE/8/DEBUG:REQUEST(send dpd request): send a message (seqno:-1183268982)
RouterE IKE/8/DEBUG:REQUEST: wait for response timeout
RouterE IKE/8/DEBUG:REQUEST: there are three fail and all SAs associated were deleted
```

(A response is received from the peer after the failover completes in its corresponding VRRP standby group)

```
RouterE IKE/8/DEBUG:REQUEST(send dpd request): send a message (seqno:1382148220)
RouterE IKE/8/DEBUG:REQUEST(recv dpd response): received a message
```

```
(seqno:1382148220)
RouterE IKE/8/DEBUG:RESPONSE(recv dpd request): received a message
(seqno:1382148220)
RouterE IKE/8/DEBUG:RESPONSE(send dpd response): send a message
(seqno:1382148220)
```

7.4.5 IPSec/IKE Multi-Instance Configuration Example

I. Network requirements

CE1 and CE3 belong to VPN1. CE2 and CE4 belong to VPN2. Both CE1 and CE2 are connected to PE1 through IPSec/IKE tunnels.

II. Network diagram

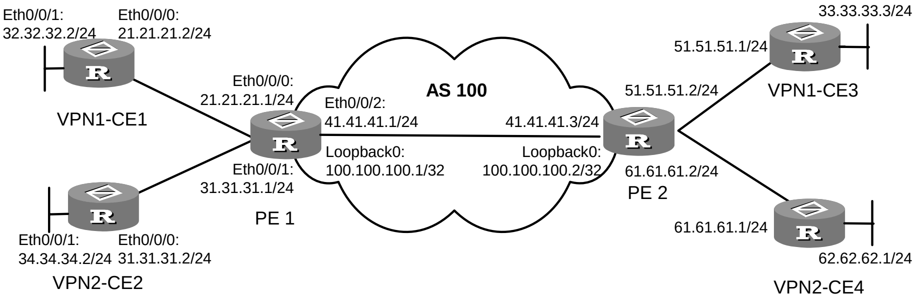


Figure 7-6 Network diagram for IPSec/IKE multi-instance configuration

III. Configuration procedure

1) Configure CE1

```
<CE1> system-view
```

# Configure an IKE peer.

```
[CE1] ike peer test
[CE1-ike-peer-test] pre-shared-key huawei
[CE1-ike-peer-test] remote-address 21.21.21.1
[CE1-ike-peer-test] quit
```

# Configure an IPSec proposal. (The details are omitted here.)

```
[CE1] ipsec proposal prop
```

# Configure an IPSec policy.

```
[CE1] ipsec policy map 1 isakmp
[CE1-ipsec-policy-isakmp-map-1] security acl 3000
[CE1-ipsec-policy-isakmp-map-1] ike-peer test
[CE1-ipsec-policy-isakmp-map-1] proposal prop
[CE1-ipsec-policy-isakmp-map-1] quit
```

# Configure Ethernet interfaces and apply IPSec policies to interface Ethernet 0/0/0.

```
[CE1] interface Ethernet0/0/0
[CE1-Ethernet0/0/0] ip address 21.21.21.2 255.255.255.0
[CE1-Ethernet0/0/0] ipsec policy map
[CE1-Ethernet0/0/0] quit
[CE1] interface Ethernet0/0/1
[CE1-Ethernet0/0/1] ip address 32.32.32.1 255.255.255.0
[CE1-Ethernet0/0/1] quit
```

# Configure the data stream to be protected by IPSec.

```
[CE1] acl number 3000
[CE1-acl-adv-3000] rule 0 permit ip source 21.21.21.0 0.0.0.255 destination
51.51.51.0 0.0.0.255
[CE1-acl-adv-3000] quit
```

# Configure static routes.

```
[CE1] ip route-static 0.0.0.0 0.0.0.0 21.21.21.1 preference 60
[CE1] ip route-static 33.33.33.0 255.255.255.0 21.21.21.1 preference 60
```

2) Configure PE1

```
<PE1> system-view
```

# Configure MPLS basic capabilities.

```
[PE1] mpls lsr-id 100.100.100.1
[PE1] mpls
[PE1-mpls] quit
[PE1] mpls ldp
```

# Configure the VPN instance vrf1.

```
[PE1] ip vpn-instance vrf1
[PE1-vpn-vrf1] route-distinguisher 100:1
[PE1-vpn-vrf1] vpn-target 100:1 export-extcommunity
[PE1-vpn-vrf1] vpn-target 100:1 import-extcommunity
[PE1-vpn-vrf1] quit
```

# Configure the VPN instance vrf2.

```
[PE1] ip vpn-instance vrf2
[PE1-vpn-vrf2] route-distinguisher 100:2
[PE1-vpn-vrf2] vpn-target 100:2 export-extcommunity
[PE1-vpn-vrf2] vpn-target 100:2 import-extcommunity
[PE1-vpn-vrf2] quit
```

# Configure the IKE peer test1.

```
[PE1] ike peer test1
[PE1-ike-peer-test1] pre-shared-key huawei
[PE1-ike-peer-test1] remote-address 21.21.21.2
[PE1-ike-peer-test1] quit
```

# Configure the IKE peer test2.

```
[PE1]  ike peer test2
[PE1-ike-peer-test2]  pre-shared-key huawei
[PE1-ike-peer-test2] remote-address 31.31.31.2
[PE1-ike-peer-test2] quit
```

# Configure IPSec proposals. (The details are omitted here.)

```
[PE1] ipsec proposal prop1
[PE1] ipsec proposal prop2
```

# Configure IPSec policies.

```
[PE1] ipsec policy map1 1 isakmp
[PE1-ipsec-policy-isakmp-map-1] security acl 3000
[PE1-ipsec-policy-isakmp-map-1]  ike-peer test1
[PE1-ipsec-policy-isakmp-map-1]  proposal prop
[PE1-ipsec-policy-isakmp-map-1] quit
[PE1] ipsec policy map2 1 isakmp
[PE1-ipsec-policy-isakmp-map-2] security acl 3001
[PE1-ipsec-policy-isakmp-map-2] ike-peer test2
[PE1-ipsec-policy-isakmp-map-2] proposal prop2
```

# Bind the VPN instances to the Ethernet interfaces and apply IPSec policies to the interfaces.

```
[PE1] interface Ethernet0/0/0
[PE1-Ethernet0/0/0] ip binding vpn-instance vrf1
[PE1-Ethernet0/0/0] ip address 21.21.21.1 255.255.255.0
[PE1-Ethernet0/0/0] ipsec policy map1
[PE1-Ethernet0/0/0] quit
[PE1] interface Ethernet0/0/1
[PE1-Ethernet0/0/1] ip binding vpn-instance vrf2
[PE1-Ethernet0/0/1] ip address 31.31.31.1 255.255.255.0
[PE1-Ethernet0/0/1] ipsec policy map2
[PE1-Ethernet0/0/1] quit
```

# Enable MPLS on the interface Ethernet0/0/2.

```
[PE1] interface Ethernet0/0/2
[PE1- Ethernet0/0/2] ip address 41.41.41.1 255.255.255.0
[PE1- Ethernet0/0/2] mpls
[PE1- Ethernet0/0/2] mpls ldp enable
[PE1- Ethernet0/0/2] quit
```

# Configure the interface LoopBack0.

```
[PE1] interface LoopBack0
[PE1-LoopBack0] ip address 100.100.100.1 255.255.255.255
```

# Configure the data stream to be protected by IPSec.

```
[PE1] acl number 3000
[PE1-acl-adv-3000] rule 0 permit ip source 51.51.51.0 0.0.0.255 destination
21.21.21.0 0.0.0.255
[PE1-acl-adv-3000] quit
[PE1] acl number 3001
[PE1-acl-adv-3001] rule 0 permit ip source 61.61.61.0 0.0.0.255 destination
31.31.31.0 0.0.0.255
[PE1-acl-adv-3001] quit
```

# Establish MP-IBGP neighbors between PE1 and PE2. Activate the MP-IBGP peers in VPNv4 address family view.

```
[PE1] bgp 100
[PE1-bgp] undo synchronization
[PE1-bgp] group g1 internal
[PE1-bgp] peer 100.100.100.2 group g1
[PE1-bgp] peer 100.100.100.2 connect-interface LoopBack0
[PE1-bgp] ipv4-family vpnv4
[PE1-bgp-af-vpn] peer g1 enable
[PE1-bgp-af-vpn] peer 100.100.100.2 group g1
[PE1-bgp-af-vpn] quit
```

# Redistribute the private network routes of CE1 and CE2.

```
[PE1-bgp] ipv4-family vpn-instance vrf1
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] undo synchronization
[PE1-bgp-af-vpn-instance] quit
[PE1-bgp] ipv4-family vpn-instance vrf2
[PE1-bgp-af-vpn-instance] import-route direct
[PE1-bgp-af-vpn-instance] undo synchronization
[PE1-bgp-af-vpn-instance] quit
```

# Enable OSPF on the interfaces and loopback interfaces that connect PE1 and PE2 for the interconnectivity inside the AS.

```
[PE1] ospf 1
[PE1-ospf-1] area 0.0.0.0
[PE1-ospf-1] network 41.41.41.0 0.0.0.255
[PE1-ospf-1] network 100.100.0.0 0.0.255.255
[PE1-ospf-1] quit
```

# Configure private network static routes.

```
[PE1] ip route-static vpn-instance vrf1 32.32.32.0 255.255.255.0 21.21.21.2
preference 60
```

The configurations for CE2, CE3 and CE4 are similar to those for CE1. The configuration for PE2 is symmetric with that for PE1.

Chapter 8 IKE Configuration

8.1 IKE Overview

8.1.1 Brief Introduction to IKE

IKE (Internet Key Exchange) is Internet shared secret exchange protocol. It is a mixed protocol, configured in a framework specified by Internet Security Association and Key Management Protocol (ISAKMP). IKE will provide automatic negotiation and exchange of shared key for IPSec and configure Security Association, thus to simplify IPSec application and management.

Network security has 2 meanings: one is internal LAN security, the other is external data exchange security. The former is implemented by means of Firewall, network address translation (NAT) etc. Emerging IPSec (IP Security) implements the latter. IPSec Security Association can be established by manual configuration, but when nodes increase in the network, manual configuration will be very difficult, and hard to ensure security. In this case, the IKE automatic negotiation can be used to establish Security Association and exchange shared secret.

IKE has a series of self-protection mechanisms to safely distribute shared key, authenticate identity, and establish IPSec Security Association etc. in unsecured network.

IKE security mechanism includes:

- Diffie-Hellman (DH) exchange and shared key distribution

Diffie-Hellman algorithm is a shared key algorithm. The both parties in communication can exchange some data without transmitting shared key and find the shared key by calculation. The pre-condition for encryption is that the both parties must have shared key. The merit of IKE is that it never transmits shared key directly in the unsecured network, but calculates the shared key by exchanging a series data. Even if the third party (e.g. Hackers) captured all exchange data used to calculate shared key for both parties, he cannot figure out the real shared key.

- Perfect Forward Secrecy (PFS)

PFS feature is a security feature. When a shared key is decrypted, there will be no impact on the security of other shared keys, because these secrets have no derivative relations among them. IPSec is implemented by adding one key exchange during IKE negotiation phase II.

- Identity authentication

Identity authentication will authenticate identity for both parties in communication. Authentication key can input to generate shared secret. It is impossible for different authentication keys to generate the same shared secret between the two parties. Authentication key is the key in identity authentication for both parties.

- Identity protection

After shared secret is generated, identity data will be encrypted and transmitted, thus implementing identity data protection.

IKE using 2 stages to implement shared secret negotiation for IPSec and creating Security Association. In the first stage, parties involved in the communication will establish a channel for identity authentication and security protection. An ISAKMP Security Association (ISAKMP SA) is established by the exchange in this stage. In the second stage, security channel established in phase 1 will be used to negotiate specific Security Association for IPSec and establish IPSec SA. IPSec SA will be used for final IP data security transmission.

The relation between IKE and IPSec is shown in the following figure.

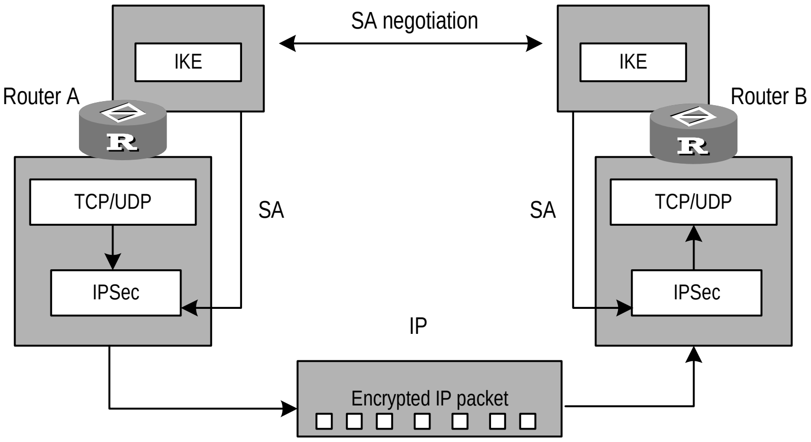


Figure 8-1 Relation between IKE and IPSec

In addition to other applications, IKE supports IKE aggressive mode and NAT traversal.

I. IKE aggressive mode

ADSL and dial-up mode are two solutions widely adopted at present in VPN construction. In these two solutions, there is an exceptional case where IP addresses of the devices at central office end are static and the IP addresses of the devices at subscriber end are dynamic. In order to support the application in this special case, aggressive mode is introduced in IKE negotiation. This mode allows IKE to search for the pre-shared key of the negotiation initiator by the IP address or ID of the negotiation initiator to accomplish the negotiation. Compared to the main mode, IKE aggressive mode allows of more flexibility and supports IKE negotiation even when the IP address of the initiator is dynamic.

II. NAT traversal

If there is a NAT GW on the VPN tunnel set up via IPSec/IKE and if this GW performs NAT on the VPN service data, you must configure the NAT traversal function for IPSec/IKE. With this function, the IKE negotiation will not authenticate the UDP port number. At the same time, traversal allows NAT GW discovery on the VPN tunnel. If a NAT GW is discovered, UDP encapsulation will be used in the subsequent IPSec data transmission, i.e., encapsulating IPSec packets in the UDP connection tunnel for IKE negotiation), to prevent the NAT GW from modifying the IPSec packets. That is, the NAT GW will change the outermost IP and UDP headers but leave the IPSec packets encapsulated in the UDP packets intact, thus ensuring the integrity of the IPSec packets. The authentication process of an IPSec data encryption/decryption requires the IPSec packet to arrive at the destination intact. At present, NAT traversal is available only in aggressive mode.

Usually IKE aggressive mode and NAT traversal are used together in an ADSL + IPSec network to solve the problems resulted from dynamic IP addresses on broadband-access enterprise networks and NAT traversal on the public network. The combination of these two features provides a security solution for substituting the ADSL broadband access for the original leased line access.

III. IKE multi-instance

IKE multi-instance enables multiple CEs to perform IKE negotiation with a PE. In conjunction with IPSec, IKE multi-instance allows the VPN-instance associated interfaces between a PE and multiple CEs to implement IPSec/IKE multi-instance.

When a CE initiates an IKE negotiation, it sends an IP packet that carries VPN instance information to the PE. The PE acquires the VPN instance information from the received negotiation packet and saves the VPN ID. When the PE sends back a negotiation, it adds this VPN ID to the IP packet and then forwards the packet to the IP layer. The IP layer then forwards the packet according to the VPN routing table to the intended CE.

8.1.2 Preparation for IKE Configuration

Prior to IKE configuration, user needs to specify following subjects, so as to smooth the configuration process:

- Make clear of algorithm strength for IKE exchange process, i.e., security protection strength (including identity authentication method, encryption algorithm, and authentication-algorithm algorithm, DH algorithm). There are different algorithm strengths. The higher strength the algorithm has, the harder it is to decrypt the protected data, but more calculation resource will be consumed. Generally, the longer the shared secret is, the higher the algorithm strength is.
- Make sure of the identity authentication key of both sides in communication.

8.2 IKE Configuration

IKE configuration includes:

1) Set a name for the local security GW
2) Define IKE proposal

- Establish IKE Proposal
- Select encryption algorithm
- Select authentication method
- Select authentication algorithm
- Select Diffie-Hellman Group ID
- Set lifetime of ISAKMP SA (optional)

3) Configure IKE peer

- Create an IKE peer
- Configure IKE negotiation mode
- Configure identity authentication key (pre-shared key)
- Configure ID type in IKE negotiation
- Specify ID of the remote security GW
- Configure IP addresses for local and remote security GWs
- Configure NAT traversal
- Configure subnet type of the IKE peer

4) Configure the parameters of Keepalive timer

- Configure interval for Keepalive transmission
- Configure timeout time for Keepalive

The term “security GW” here refers to the device configured with IPSec/IKE. It can be a GW or a router.

8.2.1 Setting a Name for the Local Security GW

If the initiator uses the GW name in IKE negotiation (that is, **id-type name** is used), you must configure the **ike local-name** command on the local device.

Perform the following configuration in system view.

Table 8-1 Configure name of the local security GW

Operation	Command
Configure name of the local security GW.	**ike local-name** *name*
Restore the default name of the local security GW.	**undo ike local-name**

8.2.2 Defining IKE Proposal

I. Establishing IKE Proposal

IKE proposal defines a set of attributes describing how IKE negotiation conducts security communications. Configuring an IKE proposal includes the tasks of IKE proposal creation, selection in encryption algorithm, authentication mode, authentication algorithm, and Diffie-Hellman group ID, and SA lifetime duration setting.

In main mode, you may create multiple IKE proposals based on precedence; negotiation can succeed so long as the negotiating parties agree on one IKE proposal.

In aggressive mode, the negotiation initiator uses only the IKE proposal with the highest precedence to negotiate with its peer. If the peer has a match, negotiation succeeds; if otherwise, the negotiation fails. The initiator will not use an IKE proposal with a lower precedence to make another negotiation attempt.

This configuration is used to define an IKE proposal. The IKE proposal configured is used to establish the security channel.

Perform the following configuration in the system view.

Table 8-2 Establish IKE proposal

Operation	Command
Create IKE proposal	**ike proposal** *proposal-number*
Delete IKE proposal	**undo ike proposal** *proposal-number*

Execute the **ike proposal** command to enter the IKE proposal view, where you can configure the encryption algorithm, authentication algorithm, Diffie-Hellman group ID, sa duration, and authentication method.

The parameter *proposal-number* is the IKE proposal number, ranging from 1 to 100. This parameter also stands for the priority. A smaller number stands for a higher priority. You can create multiple IKE proposals for each side of the negotiation. Both sides in the negotiation match the proposal from the one with the higher priority. There must be at least one matched policy for successful negotiation, that is, both side must have the same encryption and authentication algorithm, some authentication method and Diffie-Hellman group ID.

The system provides a default IKE proposal, which has the lowest priority and has the default encryption algorithm, authentication algorithm, Diffie-Hellman group ID, SA duration, and authentication method. The parameters needed by an IKE proposal are as follows.

II. Selecting Encryption Algorithm

This configuration is used to specify an encryption algorithm used by an IKE proposal.

Perform the following configuration in IKE proposal view.

Table 8-3 Select encryption algorithm

Operation	Command
Select encryption algorithm	**encryption-algorithm** { **des-cbc** | **3des-cbc** | **aes-cbc** [**128** |**192** |**256**] }
Set the encryption algorithm to the default value	**undo encryption-algorithm**

By default, the 56-bit DES algorithm in CBC mode is adopted.

III. Selecting authentication method

IKE authentication has two algorithms: pre-shared-key and PKI (rsa-signature).

Perform the following configuration in IKE proposal view.

Table 8-4 Specify authentication method

Operation	Command
Specify authentication method	**authentication-method** { **pre-share** | **rsa-signature** }
Restore the authentication method to the default value	**undo authentication-method**

IV. Selecting Authentication-algorithming Algorithm

This configuration is used to specify the authentication algorithm used by an IKE proposal.

Perform the following configuration in IKE proposal view.

Table 8-5 Select authentication algorithm

Operation	Command
Select authentication algorithm	**authentication-algorithm** { **md5** | **sha** }
Set authentication algorithm to the default value	**undo authentication-algorithm**

By default SHA-1 authentication algorithm is adopted.

V. Selecting Diffie-Hellman Group ID

This configuration is used to specify the Diffie-Hellman group ID used by an IKE proposal.

Perform the following configuration in IKE proposal view.

Table 8-6 Select Diffie-Hellman group ID

Operation	Command
Select Diffie-Hellman group ID	**dh** { **group1** | **group2** | **dh-group5** | **dh-group14** }
Restore the default value of Diffie-Hellman group ID	**undo dh**

By default, 768-bit Diffie-Hellman group (group 1) is selected.

VI. Configuring lifetime of ISAKMP SA (optional)

This configuration is used to specify the lifetime of ISAKMP SA used by an IKE proposal.

Perform the following configuration in IKE proposal view.

Table 8-7 Set sa duration of IKE SA

Operation	Command
Configure lifetime of IKE SA.	**sa duration** *seconds*
Restore the default lifetime.	**undo sa duration**

If **sa duration** expires, the ISAKMP SA will automatically update. The SA lifetime can be set as one number between 60 and 604800 seconds. As the time spent calculating DH during IKE negotiation is long on a low-end router, consider to set the **sa duration** greater than 10 minutes to prevent ISAKMP SA updates from affecting security communication.

The SA will negotiate another one to replace the old SA before the set SA duration is exceeded. The starting time of the soft timeout is 90% of the SA duration timeout. The old SA will be cleared automatically when the SA duration is exceeded, which can be called hard timeout.

By default, the ISAKMP SA duration is 86400 seconds (a day).

8.2.3 Configuring IKE Peer

I. Creating an IKE peer

Perform the following configuration in system view.

Table 8-8 Configure IKE peer

Operation	Command
Configure an IKE peer and access the IKE peer view.	**ike peer** *peer-name*
Delete the IKE peer.	**undo ike peer** *peer-name*

II. Configuring IKE negotiation mode

Perform the following configuration in IKE-peer view.

Table 8-9 Configure negotiation mode

Operation	Command
Configure IKE negotiation mode.	**exchange-mode** { **aggressive** | **main** }
Restore the default IKE negotiation mode.	**undo exchange-mode**

By default, the main mode is adopted.

🕮 **Note:**

If the IP address of one end of a security tunnel is dynamic, you must adopt the aggressive mode for IKE negotiation.

III. Configuring pre-shared key

Perform the following configuration in IKE-peer view.

Table 8-10 Configure pre-shared key

Operation	Command
Configure a pre-shared key for IKE negotiation.	**pre-shared-key** *key*
Remove the pre-shared key used in IKE negotiation.	**undo pre-shared-key**

IV. Configuring ID type in IKE negotiation

Perform the following configuration in IKE-peer view.

Table 8-11 Configure ID type in IKE negotiation

Operation	Command
Select ID type in the IKE negotiation.	**id-type** { **ip** | **name** }
Restore the default ID type in the IKE negotiation.	**undo id-type**

By default, IP address is taken as the ID in IKE negotiation.

In main mode, only IP address can be taken as the ID in IKE negotiation. In aggressive mode, however, you may use either IP address or name as the ID in IKE negotiation.

V. Specifing ID of the remote security GW

If the initiator uses its GW name in IKE negotiation (that is, **id-type name** is used), it sends the name to the peer as its identity, whereas the peer uses the username configured using the **remote-name** *name* command to authenticate the initiator. To pass authentication, this remote name must be the same one configured using the **ike local-name** command on the gateway at the initiator end.

Perform the following configuration in IKE-peer view.

Table 8-12 Specify ID of the remote security GW

Operation	Command
Specify a remote security GW.	**remote-name** *name*
Remove ID of the remote security GW.	**undo remote-name**

VI. Configuring IP addresses of the local and remote security GWs

During an IKE negotiation, the initiator sends its IP address as its identity to the peer if the **id-type ip** command is configured. The peer then uses the address or address range configured with the **remote-address** command to authenticate the initiator. To guarantee a successful authentication, you must make sure that the IP address configured with the **local-address** command on the initiator is the same address or within the address range configured with the **remote-address** command.

Perform the following configuration in IKE-peer view.

Table 8-13 Configure IP address of security GWs

Operation	Command
Configure IP address of the local security GW	**local-address** *ip-address*
Delete IP address of the local security GW	**undo local-address**
Configure IP address of the remote security GW.	**remote-address** *ip-address1* [*ip-address2*]
Delete the IP address of the remote security GW.	**undo remote-address**

Generally speaking, you do not need to configure the **local-address** command unless you want to specify a special address for the local GW (such as the address of loopback interface).

VII. Configuring NAT traversal

The NAT traversal function must be configured so long as there is a NAT IPSec device on the VPN tunnel constructed using IPSec/IKE.

Perform the following configuration in IKE-peer view.

Table 8-14 Configure the NAT traversal function of IPSec/IKE

Operation	Command
Enable the NAT traversal function of IPSec/IKE	**nat-traversal**
Disable the NAT traversal function of IPSec/IKE	**undo nat-traversal**

To save IP address space, ISPs often deploy NAT gateways on public networks so that private IP addresses can be allocated to users. The likelihood thus exists that at one end of an IPSec/IKE tunnel is a public address and at the other end is a private one. To set up the tunnel in this case, you must configure NAT traversal at both private network side and public network side.

Note:

At present, NAT traversal is available in IKE aggressive mode but not in main mode.

VIII. Configuring the NAT keepalive interval for IKE peers

Perform the following configuration in system view.

Table 8-15 Configure the NAT keepalive interval for IKE peers

Operation	Command
Configure the NAT keepalive interval for IKE peers	**ike sa nat-keepalive-timer interval** *seconds*
Disable NAT keepalive for IKE peers	**undo ike sa nat-keepalive-timer interval**

By default, NAT keepalive of IKE peers is disabled.

You may configure IKE peers to send NAT Keepalive messages which are encapsulated in UDP packets without being encrypted, to maintain validity of dynamic NAT mappings between IKE peers on NAT gateways. These messages however cannot check the state of IKE peers.

When configuring a NAT keepalive interval for IKE peers, make sure that it is less than the translation timeout of NAT.

IX. Configuring subnet type of the IKE peer

You can use these two commands only when your router is interoperable with a Netscreen device.

Perform the following configuration in IKE-peer view:

Table 8-16 Configure subnet type of the IKE peer

Operation	Command
Configure subnet type of the local GW	**local** { **multi-subnet** | **single-subnet** }
Restore the default subnet type of the local GW	**undo local**
Configure subnet type of the peer GW	**peer** { **multi-subnet** | **single-subnet** }
Restore the default subnet type of the peer GW	**undo peer**

The default is **single-subnet**.

8.2.4 Configuring Keepalive Timer

I. Configuring keepalive interval

Configure time interval for ISAKMP SA to transmit hold packet to the peer.

Perform the following configuration in system view.

Table 8-17 Configure time interval for Keepalive packet transmission

Operation	Command
Configure time interval for ISAKMP SA to transmit Keepalive packet to the peer	**ike sa keepalive-timer interval** *seconds*
Disable the above function	**undo ike sa keepalive-timer interval**

IKE will maintain the ISAKMP SA link state through this packet. Generally, if the peer has used the **ike sa keepalive-timer timeout** command to configure timeout time, this Keepalive interval must be configured on local end. When the peer did not receive this Keepalive packet within configured timeout time, this ISAKMP SA and its corresponding IPSec SA will be deleted. Therefore, the configured timeout time should be longer than Keepalive packet transmission time.

By default, this function is invalid.

II. Configuring keepalive timeout time

Configure timeout time for ISAKMP SA waiting for Keepalive packet.

Perform the following configuration in system view.

Table 8-18 Configure timeout waiting time for Keepalive packet

Operation	Command
Configure ISAKMP SA timeout time for waiting Keepalive packet	**ike sa keepalive-timer timeout** *seconds*
Disable this function	**undo ike sa keepalive-timer timeout**

IKE maintains this ISAKMP SA link status through this packet. If the peer Keepalive packet is not received within configured timeout time, the ISAKMP SA and its corresponding IPSec SA will be deleted. Therefore, configured timeout time should be longer than Keepalive packet transmission time.

On the network, packet loss will rarely exceed 3 times, so timeout time can be configured to be 3 times as long as Keepalive packet transmission time interval of the peer.

By default, this function is invalid.

8.3 Displaying and Debugging IKE

After the above configuration, execute **display** command in all views to display the running of the IKE configuration, and to verify the effect of the configuration.

Execute **debugging** and **reset** commands in user view.

Table 8-19 Display and debug IKE

Operation	Command
Display the current established security channel	**display ike sa [verbose]**
Display the parameters of each IKE proposal configuration.	**display ike proposal**
Display the configuration of IKE peers	**display ike peer**
Delete a security channel	**reset ike sa** [*connection-id*]
Enable the information debugging of IKE	**debugging ike** { **all** | **error** | **exchange** | **message** | **misc** | **transport** }
Disable the information debugging of IKE	**undo debugging ike** { **all** | **error** | **exchange** | **message** | **misc**| **transport** }

You can delete a specified security channel by specifying SA *connection-id* which can be displayed by executing the **display ike sa** command. So far as the same security channel (that is, the same remote end) is concerned, the *connection-id* information includes the information at stage 1 and the information at stage 2.

If the ISAKMP SA at stage 1 still exists when you deleting the local SA, the system will send the DELETE message in the protection mode of the ISAKMP SA to notify the peer to clear the SA database.

If no connection-id is specified, all the SAs at stage 1 will be removed.

Security channel and SA are totally different concepts. Security channel is a channel via which its two endpoints can make bidirectional communications but IPSec SA is just a unidirectional connection. In other words, security channel comprises a pair or several pairs of SAs.

8.4 Typical Configuration of IKE

8.4.1 Typical IKE Configuration Example

I. Network requirements

- Hosts 1 and 2 communicate securely, and a security channel is established with IKE automatic negotiation between security GWs A and B.
- Configure an IKE proposal assigned with the priority level 10 on the security GW A and apply the default IKE proposal on the security GW B.
- Configure authentication key for the proposal using the pre-shared key authentication method.

II. Network diagram

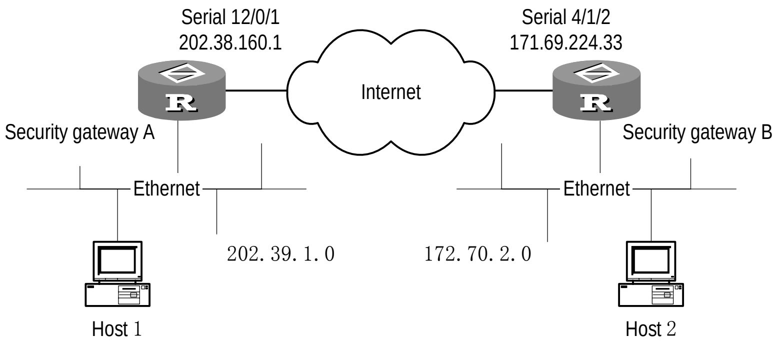


Figure 8-2 Network diagram of IKE configuration example

III. Configuration procedure

1) Make the following configurations on the security GW A:

# Configure an IKE peer.

```
[3Com] ike peer peer
[3Com-ike-peer-peer] pre-shared-key abcde
[3Com-ike-peer-peer] remote-address 171.69.224.33
```

# Configure an IKE proposal 10.

```
[3Com] ike proposal 10
```

# Set the authentication algorithm used by the IKE proposal to MD5.

```
[3Com-ike-proposal-10] authentication-algorithm md5
```

# Apply the pre-shared key authentication mode.

```
[3Com-ike-proposal-10] authentication-method pre-share
```

# Set the lifetime duration of ISAKMP SA to 5000 seconds.

```
[3Com-ike-proposal-10] sa duration 5000
```

2) Make the following configurations on the security GW B:

# Configure an IKE peer.

```
[3Com] ike peer peer
[3Com-ike-peer-peer] pre-shared-key abcde
[3Com-ike-peer-peer] remote-address 202.38.160.1
```

The configurations made above can ensure the proper IKE negotiation between GWs A and B. As GW A is configured with proposal 10 and **authentication-algorithm md5** but GW B is configured with only a default IKE proposal and **authentication-algorithm sha**, GW B will not have a proposal matching the IKE proposal 10 configured on GW A. For this reason, the system will find only a match, that is, the default IKE proposal for the both parties when it makes the match operation in proposals starting from the one with the highest priority. In addition, no match operation will be done on **duration** in the proposal matching process, as the lifetime is decided by the initiator of IKE negotiation.

For more information about the IPSec configurations, see “Section 7.4 Typical IPSec Configuration Examples”.

8.4.2 IKE Aggressive Mode and NAT Traversal Configuration Example

I. Network requirements

- The LAN of a company branch is connected to the company intranet via a leased line. The S0/0/0 interface of RouterA has a fixed IP address and Router B obtains IP address from an ISP dynamically.
- As the IP address obtained by the branch is a private one and the IP address of the S0/0/0 interface on Router A is a public address, you must enable NAT traversal on both Router A and Router B.
- To ensure information security, IPSec/IKE is adopted to create a security tunnel.

Note:

For the purpose of highlighting the configurations of IKE aggressive mode and NAT traversal function, Routers in this example are interconnected via their serial interfaces across the Internet and one end is configured to obtain IP address dynamically. You can refer to this example if you access the Internet using dial-up or broadband service.

II. Network diagram

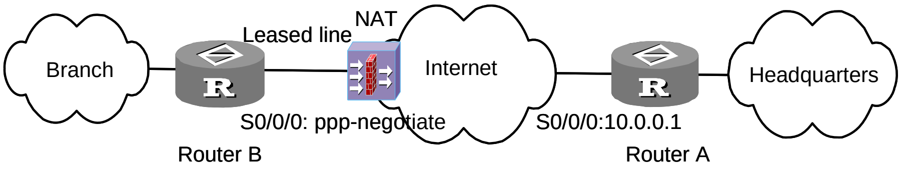


Figure 8-3 Network diagram for IKE aggressive mode and NAT traversal

III. Configuration procedure

1) Configure Router A:

# Set a name for the local security GW.

```
[RouterA] ike local-name routera
```

# Configure ACL.

```
[RouterA] acl number 3101 match-order auto
[RouterA-acl-adv-3101] rule permit ip source any destination any
[RouterA -acl-adv-3101] quit
```

# Configure an IKE peer.

```
[RouterA] ike peer peer
[RouterA -ike-peer-peer] exchange-mode aggressive
[RouterA -ike-peer-peer] pre-shared-key abc
[RouterA -ike-peer-peer] id-type name
[RouterA -ike-peer-peer] remote-name routerb
[RouterA -ike-peer-peer] nat traversal
[RouterA -ike-peer-peer] quit
```

# Create an IPSec proposal “prop”.

```
[RouterA] ipsec proposal prop
[RouterA-ipsec-proposal-prop] encapsulation-mode tunnel
[RouterA-ipsec-proposal-prop] transform esp
[RouterA-ipsec-proposal-prop] esp encryption-algorithm des
[RouterA-ipsec-proposal-prop] esp authentication-algorithm sha1
```

```
[RouterA-ipsec-proposal-prop] quit
```

# Create security policy and specify SA establishment via IKE negotiation.

```
[RouterA] ipsec policy policy 10 isakmp
```

# Create an IPSec policy and reference the IKE peer in the policy.

```
[RouterA-ipsec-policy-isakmp-policy-10] ike-peer peer
```

# Reference the ACL 3101 in the IPSec policy.

```
[RouterA-ipsec-policy-isakmp-policy-10] security acl 3101
```

# Reference the IPSec proposal “prop” in the IPSec policy.

```
[RouterA-ipsec-policy-isakmp-policy-10] proposal prop
[RouterA-ipsec-policy-isakmp-policy-10] quit
```

# Access the serial interface S0/0/0 and configure its IP address.

```
[RouterA] interface Serial0/0/0
[RouterA -Serial0/0/0] ip address 10.0.0.1 255.255.0.0
```

# Apply the IPSec policy group “policy” on the serial interface S0/0/0.

```
[RouterA-Serial0/0/0] ipsec policy policy
[RouterA-Serial0/0/0] remote address pool 1
```

2) Configure Router B:

# Set a name for the local security GW.

```
[RouterB] ike local-name routerb
```

# Configure ACL.

```
[RouterB] acl number 3101 match-order auto
[RouterB-acl-adv-3101] rule permit ip source any destination any
[RouterB-acl-adv-3101] quit
```

# Configure an IKE peer.

```
[RouterB] ike peer peer
[RouterB-ike-peer-peer] exchange-mode aggressive
[RouterB-ike-peer-peer] pre-shared-key abc
[RouterB-ike-peer-peer] id-type name
[RouterB-ike-peer-peer] remote-ip 10.0.0.1
[RouterB-ike-peer-peer] remote-name routera
[RouterB-ike-peer-peer] nat traversal
[RouterB -ike-peer-peer] quit
```

# Create an IPSec proposal “prop”.

```
[RouterB] ipsec proposal prop
[RouterB-ipsec-proposal-prop] encapsulation-mode tunnel
[RouterB-ipsec-proposal-prop] transform esp
[RouterB-ipsec-proposal-prop] esp encryption-algorithm des
[RouterB-ipsec-proposal-prop] esp authentication-algorithm sha1
```

```
[RouterB-ipsec-proposal-prop] quit
```

# Create an IPSec policy and specify to set up SA by means of IKE negotiation.

```
[RouterB] ipsec policy policy 10 isakmp
```

# Reference the IKE peer in the IPSec policy.

```
[RouterB-ipsec-policy-isakmp-policy-10] ike-peer peer
```

# Reference the ACL 3101 in the IPSec policy.

```
[RouterB-ipsec-policy-isakmp-policy-10] security acl 3101
```

# Reference the IPSec proposal “prop” in the IPSec policy.

```
[RouterB-ipsec-policy-isakmp-policy-10] proposal prop
[RouterB-ipsec-policy-isakmp-policy-10] quit
```

# Access the serial interface S0/0/0 and assign a dynamic IP address to the interface.

```
[RouterB] interface Serial0/0/0
[RouterB-Serial0/0/0] ip address ppp-negotiate
```

# Apply the IPSec policy group “policy” on the serial interface S0/0/0.

```
[RouterB-Serial0/0/0] ipsec policy policy
```

8.4.3 ADSL+IPSec/IKE Configuration Example

I. Network requirements

The following is a typical example of using IPSec with ADSL.

As shown in Figure 8-4,

- Router B is connected to the DLSAM access side of the public network directly through ADSL to work as the client of PPPoE. As Router B can obtain only private addresses from its ISP, you need to configure NAT traversal on both Router A and Router B.
- The headquarters LAN is connected to the ATM network through Router A.
- To ensure information security, IPSec/IKE is adopted to create a security tunnel.

II. Network diagram

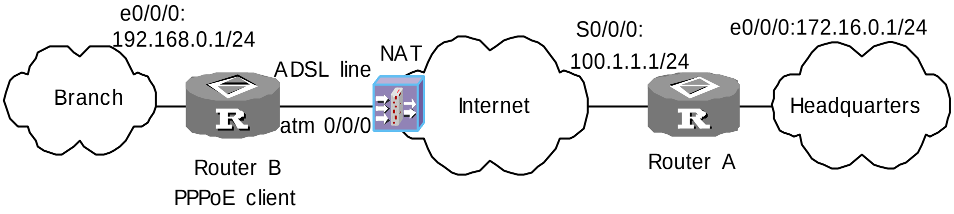


Figure 8-4 Network diagram for use of IPSec/IKE on ADSL

III. Configuration procedure

1) Configure Router A

# Assign a name to the local security gateway.

```
<RouterA> system-view
[RouterA] ike local-name routera
```

# Configure an ACL.

```
[RouterA] acl number 3101
[RouterA-acl-adv-3101]  rule  0  permit  ip  source  172.16.0.0  0.0.0.255
destination 192.168.0.0 0.0.0.255
[RouterA-acl-adv-3101] quit
```

# Configure an IKE proposal.

```
[RouterA] ike proposal 1
[RouterA-ike-proposal-1] authentication-algorithm sha
[RouterA-ike-proposal-1] authentication-method pre-share
[RouterA-ike-proposal-1] encryption-algorithm 3des-cbc
[RouterA-ike-proposal-1] dh group2
```

# Configure an IKE peer.

```
[RouterA] ike peer peer
[RouterA-ike-peer-peer] exchange-mode aggressive
[RouterA-ike-peer-peer] pre-shared-key abc
[RouterA-ike-peer-peer] id-type name
[RouterA-ike-peer-peer] remote-name routerb
[RouterA-ike-peer-peer] nat traversal
[RouterA-ike-peer-peer] quit
```

# Create IPSec proposal prop.

```
[RouterA] ipsec proposal prop
[RouterA-ipsec-proposal-prop] encapsulation-mode tunnel
[RouterA-ipsec-proposal-prop] transform esp
[RouterA-ipsec-proposal-prop] esp encryption-algorithm 3des
[RouterA-ipsec-proposal-prop] esp authentication-algorithm sha1
[RouterA-ipsec-proposal-prop] quit
```

# Create an IPSec policy and specify to set up SAs through IKE negotiation.

```
[RouterA] ipsec policy policy 10 isakmp
```

# Reference the IKE peer named peer in the IPSec policy.

```
[RouterA-ipsec-policy-isakmp-policy-10] ike-peer peer
```

# Reference ACL 3101 in the IPSec policy.

```
[RouterA-ipsec-policy-isakmp-policy-10] security acl 3101
```

# Reference the IPSec proposal prop in the IPSec policy.

```
[RouterA-ipsec-policy-isakmp-policy-10] proposal prop
[RouterA-ipsec-policy-isakmp-policy-10] quit
```

# Assign an IP address to interface Serial 0/0/0.

```
[RouterA] interface Serial0/0/0
[RouterA-Serial0/0/0] ip address 100.1.1.1 255.255.255.0
[RouterA-Serial0/0/0] ipsec policy policy
[RouterA-Serial0/0/0] quit
```

# Configure interface Ethernet 0/0/0.

```
[RouterA] interface Ethernet0/0/0
[RouterA-Ethernet0/0/0] ip address 172.16.0.1 255.255.255.0
[RouterA-Ethernet0/0/0] quit
```

# Configure a static route to the LAN of the branch.

```
[RouterA] ip route-static 192.168.0.0 255.255.255.0 Serial0/0/0
```

2) Configure on Router B

# Assign a name to the local security gateway.

```
<RouterB> system-view
[RouterB] ike local-name routerb
```

# Create a dialer rule

```
[RouterB] dialer-rule 1 ip permit
```

# Configure an ACL.

```
[RouterB] acl number 3101
[RouterB-acl-adv-3101]  rule  0  permit  ip  source  192.168.0.0  0.0.0.255
destination 172.16.0.0 0.0.0.255
[RouterB-acl-adv-3101] quit
```

# Configure an IKE proposal.

```
[RouterB] ike proposal 1
[RouterB-ike-proposal-1] authentication-algorithm sha
[RouterB-ike-proposal-1] authentication-method pre-share
[RouterB-ike-proposal-1] encryption-algorithm 3des-cbc
[RouterB-ike-proposal-1] dh group2
```

# Configure an IKE peer.

```
[RouterB] ike peer peer
[RouterB-ike-peer-peer] exchange-mode aggressive
[RouterB-ike-peer-peer] pre-shared-key abc
[RouterB-ike-peer-peer] id-type name
[RouterB-ike-peer-peer] remote-name routera
[RouterB-ike-peer-peer] remote-address 100.1.1.1
[RouterB-ike-peer-peer] nat traversal
[RouterB-ike-peer-peer] quit
```

# Create IPSec proposal prop.

```
[RouterB] ipsec proposal prop
[RouterB-ipsec-proposal-prop] encapsulation-mode tunnel
[RouterB-ipsec-proposal-prop] transform esp
[RouterB-ipsec-proposal-prop] esp encryption-algorithm 3des
[RouterB-ipsec-proposal-prop] esp authentication-algorithm sha1
[RouterB-ipsec-proposal-prop] quit
```

# Create an IPSec policy and specify to set up SAs through IKE negotiation.

```
[RouterB] ipsec policy policy 10 isakmp
```

# Reference the IKE peer named peer in the IPSec policy.

```
[RouterB-ipsec-policy-isakmp-policy-10] ike-peer peer
```

# Reference ACL 3101 in the IPSec policy.

```
[RouterB-ipsec-policy-isakmp-policy-10] security acl 3101
```

# Reference the IPSec proposal prop in the IPSec policy.

```
[RouterB-ipsec-policy-isakmp-policy-10] proposal prop
[RouterB-ipsec-policy-isakmp-policy-10] quit
```

# Create a dialer rule.

```
[RouterB] dialer-rule 1 ip permit
```

# Create interface Dialer 0, and configure its MTU and settings allowing the username and password assigned by the ISP to be used for dial and PPP authentication.

```
[RouterB] interface Dialer0
[RouterB-Dialer0] link-protocol ppp
[RouterB-Dialer0] ppp pap local-user test password simple 123456
[RouterB-Dialer0] ip address ppp-negotiate
[RouterB-Dialer0] dialer-group 1
[RouterB-Dialer0] dialer bundle 1
[RouterB-Dialer0] ipsec policy policy
[RouterB-Dialer0] mtu 1492
[RouterB-Dialer0] quit
```

# Configure a static route to interface Dialer 0.

```
[RouterB] ip route-static 172.16.0.0 255.255.0.0 Dialer 0
```

# Configure Ethernet interface 0/0/0.

```
[RouterB] interface Ethernet0/0/0
[RouterB-Ethernet0/0/0] tcp mss 1450
[RouterB-Ethernet0/0/0] ip address 192.168.0.1 255.255.255.0
[RouterB-Ethernet0/0/0] quit
```

# Configure the ATM interface on the ADSL card.

```
[RouterB] interface Atm1/0/0
```

```
[RouterB-Atm1/0/0] pvc 0/100
[RouterB-atm-pvc-Atm1/0/0-0/100] map bridge Virtual-Ethernet0
[RouterB-atm-pvc-Atm1/0/0-0/100] quit
```

# Create and configure the VE interface.

```
[RouterB] interface virtual-ethernet0
[RouterB-Virtual-Ethernet0] pppoe-client dial-bundle-number 1
[RouterB-Virtual-Ethernet0] mac-address 0011-0022-0012
```

8.5 IKE Fault Diagnosis and Troubleshooting

When configuring parameters to establish IPSec security channel, you can enable the Error debugging of IKE to help us find configuration problems. The command is as follows:

```
<3Com> debugging ike error
```

Symptom 1: Invalid user ID information

Troubleshooting: User ID is the data that the user initiating the IPSec communication uses to identify itself. In actual applications, you can make use of user ID to set up different security channels for various types of data traffic for the sake of protection. In the implementation of 3Com Corporation, a user is so far identified by its IP address.

Following is the debugging information you may view on the screen:

```
got NOTIFY of type INVALID_ID_INFORMATION
```

Or

```
drop message from A.B.C.D due to notification type INVALID_ID_INFORMATION
```

Check whether the ACLs of the IPSec policies configured on the interfaces at both ends of the negotiation are compatible. The user is recommended to configure the ACLs to mirror each other. For more information about ACL mirror, refer to Section Configure ACL in IPSec Configuration.

Symptom 2: Proposal mismatch

Troubleshooting:

Following is the debugging information you may view on the screen:

```
got NOTIFY of type NO_PROPOSAL_CHOSEN
```

Or

```
drop message from A.B.C.D due to notification type NO_PROPOSAL_CHOSEN
```

The two parties of the negotiation have no matched proposal. For the negotiation at stage 1, you can look up the IKE proposals for a match. For the negotiation at stage 2, you can check whether the parameters of the IPSec polices applied on the interfaces are matched, and whether the referenced IPSec proposals have a match in protocol, encryption and authentication algorithms.

Symptom 3: Unable to establish security channel

Troubleshooting: Check whether the network is stable and the security channel is established correctly. Sometimes there is a security channel but there is no way to communicate, and ACL of both parties are found correctly configured, and there is also matched policy.

In this case, the problem is usually caused by the restart of one router after the security channel is established. Solution:

- Use the command **display ike sa** to check whether both parties have established SA of Phase 1.
- Use the command **display ipsec sa policy** to check whether the ipsec policy on interface has established IPSec SA.
- If the above two results display that one party has SA but the other does not, then use the command **reset ike sa** to clear SA with error and re-originate negotiation.

Chapter 9 PKI Configuration

9.1 PKI Overview

9.1.1 Introduction

Public key infrastructure (PKI) is a system which uses public key technology and digital certificate to protect system security and authenticates digital certificate users. It provides a whole set of security mechanism by combining software/hardware systems and security policies together. PKI uses certificates to manage public keys: It binds user public keys with other identifying information through a trustworthy association, so that online authentication is possible. PKI provides safe network environment and enables an easy use of encryption and digital signature technologies under many application environments, to assure confidentiality, integrity and validity of online data.

A PKI system consists of public key algorithm, certificate authority, registration authority, digital certificate, and PKI repository.

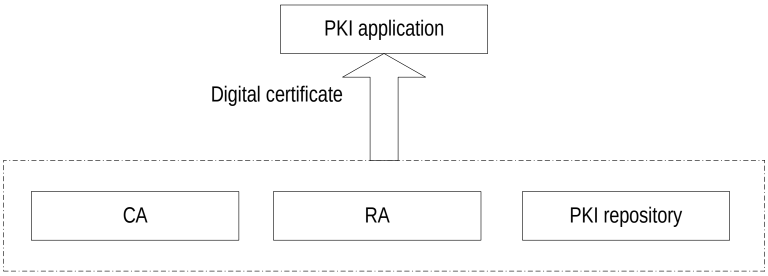


Figure 9-1 PKI components block diagram

Certificate authority issues and manages certificates. Registration authority authenticates user identity and manages certificate revocation list. PKI repository stores and manages such information as certificates and logs, and provides query function. Digital certificate, also called Public Key Certificate (PKC), underlies the security of PKI system and the trust in application. Adopting an authentication technology based on public key technology, it is a file duly signed by certificate authority that contains public key and owner information. It can be used as an identity proof for online information exchange and commercial activities. A certificate has its lifetime, which is specified in issuing. Of course, certificate authority can revoke a certificate before its expiration date.

9.1.2 Terminology

- Public key algorithm: Key algorithm that involves different encryption key and decryption key. A pair of keys are generated for each user: One is publicized as public key; the other is reserved as private key. The information encrypted by one key has to be decrypted by the other; the key pair therefore is generally used in signature and authentication. In communication, if the sender signs with its private key, the receiver needs to authenticate this signature with the sender's public key. If the sender encrypt the information with the receiver's public key, then only the receiver's private is capable of decryption.
- Certificate authority (CA): Trustworthy entity issuing certificates to persons, PCs or any other entities. CA deals with certificate requests, and checks applicant information according to certificate management policy. Then it signs the certificate with its private key and issues the certificate.
- Registration authority (RA): Extension of CA. It forwards the entities' certificate requests to CA, and digital certificates and certificate revocation list to directory server, for directory browsing and query.
- Light-weight directory access protocol (LDAP) server: LDAP provides a means to access PKI repository, with the purpose of accessing and managing PKI information. LDAP server supports directory browsing and enlists the user information and digital certificates from a RA server. Then the user can get his or others' certificates when accessing the LDAP server.
- Certificate revocation list (CRL): A certificate has its lifetime, but CA can revoke a certificate before its expiration date if the private key leaks or if the service ends. Once a certificate is revoked, a CRL is released to announce its invalidity, where lists a set of serial numbers of invalid certificates. CRL, stored in LDAP server, provides an effective way to check the validity of certificates, and offers centralized management of user notification and other applications.

9.1.3 Applications

PKI includes a set of security services using the technologies of public key and X.509 certification in distributed computing systems. It can issue certificates for various purposes, such as Web user identity authentication, Web server identity authentication, secure Email using S/MIME (secure/multipurpose internet mail extensions), virtual private network (VPN), IP Security, Internet key exchange (IKE), and secure sockets layer/transaction layer security (SSL/TLS). One CA can issue certificates to another CA, to establish certification hierarchies.

9.1.4 Configuration Task List

PKI configuration includes applying to CA for a local certificate for a designated device and authenticating validity of the certificate. The configuration involves:

- PKI certificate request
- PKI certificate validation
- Display and debug

9.2 Certificate Request Configuration

9.2.1 Certificate Request Overview

Certificate request is a process when an entity introduces itself to CA. The identity information the entity provides will be contained in the certificate issued later. CA uses a set of criteria to check applicant creditability, request purpose and identity reliability, to ensure that certificates are bound to correct identity. Offline and non-auto out-of-band (phone, storage disk and Email, for example) identity checkup may be required in this process. If this process goes smoothly, CA issues a certificate to the user and displays it along with some public information on the LDAP server for directory browsing. The user can then download its own public-key digital certificate from the notified position, and obtain those of others through the LDAP server. The request process proceeds with:

- Entering PKI domain view
- Specifying a trustworthy CA
- Configuring servers for certificate request
- Configuring entity name space
- Creating a local public — private key pair
- Setting request polling interval and count
- Configuring certificate request mode
- Delivering a certificate request manually
- Retrieving a certificate

9.2.2 Entering PKI Domain View

A PKI domain manages in a unified way a group of PKI users who trust a same third trustworthy organization. That means, it suffices with the trust each member lays on CA; no trust between the group members is required. It serves a lot in relieving system load and extending the capability of PKI certificate system.

For the configuration of domain parameters, you should enter the PKI domain view.

Perform the following configuration in system view.

Table 9-1 Enter PKI domain view

Operation	Command
Enter a designated PKI domain view	**pki domain** *name*
Delete a designated PKI domain and its relative information	**undo pki domain** *name*

By default, no PKI domain is specified.

🕮 **Note:**

Typically, a device may belong to two or more PKI domains. Then independent configuration information is required for each domain. Parameter configuration in PKI domain view is for this purpose. But currently, one device supports only one PKI domain, so you need to delete the existing domain first if you want to use a new one.

9.2.3 Specifying a Trustworthy CA

Trustworthy CAs function to provide registration service and issue certificates for entities. They are essential to PKI. Only when a CA trusted by everyone is available, can users enjoy the security services with public key technology.

Perform the following configuration in PKI domain view.

Table 9-2 Specify trustworthy CA

Operation	Command
Specify a trustworthy CA	**ca identifier** *name*
Delete the trustworthy CA	**undo ca identifier**

By default, no trustworthy CA is specified.

🕮 **Note:**

The standard set CA uses in request processing, certificate issuing and revoking, and CRL releasing is called CA policy. In general, CA uses files, called certification practice statements (CPS), to advertise its policy. CA policy can be obtained in out-of-band or other mode. You should understand CA policies before choosing a CA, for different CAs may use different methods to authenticate the public key -- subject binding.

You need CA identifiers only when obtaining CA certificates but not when applying for local certificates.

9.2.4 Configuring Servers for Certificate Request

I. Configuring the entity for certificate request

An entity is required for certificate request; it is used to prove the identity to the CA.

Perform the following configuration in PKI domain view.

Table 9-3 Configure the entity for certificate request

Operation	Command
Specify the entity for certificate request	**certificate request entity** *entity-name*
Remove the entity reference relationship	**undo certificate request entity**

By default, no entity is specified for certificate request.

🕮 **Note:**

For information about the *entity-name* argument, refer to section 9.2.5 "Configuring Entity Name Space"

II. Specifying a registration organization

Registration management is often implemented by an independent registration authority (RA), which is responsible for coping with certificate request, examining entity qualification and determining for CA whether or not to issue the digital certificate. It does not issue the certificate, as is performed by CA. Sometimes no independent RA is set. It doesn't mean that registration function of PKI is disabled, since CA takes over the registration management.

Perform the following configuration in PKI domain view.

Table 9-4 Specify a registration organization

Operation	Command
Choose between CA and RA as the registration organization	**certificate request from** { **ca** | **ra** } **entity** *entity-name*
Delete the registration organization	**undo certificate request from** { **ca** | **ra** }

By default, no registration organization is specified.

PKI security policy recommends the involvement of RA.

Note:

For details about *entity-name*, refer to “Section 9.2.5 Configuring Entity Name Space”.

III. Configuring registration server location

The registration server location (i.e., URL) needs to be specified. Then entities can present to this server the certificate request using simple certification enrollment protocol (SCEP, a protocol to communicate with certification authority).

Perform the following configuration in PKI domain view.

Table 9-5 Specify registration server location

Operation	Command
Specify the location of a registration server	**certificate request url** *string*
Delete the location setting	**undo certificate request url**

By default, no registration server location is specified.

IV. Configuring LDAP server IP

Storage of entitity certificates and CRL information is essential to a PKI system. Usually, this is done using a LDAP directory server.

Perform the following configuration in PKI domain view.

Table 9-6 Specify LDAP server IP

Operation	Command
Specify the IP address of an LDAP server	**ldap-server ip** *ip-address* [**port** *port-num*] [**version** *version-number*]
Delete the IP address setting	**undo ldap-server**

By default, no IP address or port is specified for LDAP server. Currently it is LDAP version2.

V. Configuring the fingerprint for authenticating the root certificate

When receiving the identity certificate from the CA, the router needs to use the root certificate of the CA to verify the authenticity and validity of the identify certificate. When receiving the root certificate from the CA, the router needs to authenticate the fingerprint of the CA root certificate, which is a unique hashed value of the content of the root certificate. If the fingerprint of the CA root certificate is not identical to the one configured by using the command described here, the router rejects the root certificate. The fingerprint can be MD5 or SHA1 format.

Perform the following configuration in PKI domain view.

Table 9-7 Configure the fingerprint for authenticating the root certificate

Operation	Command
Configure the fingerprint for authenticating the root certificate	**root-certificate fingerprint** { **md5** | **sha1** } *string*
Delete the fingerprint for authenticating the root certificate	**undo root-certificate fingerprint**

By default, no fingerprint is configured for authenticating the root certificate.

For an MD5 fingerprint, the value of the *string* argument must consist of 32 characters and be entered in hexadecimal format. For an SHA1 fingerprint, the value of the *string* argument must consist of 40 characters and be entered in hexadecimal format.

9.2.5 Configuring Entity Name Space

I. Name space overview

Entity name space should be taken into account when setting up PKI. In a certificate, the public key and owner name must be consistent. Each CA details about an entity with the information it considers important. A unique identifier (also called DN-distinguished name) can be used to identify an entity. It consists of several parts, such as user common name, organization, country and owner name. It must be unique among the network.

The entity DN configuration in PKI entity view comprises the configuration of:

- PKI entity name
- Entity FQDN
- Country code
- State name
- Geographic locality
- Organization name
- Organization unit name
- Common name of the entity
- IP address of the entity

Note:

Entity configuration information must comply with CA certificate issue policy, for example, in determining mandatory and optional parameters. Otherwise, certificate request may be rejected.

II. Specifying a PKI entity name

In PKI entity view, you can configure the attributes of entity DN.

Perform the following configuration in system view.

Table 9-8 Specify an entity name

Operation	Command
Specify an entity name and enter the entity view	**pki entity** *name-str*
Delete the entity name and relative parameters	**undo pki entity** *name-str*

By default, no entity name is given.

Note:

The entity name must be consistent with that specified by registration organization using the **certificate request entity** *entity-name* command. Otherwise, the certificate request fails. *name-str* is just for the convenience in referencing, and appears not as a certificate field.

Windows 2000 CA server has some restrictions on data length of certificates. If the configured entity length goes beyond certain limit, the Windows 2000 CA server does not respond to certificate requests.

III. Configuring the entity FQDN

Fully qualified domain name (FQDN) is the unique identifier of the entity among the network, for example, Email address. It is often in the format of user.domain and can be resolved to IP address. FQDN is equivalent to IP address in function. This configuration is optional.

Perform the following configuration in PKI entity view.

Table 9-9 Configure the entity FQDN

Operation	Command
Configure the entity FQDN	**fqdn** *name-str*

Operation	Command
Delete the entity FQDN	**undo fqdn**

By default, no FQDN is configured for the entity.

IV. Configuring the country code for the entity

Perform the following configuration in PKI entity view.

Table 9-10 Configure the country code for the entity

Operation	Command
Configure the country code	**country** *country-code-str*
Delete the country setting	**undo country**

By default, no country code is specified for the entity.

Note:

Country code uses two standard characters, for example, CN for China and US for the United States.

V. Configuring the state name for the entity

Perform the following configuration in PKI entity view.

Table 9-11 Configure the state name for the entity

Operation	Command
Configure the state name	**state** *state-str*
Delete the state setting	**undo state**

By default, no state name is specified for the entity.

VI. Configuring the geographic locality for the entity

Perform the following configuration in PKI entity view.

Table 9-12 Configure the geographic locality for the entity

Operation	Command
Configure the geographic locality	**locality** *locality-str*

Operation	Command
Delete the locality setting	**undo locality**

By default, no geographic locality is specified for the entity.

VII. Configuring the organization name for the entity

Perform the following configuration in PKI entity view.

Table 9-13 Configure the organization name for the entity

Operation	Command
Configure the organization name	**organization** *org-str*
Delete the organization setting	**undo organization**

By default, no organization name is specified for the entity.

VIII. Configuring the organization unit name for the entity

This optional field specifies to which of the many units of an organization this entity belongs.

Perform the following configuration in PKI entity view.

Table 9-14 Configure the organization unit name for the entity

Operation	Command
Configure the organization unit name	**organizational-unit** *org-unit-str*
Delete this name specification	**undo organizational-unit**

By default, no organization unit name is specified for the entity.

IX. Configuring the common name for the entity

Perform the following configuration in PKI entity view.

Table 9-15 Configure the common name for the entity

Operation	Command
Configure the common name	**common-name** *name-str*
Delete the common name	**undo common-name**

By default, no common name is specified for the entity.

X. Configuring the IP address for the entity

It is an optional operation, with the same function as specifying the entity FQDN.

Perform the following configuration in PKI entity view.

Table 9-16 Configure the IP address for the entity

Operation	Command
Configure the IP address	**ip** *ip-address*
Delete the IP address	**undo ip**

By default, no IP address is specified for the entity.

9.2.6 Creating a Local Public -- Private Key Pair

A pair of keys are generated during certificate request: one public and the other private. The private key is held by the user, while the public key and other information are transferred to CA center for signature and then the generation of the certificate. Each CA certificate has a lifetime that is determined by the issuing CA. When the private key leaks or the current certificate is about to expire, you have to delete the old key pair. Then another key pair can be generated for a new certificate.

If an RSA key pair already exists when you create a local key pair, the system prompts whether to replace it. Each key pair is named using this convention: Router name + host. The minimum length of a host key is 512 bits and the maximum length is 2048 bits.

Perform the following configuration in system view.

Table 9-17 Create and destroying an RSA key pair

Operation	Command
Create an RSA key pair	**rsa local-key-pair create**
Destroy an RSA key pair	**rsa local-key-pair destroy**

By default, there is no existent local RSA key pair.

⚠ **Caution:**

- If a local certificate already exists, you are not recommended to create another key pair. To ensure consistency between key pair and existing certificate, you should first delete the existing certificate and then create a new key pair.
- If a local RSA key pair exists, the newly-generated key pair will overwrite the existing one.
- The key pairs are originally for the use in SSH. Local server regularly updates local server key pair. However, the host key pair we use in certificate request remains unchanged.

9.2.7 Configuring Polling Interval and Count

If CA examines certificate request in manual mode, then a long time may be required before the certificate is issued. In this period, you need to query the request status periodically, so that you may get the certificate right after it is issued.

Perform the following configuration in PKI domain view.

Table 9-18 Configure polling interval and count

Operation	Command
Configure polling interval and count	**certificate request polling** { **interval** *minutes* | **count** *count* }
Restore the default values	**undo certificate request polling** { **interval** | **count** }

By default, the request polling message is sent for 50 times at an interval of 20 minutes.

9.2.8 Configuring Certificate Request Mode

Request mode can be manual or auto. Auto mode enables the automatic request for a certificate through SCEP when there is none and for a new one when the old one is about to expire. For manual mode, all the related configuration and operation need to be carried out manually.

Perform the following configuration in PKI domain view.

Table 9-19 Configure certificate request mode

Operation	Command
Configure certificate request mode	**certificate request mode** { **manual** | **auto** [**key-length** *key-length* | **password** { **simple** | **cipher** } *password*]* }

Operation	Command
Restore the default request mode	**undo certificate request mode**

By default, manual mode is selected.

9.2.9 Delivering a Certificate Request Manually

A certificate request completes with user public key and other registered information. All configured, you can deliver the certificate request to a PKI RA.

Perform the following configuration in system view.

Table 9-20 Deliver a certificate request

Operation	Command
Deliver a certificate request.	**pki request-certificate domain** *domain-name* [*password*] [**pkcs10** [**filename** *filename*]]

⚠ **Caution:**

- If a local certificate already exists, certificate request operation is disallowed to eliminate inconsistency between certificate and registration information resulted from configuration change. To request a new certificate, you should first delete the existing local certificate and all the CA certificates locally stored using the **pki delete certificate** command.
- If you cannot send certificate request to CA using SCEP, you can select the parameter **pkcs10** to print out the request information, copy it and send one to CA in out-of-band mode.
- Before you deliver the certificate request, make sure the clocks of entity and CA are synchronous. Otherwise, fault occurs to the certificate validation period.
- This operation will not be saved.

9.2.10 Retrieving a Certificate Manually

Certificate retrieval serves two purposes: store locally the certificate related to local security domain to improve query efficiency; prepare for certificate validation.

When downloading a digital certificate, select the **local** keyword for a local certificate and **ca** keyword for a CA certificate.

Perform the following configuration in system view.

Table 9-21 Retrieve a certificate

Operation	Command
Retrieve a certificate and download it locally	**pki retrieval-certificate** { **local** | **ca** } **domain** *domain-name*

⚠ **Caution:**

- If a CA certificate already exists locally, CA certificate request operation is disallowed to eliminate inconsistency between certificate and registration information resulted from configuration change. To request a new certificate, you should first delete the existing CA and local certificates using the **pki delete certificate** command.
- This operation will not be saved.

9.2.11 Importing an Certificate

Use the following command to import an existing local certificate or CA certificate.

Perform the following configuration in system view.

Table 9-22 Import a certificate

Operation	Command
Import a certificate	**pki import-certificate** { **local** | **ca** } **domain** *domain-name* { **der** | **p12** | **pem** } [**filename** *filename*]

9.2.12 Deleting a Certificate

You can delete an existing local certificate or CA certificate.

Perform the following configuration in system view.

Table 9-23 Delete a certificate

Operation	Command
Delete a certificate	**pki delete-certificate** { **local** | **ca** } **domain** *domain-name*

9.3 Certificate Validation Configuration

9.3.1 Configuration Task List

At every stage of data communication, both parties should verify the validity of corresponding certificates, including issue time, issuer and certificate validity. The core is to verify the signature of CA and to make sure the certificate is still valid. It is believed that CA never issues fake certificates, so every certificate with an authentic CA signature will pass the verification. For example, if you receive an Email, which contains a certificate with public key and is encrypted with private key, then you should verify the validity of this certificate, to determine whether it is valid and trustworthy.

For certificate validation, you need to:

- Specify CRL distribution point location
- Configure CRL update period
- Enable/Disable CRL check
- Retrieve CRL
- Verify certificate validity

9.3.2 Specifying CRL Distribution Point location

Perform the following configuration in PKI domain view.

Table 9-24 Configure CRL distribution point location

Operation	Command
Specify CRL distribution point location	**crl url** *url-string*
Delete the location setting	**undo crl url**

By default, no CRL distribution point location is specified.

9.3.3 Configuring CRL Update Period

CRL update period refers to the interval to download CRLs from CRL access server to a local machine.

Perform the following configuration in PKI domain view.

Table 9-25 Configure CRL update period

Operation	Command
Specify CRL update period	**crl update period** *hours*
Restore the default period	**undo crl update period**

By default, CRLs are updated according to their validity period.

Note:

CRL update period configured manually takes priority over that specified in CRLs.

9.3.4 Enabling/Disabling CRL Check

CRL check is optional for certificate validation. If it is enabled, you must check CRL to decide on the certificate validity.

Perform the following configuration in PKI domain view

Table 9-26 Enable/disable CRL check

Operation	Command
Disable CRL check	**crl check disable**
Enable CRL check	**undo crl check disable**

By default, CRL check is enabled.

9.3.5 Retrieving a CRL

Having finished the above configuration tasks, you can retrieve CRL in any view. The purpose of downloading CRL is to verify the validity of the certificates on a local device.

Perform the following configuration in system view.

Table 9-27 Retrieve a CRL

Operation	Command
Retrieve a CRL and download it locally	**pki retrieval-crl domain** *domain-name*

Note:

This operation will not be saved in configuration.

9.3.6 Verifying Certificate Validity

You can verify the validity of a local certificate using the parameter “local” ; or a CA certificate using the parameter “ca”.

Perform the following configuration in system view.

Table 9-28 Verify certificate validity

Operation	Command
Verify the validity of a local certificate	**pki validate-certificate** { **local** | **ca** } **domain** *domain-name*

Note:

This operation will not be saved in configuration.

9.4 Display and Debug

I. Displaying certificates

If the certificate retrieval succeeds, you can display the fields of the certificates locally downloaded. Certificate format and fields comply with X.509 standard. All kinds of identifying information about user and CA are included, such as user email address; public key of the certificate holder; issuer, serial number, and validity (period) of the certificate, etc.

Perform the following configuration in any view.

Table 9-29 Display certificates

Operation	Command
Displaying certificates	**display pki certificate** { { **local** | **ca** } **domain** *domain-name* **| request-status** }

II. Displaying CRL

The fields of a CRL that is retrieved and locally downloaded can be displayed by the following operation. CRL complies with X.509 standard, covering version, signature (algorithm), issuer name, this update, next update, user public key, signature value, serial number, and revocation date, etc.

Perform the following configuration in any view.

Table 9-30 Display CRLs

Operation	Command
Displaying CRLs	**display pki crl domain** *domain-name*

III. Displaying and debugging configuration

Using the **display current** command, you can view current PKI configuration. You can enable PKI debugging to monitor and diagnose relevant certificate implementation.

Perform the following configuration in any view.

Table 9-31 Display and debug PKI information

Operation	Command
Enable PKI debugging	**debugging pki** { **verify** | **request** | **retrieval** | **error** }
Disable PKI debugging	**undo debugging pki** { **verify** | **request** | **retrieval** | **error** }

By default, all PKI debugging is disabled.

9.5 Typical Configuration Examples

9.5.1 IKE Authentication with PKI Certificate

I. Network requirement

An IPSec security channel is created between Router A and Router B to ensure the security of the data stream between the subnet represented by PC A (10.1.1.x) and the subnet represented by PC B (10.1.2.x). IKE automatic negotiation creates secure communication between Router A and Router B. IKE authentication policy adopts PKI certificate system to authenticate identity.

Figure 9-2 supposes that Router A and Router B have different CAs (they can be the same depending on the real situation).

II. Network diagram

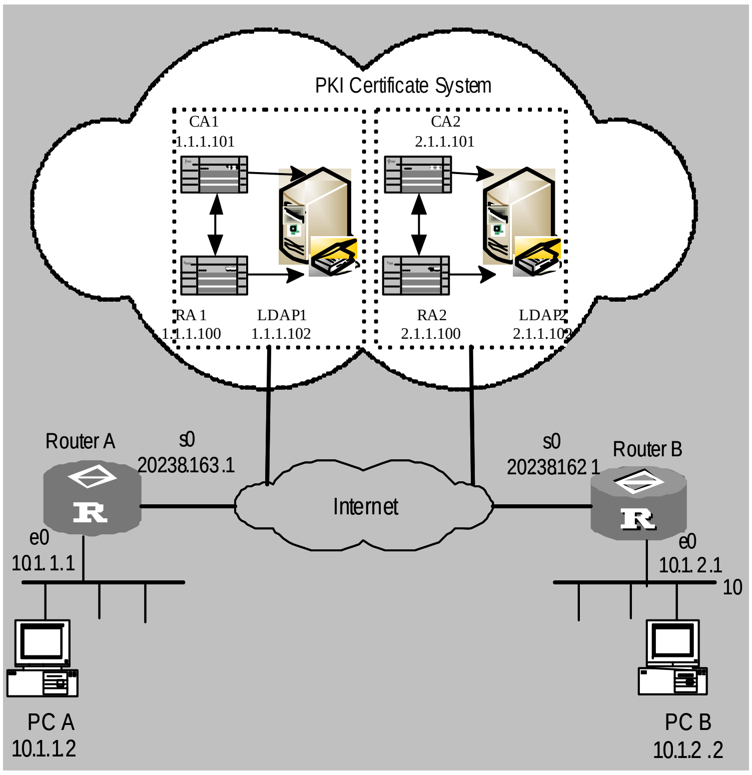


Figure 9-2 IKE authentication with PKI certificate

III. Configuration procedures

1) Configure Router A:

# Use the defaulted IKE policy on Router A and enable PKI (rsa-signature) to authenticate identity.

```
[RouterA] ike proposal 1
[RouterA-ike-proposal-1] authentication-method rsa-signature
[RouterA-ike-proposal-1] quit
```

# Configure parameters on PKI domain.

```
[RouterA]pki domain 1
[RouterA-pki-domain-1] ca identifier CA1
[RouterA-pki-domain-1]          certificate          request          url
http://1.1.1.100/certsrv/mscep/mscep.dll
[RouterA-pki-domain-1] certificate request entity en
[RouterA-pki-domain-1] ldap-server ip 1.1.1.102
```

# Configure CRL distribution point location (if CRL check is disabled, this configuration is not necessary).

```
[RouterA-pki-domain-1] crl url ldap://1.1.1.102
[RouterA-pki-domain-1] quit
```

# Configure entity DN.

```
[RouterA] pki entity en
[RouterA-pki-entity-en] ip 202.38.163.1
[RouterA-pki-entity-en] common-name RouterA
```

# Create local key pair using RSA algorithm.

```
[RouterA-pki-entity-en] rsa local-key-pair create
[RouterA-pki-entity-en] quit
```

# Request certificate

```
[RouterA] pki retrieval-certificate ca domain 1
[RouterA] pki request-certificate 1
```

2) Configure Router B:

# Use the defaulted IKE policy on Router B and enable PKI (rsa-signature) to authenticate identity.

```
[RouterB] ike proposal 1
[RouterB-ike-proposal-1] authentication-method rsa-signature
[RouterB-ike-proposal-1] quit
```

# Configure parameters on PKI domain.

```
[RouterB]pki domain 1
[RouterB-pki-domain-1] ca identifier CA2
[RouterB-pki-domain-1]          certificate          request          url
http://2.1.1.100/certsrv/mscep/mscep.dll
[RouterB-pki-domain-1] certificate request entity en
[RouterB-pki-domain-1] ldap-server ip 2.1.1.102
```

# Configure CRL distribution point location (if CRL check is disabled, this configuration is not necessary).

```
[RouterB -pki-domain-1] crl url ldap://2.1.1.102
[RouterB-pki-domain-1] quit
```

# Configure entity DN.

```
[RouterB] pki entity en
[RouterB-pki-entity-en] ip 202.38.162.1
[RouterB-pki-entity-en] common-name RouterB
```

# Create local key pair using RSA algorithm.

```
[RouterB-pki-entity-en] rsa local-key-pair create
[RouterB-pki-entity-en] quit
```

# Request certificate

```
[RouterB] pki retrieval-certificate ca domain 1
[RouterB] pki request-certificate 1
```

🕮 **Note:**

The configuration of IKE negotiation using PKI identity authentication is described above. If you want to create an IPSec security channel to ensure communication security, you also need to configure IPSec. Refer to the configuration tasks described in chapters “IPSec Configuration” and “IKE Configuration”.

9.6 Troubleshooting

9.6.1 Fault 1: Failing to Retrieve a CA Certificate

Troubleshooting: If you fail to obtain a CA certificate, the reasons might include:

1) Software problems

- No trustworthy CA is specified.
- Server URL for the certificate request through SCEP is not correct or not configured. You can check if the server is well connected by using the **ping** command.
- No RA is specified.

2) Hardware problems

- Network connection faults, such as broken network cable and loose interface.

9.6.2 Fault 2: Failing to Request a Local Certificate

Troubleshooting: If you fail to request a local certificate when the router has finished the configuration of PKI domain parameters and entity DN, and has created a new RSA key pair, the reasons might include:

1) Software problems

- No CA/RA certificate has been retrieved.
- No key pair is created, or the current key pair has had a certificate.
- No trustworthy CA is specified.
- Server URL for the certificate request through SCEP is not correct or not configured. You can check if the server is well connected by using the **ping** command.
- No certificate authority is configured.
- The necessary attributes of entity DN are not configured. You can configure the relevant attributes by checking CA/RA authentication policy.

2) Hardware problems

Network connection faults, such as broken network cable and loose interface.

9.6.3 Fault 3: Failing to Retrieve a CRL

Troubleshooting: If you fail to retrieve a CRL, the reasons might include:

1) Software problems

- No local certificate exists when you try to retrieve a CRL.
- IP address of LDAP server is not configured.
- CRL distribution point location is not configured.
- LDAP server version is wrong.

2) Hardware problems

Network connection faults, such as broken network cable and loose interface.

VPN

Table of Contents

Chapter 1 VPN Overview

1.1 VPN Overview

Along with the increasingly wide application of the Internet, Virtual Private Network (VPN) emerged to construct private networks on public networks. “Virtual” here mainly indicates that VPN is a kind of logical networks.

Employees travel around on business more and more frequently; foreign services and customers are scattered more widely; cooperation is conducted with a growing number of partners - all these are sound quite familiar to all the growing companies. More and more companies therefore turn to the Internet for market promotion, sales, aftersales services, and also for conducting training, cooperation and other counseling activities. This provides a broad market for the application of VPN.

1.1.1 Features of VPN

- Different from a traditional network, VPN does not exist physically. It is a kind of logical network, a virtual network formed through resources collocation employing the current public network.
- Each VPN is only for a particular enterprise or group of users. For VPN users, VPN is just like any traditional private network. As a kind of private network, VPN keeps resources independent of the underlying network, meaning resources of each VPN are normally inaccessible for other VPNs over the underlying network and users outside this VPN. It also delivers adequate security, safeguarding the internal information of VPN against external invasion.
- VPN is a kind of upper layer service but not simple. It establishes network interconnection between private network users, including network topology inside VPN, route calculation, joining and leaving of members, etc. Thus, VPN technology is much more complicated, compared to common point-to-point applications alike.

1.1.2 Benefits of VPN

VPN allows you to:

- Establish reliable and safe connection between remote users, oversea agencies, partners, suppliers and company headquarters, ensuring security of data transmission. This advantage is of special significance to the amalgamation of E-business or financial network with communication network.
- Provide information communication over public networks, thus allowing enterprises to connect with remote offices, staff traveling on business and

business partners at a low cost, while improving utility of network resources. This will help Internet Service Providers (ISPs) increase profits.

- Add or delete users through software configuration rather than changing hardware facilities, thus delivering great flexibility.
- Support mobile access of VPN users at any time in any place, thus meeting growing mobile service demands.
- Create VPN with QoS (e.g. MPLS VPN), providing differentiated services for VPN users and by pricing these services differently obtaining more profits. For the fundamentals and related introduction of MPLS VPN, refer to the chapter “MPLS Configuration”.

1.1.3 Structure of VPN Network

VPN comprises a group of sites. A site might join one or more VPNs, but any two sites are IP reachable only if they belong to the same VPN. According to its standard definition, VPN with all its Sites coming from a single enterprise is called Intranet, and cross-enterprise VPN is by contrast called Extranet.

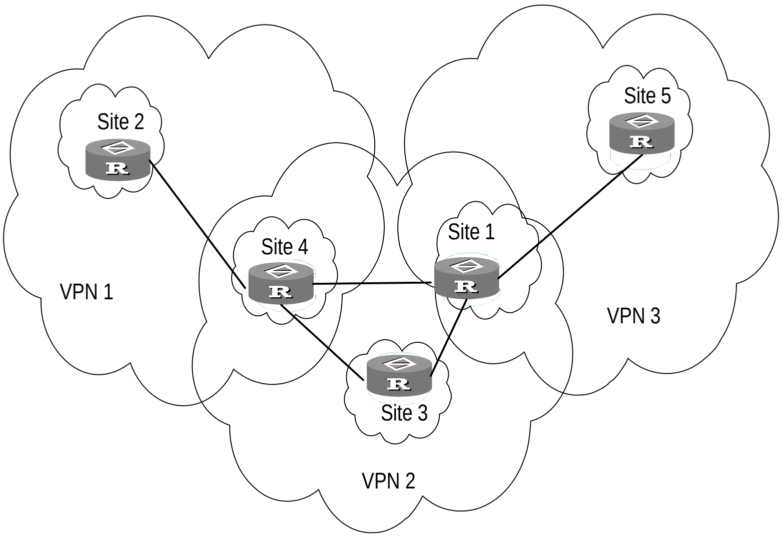


Figure 1-1 The composition of VPN

The above chart demonstrates the relationship between five sites and three VPNs.

- VPN1---Site2, Site4
- VPN2---Site1, Site3, Site4
- VPN3---Site1, Site5

1.2 Fundamental Technology of VPN

I. Basic Networking Application of VPN

Take an enterprise as an example. Its intranet through VPN is shown in following figure.

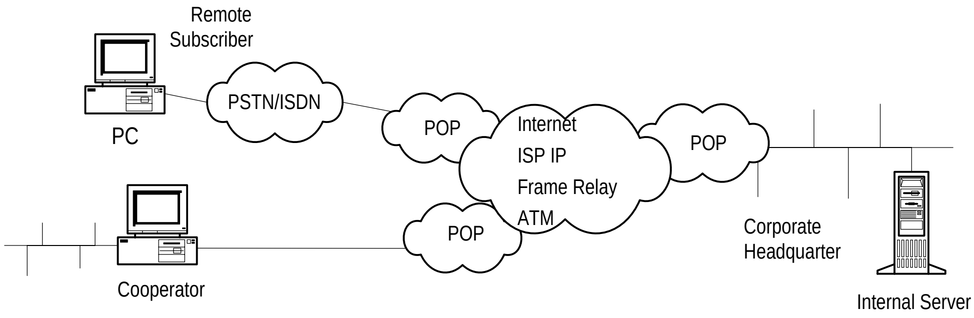


Figure 1-2 Diagram of VPN application

It can be seen that enterprise internal resource sharers can access local ISP at its POP (Point of Presence) server via PSTN/ISDN network or local network and access the internal resources of the company. With traditional WAN networking technology, however, they need to be connected using dedicated lines to achieve the same purpose. VPN allows remote end users and clients in other cities to access enterprise internal resources without being authorized by their local ISPs, which is of great significance for staffs on business trip and geographically scattered clients.

An enterprise can deploy VPN services simply by setting up a VPN-supported server for resource sharing (e.g. a Windows NT server or a router supporting VPN). The resource sharers connect to local POP server via PSTN/ISDN or LAN before they directly call the remote server (VPN server) of the enterprise. The call process is completed by ISP Network Access Server (NAS) and VPN server together.

II. Mechanism of VPN

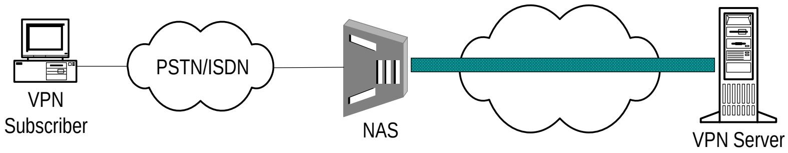


Figure 1-3 Diagram of accessing VPN

As shown in the above figure, through PSTN/ISDN network, a subscriber accesses ISP NAS (Network Access Server). After NAS server recognizes that this is a VPN user by checking user name or access number, it establishes a connection, which is called tunnel, to the user’s destination VPN server. Then NAS encapsulates the user data into IP packets and transmits it to the VPN server through this tunnel. Upon the receipt of this IP packet, VPN server removes the encapsulation to get the original data. In the opposite direction, the packet is handled likewise. On both sides of the tunnel, packets can be encrypted to make other users on the Internet unable to access them, so they are safe and authentic. For users, tunnels are only the logical extension of their PSTN/ISDN links and thus can be operated like the physical links.

Tunnels are implemented using tunneling protocols. Tunneling protocols are divided into layer 2 tunneling protocols and layer 3 tunneling protocols depending on at which layer of OSI model tunnel is implemented.

1) Layer 2 tunneling protocols

Layer 2 tunneling protocols encapsulate PPP frames entirely into internal tunnels. The existing layer 2 tunneling protocols include:

- PPTP (Point to Point Tunneling Protocol): Supported by companies like Microsoft, Ascend, and 3COM and in OS of Windows NT 4.0 and its later versions. This protocol supports tunneling encapsulation of PPP in IP networks. As a call control and management protocol, PPTP uses an enhanced Generic Routing Encapsulation (GRE) technology to provide the encapsulation service with flow control and congestion control for transmitted PPP packets.
- L2F (Layer 2 Forwarding): Supported by Nortel and some other companies. It supports the tunnel encapsulation for the higher-level link layer and physically separates dial-up server and dial-up connection.
- L2TP (Layer 2 Tunneling Protocol): Drafted by IETF, Microsoft and other companies. Absorbing the advantages of above two protocols, it is accepted by most companies and has become a standard RFC. L2TP provides both dial-up VPN service and leased line VPN service.

2) Layer 3 tunneling protocols

Both start point and end point of layer 3 tunneling protocol are in ISP. PPP session terminates at NAS. Only layer 3 packets are carried in tunnels. The existing layer 3 tunneling protocols include:

- GRE (Generic Routing Encapsulation), which is used to encapsulate a network layer protocol into another one.
- IPSec (IP Security), which provides a complete architecture of data security on IP networks by using several protocols rather than a single one, such as AH (Authentication Header), ESP (Encapsulating Security Payload), and IKE (Internet Key Exchange).

GRE and IPSec mainly apply in private line VPN.

3) Contrast between layer 2 tunneling protocols and layer 3 tunneling protocols

Compared with layer 2 tunneling protocols, the advantages of layer 3 tunneling protocols are their security, scalability and reliability. In terms of security, layer 2 tunnel imposes great challenges to security of user networks and firewall technologies while layer 3 tunnel does not, because layer 2 tunnel generally terminates at customer premise equipment and layer 3 tunnel at ISP gateway.

Concerning scalability, layer 2 tunnel is not as efficient as layer 3 tunnel in transmission due to the encapsulation of entire PPP frames. Besides, its PPP session runs through the entire tunnel and terminates at customer premise equipment, and thus requires the user-side gateway to store a large amount of PPP session status and information, which may not only overload the system but also decrease the scalability. The introduction of tunneling latency may incur such problems as PPP session timeout in time sensitive LCP and NCP negotiations of PPP. On the contrary, layer 3 tunnel terminates within ISP gateway, and PPP session terminates at NAS; thus user gateway needs not to manage and maintain status of each PPP session, and thereby reduces system load.

Normally, layer 2 tunneling protocols and layer 3 tunneling protocols are used separately. The reasonable combination of two types of protocols, however, may deliver better security and functions (e.g. using L2TP and IPSec together).

1.3 Classification of VPN

IP VPN means emulating private line service of WAN (e.g. remote dial-up, DDN, etc.) over IP networks (including the Internet or dedicated IP backbone). IP VPN is classified as follows:

I. Classified by operation mode

1) CPE-based VPN (Customer Premises Equipment based VPN)

Users not only have to install expensive devices and special authentication tools, but also maintain complex VPN (e.g. channel maintenance, bandwidth management, etc.). Networking in this way features both high complexity and low service scalability.

2) NBIP-VPN (Network-based VPN)

The maintenance of VPN (permitting users to conduct service management and control to some extent) is conducted by ISP, and all functions are implemented at network device side, so as to reduce users' investment, reinforce the flexibility and scalability of services, and bring new incomes to ISP.

II. Classified by service application

1) Intranet VPN

Intranet VPN interconnects points distributed inside an enterprise by making use of public network. It is an extended or substitute form of traditional private network or other enterprise network.

2) Access VPN

Access VPN allows remote users like staff traveling on business and remote small offices to establish private network connections with the intranet and extranet of their enterprise over a public network. Access VPN provides two types of connections: client-initiated VPN connection and NAS-initiated VPN connection.

3) Extranet VPN

Extranet VPN extends an enterprise network to suppliers, cooperators and clients by using VPN, allowing different enterprises to construct VPN over public networks.

III. Classified by networking model

1) VLL

Virtual Leased Line (VLL) is emulation to traditional leased line services. By emulating leased line over IP networks, it provides asymmetric and low cost “DDN” service. From the view of end users of VLL, it is similar to traditional leased lines.

2) VPDN

Virtual Private Dial Network (VPDN) means implementing virtual private network by employing the dial-up function of public networks (e.g. ISDN and PSTN) and access networks, to provide access service for enterprises, small ISPs, and mobile businesspersons.

3) VPLS service

Virtual Private LAN Segment (VPLS) interconnects LANs via virtual private network segments in virtue of IP public networks. It is an extension of LANs on IP public networks.

4) VPRN

Virtual Private Routing Network (VPRN) interconnects headquarters, branches and remote offices via network management virtual router in virtue of IP public networks. There are two kinds of VPRN services: VPRN implemented using traditional VPN protocol (IPSec, GRE, etc.) and VPRN by means of MPLS.

IV. Classified by working layer

1) L3VPN: including BGP/MPLS VPN, IPSec VPN, GRE VPN, etc.
2) L2VPN: including MPLS L2VPN in Martini mode, MPLS L2VPN in Kompalla mode, MPLS L2VPN in SVC mode, VPLS and static CCC configuration.
3) VPDN: including L2TP, PPTP, etc.

Chapter 2 Configuration of L2TP

2.1 Introduction to L2TP Protocol

2.1.1 VPDN Overview

Virtual Private Dial Network (VPDN) means implementing virtual private network by employing the dial-up function of public networks (e.g. ISDN and PSDN) and access networks, thus providing access service for enterprises, small ISPs and mobile businessmen.

VPDN sets up safe virtual private networks in public networks for enterprises by making use of special network encryption protocols. In this way, overseas agencies and traveling staff of an enterprise can access the headquarters' network by making use of encrypted virtual tunnels over public networks, while other users in public networks have no access to internal resources of the enterprise network through virtual tunnels.

There are two VPDN implementation approaches:

1) NAS sets up tunnel with VPDN gateway by making use of a tunneling protocol. In this way, users’ PPP connections are directly connected to enterprise’s gateway. Protocols available now are L2F and L2TP. This approach has a great deal of advantages: transparent tunnel setup process from the perspective of users, network access with one login, user authentication and address assignment by enterprise network without occupying public addresses, and support to a wide range of platforms for network access. It requires however: a) NAS supporting the VPDN protocol, and b) authentication system supporting VPDN attributes, and c) router or special VPN server working as gateway.
2) Client sets up tunnel with VPDN gateway. In this way, client first creates connection with the Internet, and then sets up a tunnel with gateway by using the special client software (e.g. L2TP client supported by Win2000). This approach allows users to access network by whatever available means and wherever they are without the intervention of ISP. The bad news is the limitation in platform, meaning users need to install special software (usually Win2000 platform).

There are three types of VPDN tunneling protocols: PPTP, L2F, and L2TP, with L2TP being most popular.

2.1.2 Introduction to L2TP Protocol

I. Protocol background

PPP defined a kind of encapsulation technology that allows the transmission of various kinds of data packets on layer 2 point-to-point links. Meanwhile, PPP is performed between users and NAS, with endpoint of layer 2 link and PPP session sticking on the same hardware.

L2TP provides tunnel transmission for PPP link layer packets. It extents PPP model in that it permits link endpoint of layer 2 and PPP session point staying at different devices and allows information interaction by using packet switching network technologies. It combines the advantages of PPTP and L2F. Therefore, it becomes the industrial standard of IETF in layer 2 tunneling.

II. Typical L2TP networking application

Figure 2-1 shows a typical network where VPDN is constructed using L2TP:

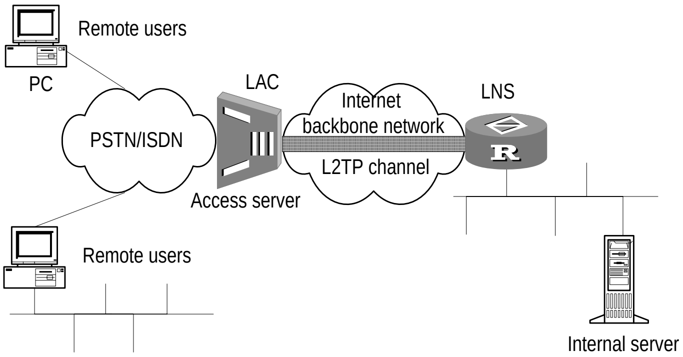


Figure 2-1 Network diagram of typical VPDN application created by L2TP

In this figure, LAC stands for L2TP Access Concentrator, a switching network device with the capability to process PPP and L2TP requests. Usually, LAC functions as Network Access Server (NAS) to provide access service to users by making use of PSTN/ISDN. LNS stands for L2TP Network Server, a device functioning in the PPP system as L2TP server.

LAC lies between LNS and remote system (remote users and remote branches) to transmit packets between them, encapsulate packets from remote system in L2TP protocol and send the encapsulated packets to LNS, and decapsulate packets from LNS and send the remaining part to remote system. Local connection or PPP link can be adopted between LAC and remote system, but PPP link is always involved in VPDN applications. As one end of the L2TP tunnel, LNS is the peer device of LAC, and also is the logic terminating point of PPP session transmitted in tunnel by LAC.

III. Technology details of L2TP protocol

1) Architecture of L2TP protocol

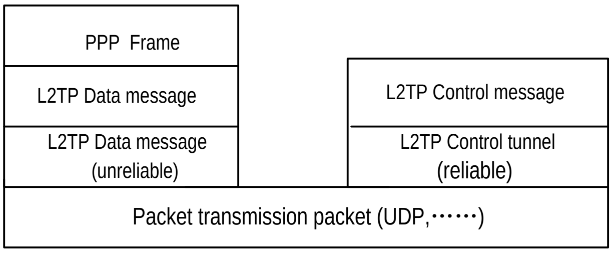

PPP Frame
L2TP Data message
L2TP Control message
L2TP Data message (unreliable)
L2TP Control tunnel (reliable)
Packet transmission packet (UDP,……)

Figure 2-2 Architecture of L2TP protocol

The architecture of L2TP protocol shown above describes the relationship between PPP frame, control tunnel and data tunnel. PPP frame is transmitted in unreliable L2TP data channel. Control message is transmitted in reliable L2TP control channel.

Usually L2TP data is carried in UDP packets for transmission. L2TP registers the UDP port 1701, but this port is only used for the tunnel setup at the early stage. L2TP tunnel initiator selects an arbitrary port from available ones (unnecessarily being 1701) and forwards packets to 1701 port of the receiver. After the receiver receives the packets, it also selects a free port randomly (unnecessarily being 1701) and forwards packets again to the specified port of the initiator. Thus, ports of the two sides are determined. They will remain unchanged until the tunnel connection is disconnected.

2) Definitions of tunnel and session

There are two kinds of connections between LNS-LAC pairs: Tunnel connection and Session connection. Tunnel connections define pairs of LNS and LAC while Session connections are multiplexed in a Tunnel connection to present PPP sessions in it. Several L2TP tunnels can be created between a LNS-LAC pair, which consist of a control connection, and one or several Sessions. Session connections can be set up only after tunnels are created successfully (including such information exchange as ID protection, L2TP version, frame type, hardware transmission type, etc.). Each session connection corresponds to a PPP data stream between LAC and LNS. Both control messages and PPP data packets are transmitted in the tunnels.

L2TP uses Hello packets to check the connectivity of a tunnel. LAC and LNS forward Hello packets to peer ends at regular intervals. If no response to Hello packet is received within a certain period, the tunnel will be cleared.

3) Definitions of control message and data message

There are two kinds of messages in L2TP: control messages and data messages. Control messages are used for the setup, maintenance and transmission control of tunnel and session connections, while data messages are for PPP frame encapsulation and transmission in tunnels. The transmission of control messages is reliable, delivering flow and congestion control. On the contrary, the transmission of data messages is unreliable, meaning it lacks mechanisms of retransmission, flow control, and congestion control.

Control messages and data messages share the same type of packet headers. Tunnel ID and Session ID are included in L2TP packet header, to identify different tunnels and sessions. The packets with the same Tunnel ID but different Session IDs will be multiplexed in the same tunnel. Tunnel ID and Session ID in the packet header are assigned by peer ends.

IV. Two typical L2TP tunnel modes

The following figure shows the tunnel modes available between remote system or LAC clients (hosts running L2TP) and LNS:

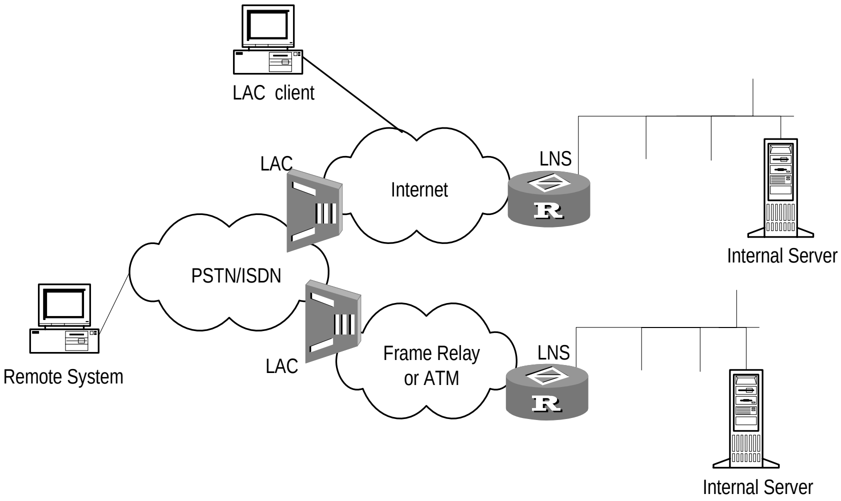


Figure 2-3 Two typical L2TP tunnel modes

1) Initiated by remote dial-up user. Remote system dials in LAC via PSTN/ISDN. LAC sends tunnel setup request to LNS through the Internet. Dial-up users' addresses are assigned by LNS. The authentication and accounting of remote dial-up users can be accomplished either by LAC side as an agent or by LNS side directly.
2) Initiated directly by LAC users (local users who support L2TP). In this case, LAC users can send tunnel setup request directly to LNS, without requiring an additional LAC device. LAC users' addresses are assigned by LNS.

V. Call setup flow of L2TP tunnel

Typical L2TP application network is as follows:

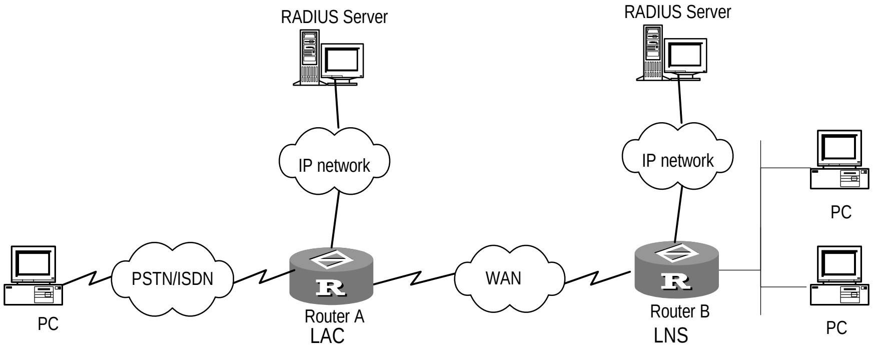


Figure 2-4 Typical L2TP application network

Call setup flow of L2TP tunnel is shown in the following figure:

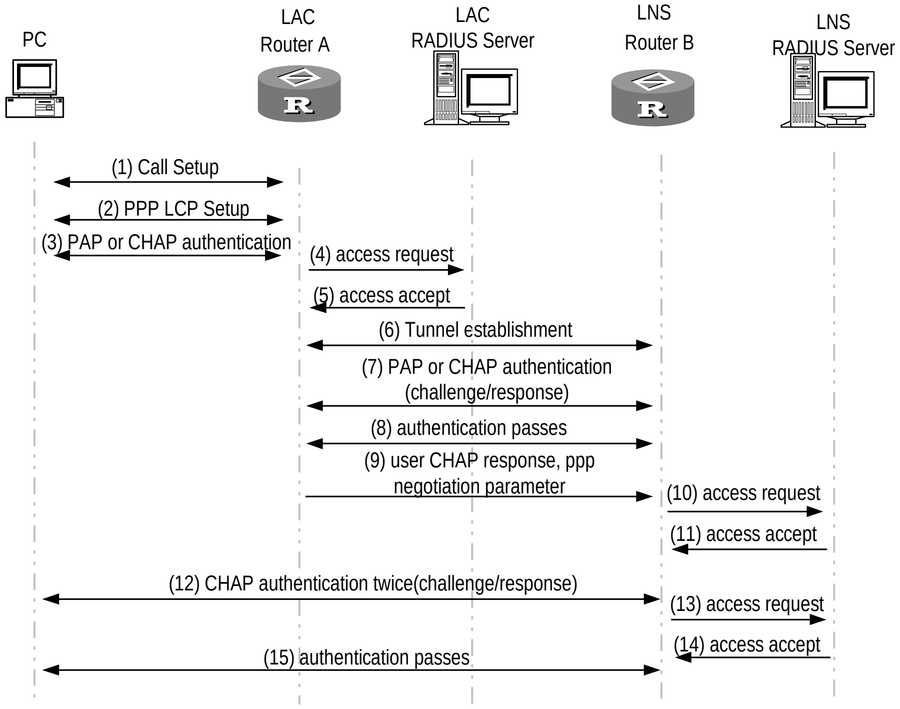


Figure 2-5 Call setup flow of L2TP channel

The following is the call setup process using L2TP tunnel:

1) The PC at user side initiates setup request;
2) The PC and LAC equipment (Router A) negotiate PPP LCP parameters;
3) LAC performs PAP or CHAP authentication based on the information provided by the PC;
4) LAC sends access request including VPN user's name and password to RADIUS server for authentication;

5) RADIUS server authenticates this user and sends back access accept, such as LNS address, after authentication is passed successfully; LAC is ready for initiating a new tunnel request;
6) LAC initiates a tunnel request to the LNS address sent back by RADIUS server;
7) LAC informs LNS of “CHAP challenge” information, LNS sends back CHAP response and its own CHAP challenge, and LAC sends back CHAP response;
8) Authentication passes successfully;
9) LAC transmits the information of CHAP response, response identifier and PPP negotiation parameters to LNS;
10) LNS sends the access request to RADIUS server for authentication;
11) RADIUS server authenticates this access request and sends back a response if authentication is successful;
12) If local mandatory CHAP authentication is configured at LNS, LNS will authenticate the VPN user by sending CHAP challenge and the VPN user at PC sends back responses;
13) LNS resends this access request to RADIUS for authentication;
14) RADIUS server re-authenticates this access request and sends back a response if authentication is successful;

The authentication passes and the VPN user can use the internal resources of the enterprise.

2.2 LAC Configuration

Concerning L2TP configuration, configuration of LAC side differs from that of LNS side. This section mainly covers the configuration of LAC side. In configuration task list, L2TP must be enabled and L2TP group must be created before any other functions can be configured. For detailed introduction to related PPP configuration commands, refer to the chapters and sections for them.

Configuration tasks at LAC side include:

- Enable L2TP (required)
- Create L2TP group (required)
- Set the condition triggering L2TP tunnel setup request and LNS addresses (required)
- Set local name (optional)
- Set Tunnel authentication and password (optional)
- Configure AVP hiding (optional)
- Set Hello interval in the tunnel.(optional)
- Set user name and password and configure user authentication (required)
- Disconnect Tunnel by force (optional)
- Enable/disable the flow control function of the tunnel (optional)
- Set L2TP session idle-timeout timer (optional)
- Configure the tunnel-hold function of L2TP (optional)

- Set the LAC to function as client (optional)

2.2.1 Enabling L2TP

Only after L2TP is enabled can L2TP functions on the router work normally. If L2TP is disabled, the router cannot provide related functions even if parameters of L2TP have been configured.

These configurations are compulsory on LAC side.

Perform the following configuration in system view.

Table 2-1 Enable/disable L2TP

Operation	Command
Enable L2TP.	**l2tp enable**
Disable L2TP.	**undo l2tp enable**

By default, L2TP is disabled.

2.2.2 Creating L2TP Group

L2TP group needs to be created in order to fulfill related parameter configurations of L2TP. It allows you not only to configure L2TP functions as needed but also to implement one-to-one and one-to-many networking applications between LAC and LNS. L2TP groups are numbered separately on LAC and LNS, so LAC and LNS only need to keep consistent in the configurations of the involved L2TP groups (e.g. remote name of tunnel , start L2TP and LNS address, etc.).

These configurations are compulsory on LAC side.

Perform the following configuration in system view.

Table 2-2 Create/delete L2TP group

Operation	Command
Create L2TP group.	**l2tp-group** *group-number*
Delete L2TP group.	**undo l2tp-group** *group-number*

After a L2TP group is created, other configurations related to the L2TP group can be performed in L2TP group view, for example, name of peer end, condition triggering L2TP tunnel setup request and LNS address.

By default, no L2TP group is created.

2.2.3 Setting Condition Triggering L2TP Tunnel Setup Request and LNS Address

A router will not send L2TP Tunnel setup request to some other router or LNS server unless certain conditions are met. By configuring decision making rule based on user information and specifying IP address of LNS, you may allow the router to determine whether a user is a VPN user and initiate connection with the LNS. Up to five LNS addresses can be configured, meaning LNS backup is allowed. In normal operations, local router (LAC) sends Tunnel setup request to the peer end (LNS) in the order in which LNS addresses are configured until some LNS accepts the request. This LNS becomes the peer end of L2TP tunnel.

Perform the following configuration in L2TP group view.

Table 2-3 Set condition triggering L2TP Tunnel setup request and LNS address

Operation	Command
Configure to check if the user is VPN user and set IP address of LNS	**start l2tp** { **ip** *ip-addr* [**ip** *ip-addr*] [**ip** *ip-addr*] **...** } { **domain** *domain-name* | **fullusername** *user-name* }
Cancel the Tunnel setup request configuration.	**undo start**

The parameters above have no default values and they can be configured as needed. But at least one triggering condition must be configured for initiating L2TP Tunnel setup request.

📖 **Note:**

When multiple LNSs are configured, since the client PPP connections have different timeout periods, connections to the IP addresses following the first one (that is, connections to the redundant LNSs) may not be able to set up. Thus, you are recommended to configure two LNSs at most.

2.2.4 Setting Tunnel Name

A user can configure local tunnel name on LAC side. The tunnel name of LAC side must keep in line with the remote name of tunnel configured on LNS side.

These configurations are optional on LAC side.

Perform the following configuration inL2TP group view.

Table 2-4 Set local Tunnel name

Operation	Command
Set local Tunnel name.	**tunnel name** *name*
Restore the default local Tunnel name.	**undo tunnel name**

By default, local tunnel name is the hostname of the router.

2.2.5 Setting Tunnel Authentication and Password

As needed, a user can decide whether to start tunnel authentication before creating tunnel connection. Tunnel authentication request can be sent by either LAC side or LNS side. If one end of a tunnel starts tunnel authentication, the other end must also start tunnel authentication in order to set up the tunnel connection. In addition, both ends must use the same password, which cannot be void. Otherwise, the local end will disconnect the tunnel automatically. If tunnel authentication is disabled on both ends, the consistency of password will be insignificant.

These configurations are optional on LAC side.

Perform the following configuration in L2TP group view.

Table 2-5 Set Tunnel authentication and authentication password

Operation	Command
Start Tunnel authentication.	**tunnel authentication**
Disable Tunnel authentication.	**undo tunnel authentication**
Set the password of Tunnel authentication.	**tunnel password** { **simple** | **cipher** } *password*
Restore the password of Tunnel authentication to the default.	**undo tunnel password**

By default, tunnel authentication is enabled, with password of tunnel authentication being null. For the sake of tunnel security, it is not suggested to disable tunnel authentication.

2.2.6 Configuring AVP Hiding

L2TP uses attribute value pair (AVP) to transfer and negotiate some parameter attributes. By default, AVP is transferred in simple text. For security, users can hide AVP data in transmission by using the following configuration. AVP hiding only works when both of the two ends use tunnel authentication.

These configurations are optional on LAC side.

Perform the following configuration in L2TP group view.

Table 2-6 Configure AVP hiding

Operation	Command
Enable AVP hiding	**tunnel avp-hidden**
Restore the default AVP transfer mode	**undo tunnel avp-hidden**

By default, AVP is transferred in simple text.

2.2.7 Setting Hello Interval in Tunnel

In order to check the connectivity of the tunnel between LAC and LNS, LAC and LNS send Hello packets to each other periodically and the receiver will respond upon the receipt of the packets. If LAC or LNS does not receive response from the peer end in a specified interval, it will resend Hello packet and will regard the L2TP tunnel connection has been disconnected if receiving no response after making three transmission attempts. In this case, LAC and LNS need to set up a new tunnel connection.

This configuration is optional on LAC side.

Perform the following configuration in L2TP group view.

Table 2-7 Set Hello interval in a tunnel

Operation	Command
Set Hello interval in a tunnel.	**tunnel timer hello** *hello-interval*
Restore the default Hello interval.	**undo tunnel timer hello**

By default, Hello interval is 60 seconds. If this configuration is not performed on LAC side, LAC will send Hello packet to the peer end at intervals of the default value.

2.2.8 Setting Username, Password and Local User Authentication

If you have configured local authentication when configuring AAA authentication on LAC side, you also need to configure local username and password on this side.

LAC performs user authentication to determine whether a user is a valid VPN user by comparing remote dial-in username and password with usernames and passwords registered at the local end. It originates Tunnel setup request only upon successful authentication. Otherwise, the user will be diverted to other kinds of services.

These configurations are compulsory on LAC side.

I. Configuring user name and password

Table 2-8 Configure a username and password

Operation	Command
Configure a user name and password (in system view).	**local-user** *username*
Delete the current setting (in system view).	**undo local-user** *username*
Configure local user password (in local user view).	**password** { **simple** | **cipher** } *password*

By default, no local username and password are configured at the LAC side.

II. Configuring PPP user authentication mode

Perform the following configuration in interface or virtual template interface view.

Table 2-9 Configure/cancel PPP user authentication mode

Operation	Command
Configure a PPP user authentication mode.	**ppp authentication-mode** { **chap** | **pap** } { **call-in** | **domain** *isp-name* }
Disable PPP user authentication.	**undo ppp authentication-mode**

The interface where you configure local authentication must be the one connected to users.

III. Configuring a PPP domain user and an authentication scheme

Table 2-10 Configure a PPP domain user and an authentication scheme

Operation	Command
Create an ISP domain and enter its view (in system view).	**domain** { *isp-name* | **default** { **disable** | **enable** *isp-name* } }
Delete the specified ISP domain (in system view.	**undo domain** *isp-name*
Configure the local authentication scheme for the PPP domain user. (in ISP domain view).	**scheme local**

2.2.9 Disconnecting an L2TP Connection

A connection can be disconnected for one of these reasons: no user is present, fault occurs on the network, or the administrator requests to do so.

Both LAC side and LNS side can start tunnel disconnection. After a tunnel is disconnected, the control connection and sessions on it are cleared. This tunnel can be set up when a new user dials in.

These configurations are optional on LAC side.

Perform the following configurations in user view.

Table 2-11 Disconnect a connection

Operation	Command
Disconnect a tunnel	**reset l2tp tunnel** { *remote-name* **|** *tunnel-id* }
Disconnect a session	**reset l2tp session session-id** *session-id*
Disconnect a user	**reset l2tp user user-name** *user-name*

2.2.10 Setting Flow Control Function of Tunnel

This configuration can enable/disable the simple flow control function on a tunnel.

Perform the following configuration in L2TP group view.

Table 2-12 Set flow control function of a tunnel

Operation	Command
Enable flow control function of a tunnel.	**tunnel flow-control**
Disable flow control function of a tunnel.	**undo tunnel flow-control**

By default, the flow control function of tunnels is disabled.

2.2.11 Setting the L2TP Session Idle-Timeout Timer

An L2TP session is disconnected automatically if the session is idle or no data is transmitted or received on it for a specified period of time. You may set a session idle-timeout timer to specify this idle period. This period can be 0 seconds, that is, never expired.

Table 2-13 Set the L2TP session idle-timeout timer

Operation	Command
Set the L2TP session idle-timeout timer	**session idle-time** *seconds*
Disable the L2TP session idle-timeout timer	**undo session idle-time**

By default, L2TP session idle-timeout timer never expires.

2.2.12 Configuring the Tunnel-Hold Function of L2TP

Normally, the LAC sets up a tunnel with the LNS only when receiving an L2TP session request from a PPP user. This tunnel is automatically torn down after all PPP sessions are disconnected.

For some applications that require fast connection setup, however, a tunnel must be available beforehand so that the system can set up a session immediately after receiving a PPP session request. To this end, the LAC and the LNS must always maintain a tunnel connection even when no session is present on it.

Perform the following configuration in L2TP group view.

Table 2-14 Configure the tunnel-hold function of L2TP

Operation	Command
Enable the tunnel-hold function of L2TP	**tunnel keepstanding**
Disable the tunnel-hold function of L2TP	**undo tunnel keepstanding**

By default, the tunnel-hold function of L2TP is disabled.

📖 **Note:**

To have the tunnel-hold function take effect, you must configure it on both LAC and LNS.

After you configure the tunnel-tunnel function of L2TP, you can execute the **start l2tp tunnel** command to start a tunnel connection.

Perform the following configuration in L2TP group view.

Table 2-15 Start an L2TP tunnel connection

Operation	Command
Start an L2TP tunnel connection	**start l2tp tunnel**

2.2.13 Setting LAC to Function as Client

Normally, the L2TP client is the host that dials to the LAC, where the connection between the user and the LAC is always PPP connection.

If the LAC is functioning as the client, the connection between the host and the LAC can be an IP connection allowing the LAC to forward the IP packets from the host to the LNS. This is equivalent to creating a virtual PPP user associated with multiple actual users on the LAC and maintaining a permanent connection for it. The IP packets of all these actual users are forwarded to the LNS through this virtual user.

To use the LAC as the client, you must add the following configurations in addition to other LAC configurations:

- Create a virtual template interface
- Configure the parameters of the virtual template interface, including IP address, PPP authentication mode, and username and password for PPP authentication
- Enable the LAC client to set up L2TP tunnel

🕮 **Note:**

When the LAC is functioning as the L2TP client, you must set the L2TP session idle-timeout timer to 0 or disable it, preventing the session of the virtual user is disconnected when no data is transmitted or received.

I. Creating a virtual template interface

Perform the following configuration in system view.

Table 2-16 Create/delete a virtual template interface

Operation	Command
Create a virtual template interface	**interface virtual-template** *virtual-template-number*
Delete a virtual template interface	**undo interface virtual-template** *virtual-template-number*

II. Configuring the parameters of the virtual template interface

Perform the following configuration in virtual template interface view.

Table 2-17 Configure the parameters of the virtual template interface

Operation	Command
Assign an IP address to the virtual template interface	**ip address** *address mask*
Configure a PPP authentication mode	**ppp authentication-mode** { **pap** | **chap** }
Configure the username for CHAP authentication	**ppp chap user** *user-name*
Configure the password for CHAP authentication	**ppp chap password** { **simple** | **cipher** } *password*

Operation	Command
Configure the username and password for PAP authentication	**ppp pap local-user** *user-name* **password** { **simple** | **cipher** } *password*

III. Enabling/disabling the LAC client to set up L2TP tunnel

Perform the following configuration in virtual template interface view.

Table 2-18 Enable/disable the LAC client to set up L2TP tunnel

Operation	Command
Enable the LAC client to set up L2TP tunnel	**l2tp-auto-client enable**
Disable the LAC client to set up L2TP tunnel	**undo l2tp-auto-client enable**

By default, the LAC client is disabled to set up L2TP tunnel.

2.3 LNS Configuration

In LNS configuration task list, L2TP must be enabled and L2TP group must be created before any other functions can be configured. Regarding the configuration of L2TP supporting multi-instance, no configurations can become valid unless the L2TP multi-instance function is enabled. For detailed introduction to related commands of PPP and Virtual-Template, refer to corresponding chapters and sections.

The major configuration tasks on LNS side include:

- Enable L2TP (required)
- Enable L2TP multi-instance function (optional)
- Create L2TP group (required)
- Create virtual template (required)
- Set the parameters for call receiving (required)
- Set tunnel authentication and password (optional)
- Set the transmission mode of AVP data (optional)
- Set Hello interval in the tunnel (optional)
- Configure mandatory local CHAP authentication (optional)
- Configure mandatory LCP renegotiation (optional)
- Set local address and assigned address pool (the former is required and the latter is optional.)
- Set user name and password and configure user authentication (optional)
- Disconnect tunnel by force(optional)
- Set the flow control function of tunnel (optional)

2.3.1 Enabling L2TP

Only after L2TP is enabled can L2TP functions on the router work normally. If L2TP is disabled, the router cannot provide related functions even if parameters of L2TP have been configured.

These configurations are compulsory on LNS side.

Perform the following configuration in system view.

Table 2-19 Enable/disable L2TP

Operation	Command
Enable L2TP.	**l2tp enable**
Disable L2TP.	**undo l2tp enable**

By default, L2TP is disabled.

2.3.2 Enabling L2TP Multi-Instance Function

Only when L2TP multi-instance function is enabled can the router perform LNS for several enterprises. L2TP multi-instance function, mainly used in MPLS-VPN networking, enriches VPN networking portfolio. In actual networking applications, intranet routing is accomplished by vpn-instance. For configurations of vpn-instance, refer to chapters related to MPLS configurations. In Section 2.5.4 L2TP Multi-Instance Networking Application, a brief configuration procedure is described.

In L2TP multi-instance applications, these configurations are compulsory at LNS side.

Perform the following configuration in system view.

Table 2-20 Enable/disable L2TP multi-instance function

Operation	Command
Enable L2TP multi-instance function.	**l2tpmoreexam enable**
Disable L2TP multi-instance function.	**undo l2tpmoreexam enable**

By default, L2TP multi-instance function is disabled. This function is not available when the LAC does not employ agent authentication.

2.3.3 Creating L2TP Group

L2TP group needs to be created in order to fulfill related parameter configurations of L2TP. It allows you not only to configure L2TP functions on the router as needed but also to implement one-to-one and one-to-many networking applications between LAC and LNS easily. L2TP groups are numbered separately on LAC and LNS, so LAC and

LNS only need to keep consistent in the configurations of the involved L2TP groups such as remote name of tunnel, start L2TP and LNS address.

These configurations are compulsory on LNS side.

Perform the following configuration in system view.

Table 2-21 Create/delete L2TP group

Operation	Command
Create L2TP group.	**l2tp-group** *group-number*
Delete L2TP group.	**undo l2tp-group** *group-number*

After L2TP group is created, other configurations related to the L2TP group can be performed in L2TP group view, for example, local name and remote name of tunnel.

By default, no L2TP group is created.

2.3.4 Creating Virtual Template

Virtual template is mainly used to configure parameters of virtual interface created dynamically by the router in operation, e.g. MP logical interface and L2TP logical interface, etc.

These configurations are compulsory on LNS side.

Perform the following configuration in system view.

Table 2-22 Create/delete virtual template

Operation	Command
Create a virtual template.	**interface virtual-template** *virtual-template-number*
Delete the virtual template.	**undo interface virtual-template** *virtual-template-number*

By default, no virtual template is created.

2.3.5 Setting Parameters for Call Receiving

LNS can adopt different virtual templates for receiving tunnel setup request from different LACs. When receiving a tunnel setup request from an LAC, LNS needs to check that the name of LAC is a valid remote name of tunnel before allowing it to create the tunnel.

These configurations are compulsory on LNS side.

Perform the following configuration in L2TP group view.

Table 2-23 Set parameters for call receiving

Operation	Command
Set remote name of tunnel (L2TP group not being 1).	**allow l2tp virtual-template** *virtual-template-number* **remote** *remote-name* [**domain** *domain-name*]
Set remote name of tunnel (L2TP group being 1).	**allow l2tp virtual-template** *virtual-template-number* [**remote** *remote-name*] [**domain** *domain-name*]
Remove remote name of tunnel	**undo allow**

When the group number of L2TP is 1 (the default L2TP group number), you do not need to specify *remote-name*. If *remote-name* is specified in L2TP group view 1, L2TP group 1 will not be regarded as the default L2TP group.

🕮 **Note:**

- Only L2TP group 1 can be set as default group.
- Any computer can initiates a tunnel setup request when L2TP group 1 (the default group) is set.
- The **start** command and the **allow** command are mutually exclusive to each other. After one is configured, another one goes invalid automatically.

2.3.6 Setting Tunnel Authentication and Password

As needed, a user can decide whether to start tunnel authentication before creating tunnel connection. Tunnel authentication request can be sent by either LAC side or LNS side. If one end of a tunnel starts tunnel authentication, the other end must also start tunnel authentication in order to set up the tunnel connection. In addition, both ends must use the same password, which cannot be void. Otherwise, the local end will disconnect the tunnel automatically. If tunnel authentication is disabled on both ends, the consistency of password will be insignificant.

These configurations are optional on LNS side.

Perform the following configuration in L2TP group view.

Table 2-24 Set tunnel authentication and authentication password

Operation	Command
Start tunnel authentication.	**tunnel authentication**
Disable tunnel authentication.	**undo tunnel authentication**

Operation	Command
Set a password for tunnel authentication.	**tunnel password** { **simple** | **cipher** } *password*
Remove the password for tunnel authentication.	**undo tunnel password**

By default, tunnel authentication is enabled, with the password being null. For the sake of tunnel security, you are not recommended to disable tunnel authentication.

2.3.7 Setting Transfer Mode of AVP Data

AVP is adopted in L2TP protocol to move and negotiated some attribute parameters of L2TP. By default, AVP is transferred in plain text. For security, users can hide these AVP in transmission by using the following configuration. The function of hidden VAP only works when both of the two ends use tunnel authentication.

These configurations are optional on LNS side.

Perform the following configuration in L2TP group view.

Table 2-25 Set the transfer mode of AVP data

Operation	Command
Configure hidden AVP data for transfer.	**tunnel avp-hidden**
Restore default transfer mode of AVP.	**undo tunnel avp-hidden**

By default, AVP is transferred in plain text.

2.3.8 Setting Hello Interval in Tunnel

In order to check the connectivity of the tunnel between LAC and LNS, LAC and LNS send Hello packets to each other periodically and the receiver will respond upon the receipt of the packets. If LAC or LNS does not receive response from the peer end in a specified interval, it will resend Hello packet and will regard the L2TP tunnel connection has been disconnected if receiving no response after making three transmission attempts. In this case, LAC and LNS need to set up a new tunnel connection.

This configuration is optional on LNS side.

Perform the following configuration in L2TP group view.

Table 2-26 Set Hello interval

Operation	Command
Set Hello interval.	**tunnel timer hello** *hello-interval*

Operation	Command
Restore the default value of Hello interval.	**undo tunnel timer hello**

By default, Hello interval is 60 seconds. If this configuration is not performed on LNS side, LNS will adopt this default value to send Hello packet to the peer end periodically.

2.3.9 Enabling Mandatory Local CHAP Authentication

After LAC performs agent authentication on a user, LNS can authenticate the user again. The user therefore undergoes authentication twice: once on LAC side and once on LNS side. Only after both the two authentications succeed, can L2TP tunnel be created.

In an L2TP network, LNS side authenticates users in three ways: agent authentication, mandatory CHAP authentication, and LCP re-negotiation.

Among these three authentication approaches, LCP re-negotiation is of the first priority. If both LCP re-negotiation and mandatory CHAP authentication are configured on LNS side, L2TP will choose the former, adopting the authentication mode configured in the associated virtual template.

If only CHAP authentication is configured, LNS will perform CHAP authentication on users.

To perform mandatory CHAP authentication on LNS side, you must configure username, password and user authentication and enable AAA on this side. Mandatory local CHAP authentication is optional on LNS side.

Perform the following configuration in L2TP group view.

Table 2-27 Enable mandatory local CHAP authentication

Operation	Command
Enable mandatory local CHAP authentication.	**mandatory-chap**
Disable local CHAP authentication.	**undo mandatory-chap**

When LNS adopts agent authentication (that is, neither LCP re-negotiation nor mandatory CHAP authentication is configured), the following applies: If no authentication mode is configured in the virtual template, LAC sends to LNS all authentication information received from the user as well as authentication mode configured on LAC side, and LNS side will accept the authentication result on LAC side.

When LNS adopts agent authentication, the following applies: If the authentication mode configured in the virtual template is PAP and the authentication is successful, sessions are permitted to be established. If the authentication mode configured in the virtual template is CHAP and that configured on LAC side is PAP, authentication fails and session cannot be correctly created as the CHAP authentication level demanded by LNS is higher than PAP authentication supplied by LAC.

Local end does not perform CHAP authentication by default.

2.3.10 Forcing LCP to Re-negotiate

For NAS-Initialized VPN, the user first performs PPP negotiation with NAS when PPP session starts. If the negotiation passes, NAS initializes L2TP tunnel connection, and transmits user information to LNS so that LNS can judge whether the user is legal or not according to the received agent authentication information,

But in some cases (e.g. authentication and accounting need performing on LNS side simultaneously), required re-negotiation needs to be created between LNS and the user, and agent authentication information on NAS side will be ignored.

The configuration of mandatory LCP re-negotiation is optional on LNS side.

Perform the following configuration in L2TP group view.

Table 2-28 Enable/disable mandatory LCP re-negotiation

Operation	Command
Enable mandatory LCP re-negotiation.	**mandatory-lcp**
Disable mandatory LCP re-negotiation.	**undo mandatory-lcp**

By default, LCP re-negotiation is not performed.

Despite LCP re-negotiation is enabled, LNS will not perform authentication on the user if authentication is not configured in the associated virtual template. In this case, the user is only authenticated once on LAC side, and the address from the global address pool is assigned to the client directly.

2.3.11 Setting Local Address and Assigning Address Pool

After the L2TP tunnel connection between LAC and LNS is created, LNS should assign IP addresses for VPN users from address pool. Before address pool is specified, you must use the **ip pool** command in system view or domain view to define an address pool. For detailed description about the **ip pool** command, refer to the “Security” part of this manual. If LNS adopts agent authentication, mandatory CHAP authentication, or LCP re-negotiation with authentication, the system uses the address pool configured in domain view for address assignment; if you do not configure the LNS to authenticate or the LNS adopts mandatory LCP re-negotiation that does not include the authentication process, the system uses the global address pool for address assignment.

The address pool configuration is optional on LNS side.

Perform the following configuration in virtual template view.

Table 2-29 Set local address and assigned address pool

Operation	Command
Set local IP address.	**ip address** *X.X.X.X netmask*
Remove the local IP address.	**undo ip address** *X.X.X.X netmask*
Specify an address pool for remote address assignment.	**remote address** { **pool** [*pool-number*] | *X.X.X.X* }
Delete the address pool for remote address assignment.	**undo remote address**

If you do not assign a value to the *pool-number* parameter behind the keyword **pool** when specifying a global address pool, the system will use the default global address pool (address pool 0) for assignment. If you do not assign a value to the *pool-number* parameter behind the keyword **pool** when specifying a domain address pool, the system will use the default domain address pool (domain address pool 0) for assignment. If domain address pool 0 does not exist, the system selects other domain address pools one by one.

2.3.12 Setting Username, Password and User Authentication

On LNS side, if mandatory CHAP authentication has been configured, it needs to configure local registered username and password on LNS side.

LAC performs user authentication to determine whether a user is a valid VPN user by comparing remote dial-in username and password with usernames and passwords registered at the local end. If the authentication passes, the VPN user is allowed to communicate with LNS; if it fails, L2TP will be notified to clear the L2TP connection.

These configurations are optional on LNS side. For more information on how to configure them, refer to the section “2.2.8 Setting Username, Password and Local User Authentication”.

2.3.13 Disconnecting an L2TP Connection

A connection can be disconnected for one of these reasons: no user is present, fault occurs on the network, or the administrator requests to do so.

Both LAC side and LNS side can start disconnection. After a tunnel is disconnected, the control connection and sessions on it are cleared. This tunnel can be set up when a new user dials in.

These configurations are optional on LNS side.

Perform the following configurations in user view.

Table 2-30 Disconnect a connection by force

Operation	Command
Disconnect a tunnel	**reset l2tp tunnel** { *remote-name* **|** *tunnel-id* }
Disconnect a session	**reset l2tp session session-id** *session-id*
Disconnect a user	**reset l2tp user user-name** *user-name*

2.3.14 Enabling/Disabling Flow Control Function of Tunnel

This configuration can enable/disable the simple flow control function on a tunnel.

These configurations are optional on LAC side.

Perform the following configuration in L2TP group view.

Table 2-31 Enable/disable flow control function of a tunnel

Operation	Command
Enable flow control function of a tunnel.	**tunnel flow-control**
Disable flow control function of a tunnel.	**undo tunnel flow-control**

By default, the flow control function of tunnels is disabled.

2.4 Displaying and Debugging L2TP

After performing the above configuration tasks, execute **display** commands in any view to view the running status of L2TP configurations, and to verify the configuration effect. The **debugging** commands can be used in user view.

Table 2-32 Display and debug L2TP

Operation	Command
Display information about the current L2TP users	**display l2tp user**
Display information about the current L2TP tunnels	**display l2tp tunnel**
Display information about the current L2TP sessions	**display l2tp session**
Enable all L2TP information debugging	**debugging l2tp all**
Disable all L2TP debugging	**undo debugging l2tp all**
Enable L2TP control packet debugging	**debugging l2tp control**
Disable L2TP control packet debugging	**undo debugging l2tp control**

Operation	Command
Enable PPP packet content debugging	**debugging l2tp dump**
Disable PPP packet content debugging	**undo debugging l2tp dump**
Enable L2TP error debugging	**debugging l2tp error**
Disable L2TP error debugging	**undo debugging l2tp error**
Enable L2TP event debugging	**debugging l2tp event**
Disable L2TP event debugging	**undo debugging l2tp event**
Enable hidden AVP debugging	**debugging l2tp hidden**
Disable hidden AVP debugging	**undo debugging l2tp hidden**
Enable L2TP payload debugging	**debugging l2tp payload**
Disable L2TP payload debugging	**undo debugging l2tp payload**
Enable L2TP time stamp debugging	**debugging l2tp time-stamp**
Disable L2TP time stamp debugging	**undo debugging l2tp time-stamp**

2.5 L2TP Configuration Example

Both NAS and user end can initiate L2TP calls. They are illustrated separately as follows.

2.5.1 NAS-Initialized VPN

I. Network requirements

A VPN user can access the network of its company's headquarters by taking the following procedure:

- User dials up to access the network.
- NAS performs authentication on this user, and then originates a tunnel setup request to LNS if it is a VPN user.
- After establishing the tunnel with LNS, NAS sends packets to LNS, providing the negotiated information between NAS and VPN users.
- LNS decides whether to accept the connection according to the pre-negotiated information.
- User communicates with the company headquarters by using the tunnel between NAS and LNS.

II. Network diagram

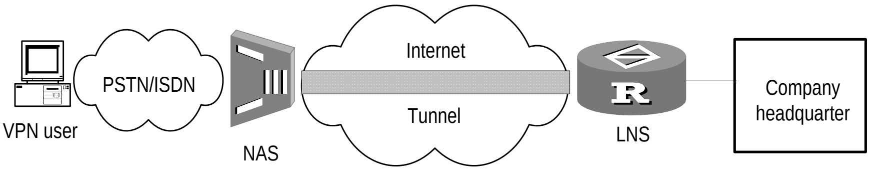


Figure 2-6 Network diagram of NAS-Initialized VPN

III. Configuration procedure

1) Configuration on user end

On user end, input VPN username “vpdnuser” and password “Hello” in dial-up internet window, with dial-in number being 170. Input username “username” and password “userpass” for RADIUS authentication in the dial-up terminal window displayed after dialing.

2) Configuration on NAS side

(In this example 3Com A8010 access server is used as the device on LAC side)

# On A8010, set “170” as the dial-in number.

# On RADIUS access server, configure a VPN user with user name “username” and password “userpass”, and set IP address of the corresponding LNS device (In this example, IP address of the serial port connected with the tunnel on LNS side is 202.38.160.2.).

# Set local device name to A8010, adopt tunnel authentication, set tunnel authentication password to 3Com.

3) Configuration on the router (on LNS side)

# Set user name and password (consistent with the setting on user end).

```
[3Com] local-user vpdnuser
[3Com-luser-vpdnuser] password simple Hello
[3Com-luser-vpdnuser] service-type ppp
[3Com-luser-vpdnuser] quit
```

# Perform local authentication on VPN users.

```
[3Com] domain system
[3Com-isp-system] scheme local
[3Com-isp-system] ip pool 1 192.168.0.2 192.168.0.100
```

# Enable L2TP, and set an L2TP group.

```
[3Com] l2tp enable
[3Com] l2tp-group 1
```

# Configure a virtual template.

```
[3Com] interface virtual-template 1
[3Com-virtual-template1] ip address 192.168.0.1 255.255.255.0
[3Com-virtual-template1] ppp authentication-mode domain chap
[3Com-virtual-template1] remote address pool 1
```

# Configure local name and remote name of the tunnel on LNS side.

```
[3Com] l2tp-group 1
[3Com-l2tp1] tunnel name LNS
[3Com-l2tp1] allow l2tp virtual-template 1 remote A8010
```

# Enable tunnel authentication and set tunnel authentication password.

```
[3Com-l2tp1] tunnel authentication
[3Com-l2tp1] tunnel password simple 3Com
```

2.5.2 Client-Initialized VPN

I. Network requirements

A VPN user access company headquarters following the procedure below:

It first connects to the Internet, and then originates a tunnel setup request to LNS. Upon the acceptance of this request, a virtual tunnel is established between LNS and the VPN user for the data transmission between the user and the company headquarters.

II. Network diagram

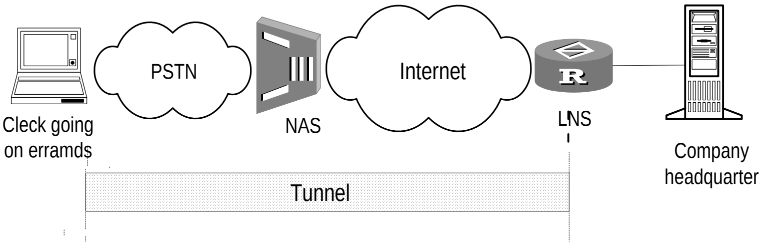


Figure 2-7 Network diagram of Client-Initialized VPN

III. Configuration procedure

1) Configuration on user side:

Make sure that the user-side host is installed with L2TP client software, WinVPN Client for example, and the user is connected to the Internet through a dial-up link before proceeding to perform the following configuration tasks. (The configuration procedure depends on the installed client software).

# Set VPN username to “vpdnuser” and password to “Hello” on user side.

# Set IP address of LNS to the Internet interface address of the router (In this example IP address of the serial port connected with tunnel on LNS side is 202.38.160.2).

# Revise connection attributes. Set adopted protocol to L2TP, encryption attribute to user defined. Choose CHAP authentication for tunnel authentication, with tunnel password being “3Com”.

2) Configuration on the router (on LNS side)

# Set username and password (consistent with the configuration on user side).

```
[3Com] local-user vpdnuser
[3Com-luser-vpdnuser] password simple Hello
[3Com-luser-vpdnuser] service-type ppp
```

# Perform local authentication on VPN users.

```
[3Com] domain system
[3Com-isp-system] scheme local
[3Com-isp-system] ip pool 1 192.168.0.2 192.168.0.100
```

# Enable L2TP and set an L2TP group.

```
[3Com] l2tp enable
[3Com] l2tp-group 1
```

# Configure a virtual template.

```
[3Com] interface virtual-template 1
[3Com-virtual-template1] ip address 192.168.0.1 255.255.255.0
[3Com-virtual-template1] ppp authentication-mode chap domain system
[3Com-virtual-template1] remote address pool 1
```

# Configure local name and remote name of the tunnel on LNS side.

```
[3Com] l2tp-group 1
[3Com-l2tp1] tunnel name LNS
[3Com-l2tp1] allow l2tp virtual-template 1
```

# Enable tunnel authentication and set tunnel authentication password.

```
[3Com-l2tp1] tunnel authentication
[3Com-l2tp1] tunnel password simple 3Com
```

2.5.3 Interconnecting Single User with Headquarters via Router

I. Network requirements

A user needs to communicate with its headquarters, but the network address of the headquarters is a private address, e.g. 10.8.0.0, so the user cannot directly access headquarters’ internal server through the Internet. With VPN, the user can access data of the internal network.

Suppose that the route between the LAC and the LNS is up.

II. Network diagram

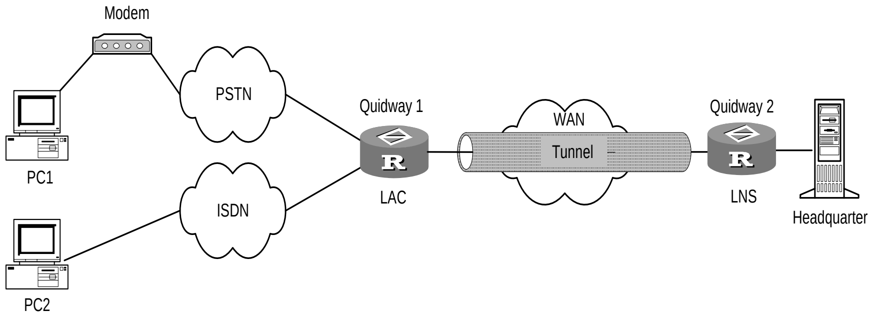


Figure 2-8 Network diagram for interconnecting a single user with its headquarters

III. Configuration procedure

1) Configuration on user side

Create a dialup network, using the access number specified on the router of 3Com1 and accepting network addresses assigned by LNS to users.

Input username “vpdnuser@huawei.com” in the pop-up dial-in terminal window, with password being “Hello” (the username and password have been registered on LNS of the company).

2) Configuration on router 3Com1 (on LAC side)

# Set username and password.

```
[3Com1] local-user vpdnuser
[3Com1-luser-vpdnuser] password simple Hello
[3Com1-luser-vpdnuser] service-type ppp
[3Com1-luser-vpdnuser] quit
```

# Configure IP address on interface Async1/0/0.

```
[3Com1] interface Async1/0/0
[3Com1-Async1/0/0] ip address 202.38.160.1 255.255.255.0
[3Com1-Async1/0/0] ppp authentication-mode chap domain huawei.com
[3Com1-Async1/0/0] quit
```

# Apply local authentication to the domain user **huawei.com**.

```
[3Com1] domain huawei.com
[3Com1-isp-huawei.com] scheme local
```

# Set an L2TP group and configure related attributes.

```
[3Com1] l2tp enable
[3Com1] l2tp-group 1
[3Com1-l2tp1] tunnel name LAC
[3Com1-l2tp1] start l2tp ip 202.38.161.2 domain huawei.com
```

# Enable tunnel authentication and set password of tunnel authentication.

```
[3Com1-l2tp1] tunnel authentication
[3Com1-l2tp1] tunnel password simple 3Com
```

3) Configuration on router 3Com2 (on LNS side)

# Configure an IP address for interface Serial1/0/0.

```
[3Com2] interface serial1/0/0
[3Com2-serial 1/0/0] ip address 202.38.161.2 255.255.255.0
[3Com2-serial 1/0/0] quit
```

# Set the username and password, same as what configured on LAC side.

```
[3Com2] local-user vpdnuser
[3Com2-luser-vpdnuser] password simple Hello
[3Com2-luser-vpdnuser] service-type ppp
[3Com2-luser-vpdnuser] quit
```

# Configure the virtual template of “Virtual-Template 1”.

```
[3Com2] interface virtual-template 1
[3Com2-virtual-template1] ip address 192.168.0.1 255.255.255.0
[3Com2-virtual-template1] ppp authentication-mode chap domain huawei.com
[3Com2-virtual-template1] remote address pool 1
```

# Configure a domain user and specify to use the local authentication scheme.

```
[3Com2] domain huawei.com
[3Com2-isp-huawei.com] scheme local
[3Com2-isp-huawei.com] ip pool 1 192.168.0.2 192.168.0.100
[3Com2-isp-huawei.com] quit
```

# Set an L2TP group and configure related attributes.

```
[3Com2] l2tp enable
[3Com2] l2tp-group 1
[3Com2-l2tp1] tunnel name LNS
[3Com2-l2tp1] allow l2tp virtual-template 1 remote LAC
```

# Enable tunnel authentication and set password of tunnel authentication to 3Com.

```
[3Com2-l2tp1] tunnel authentication
[3Com2-l2tp1] tunnel password simple 3Com
```

# Perform mandatory local CHAP authentication.

```
[3Com2-l2tp1] mandatory-chap
```

2.5.4 L2TP Multi-Instance Networking Application

I. Network requirements

Several enterprises share the same LNS while each of them needs to communicate with its own headquarters. As network addresses of the headquarters’ networks are private addresses, such as 10.8.0.0, the users cannot directly access the internal servers of their own enterprises via the Internet in normal circumstances. However, they can access the resources on the intranets by creating multi-instance-supported VPN.

Suppose the domain names of 01 enterprise headquarters and 02 enterprise headquarters are respectively 263.net and 163.net, and PC1 and PC2 are respectively 01 enterprise user and 02 enterprise user.

II. Network diagram

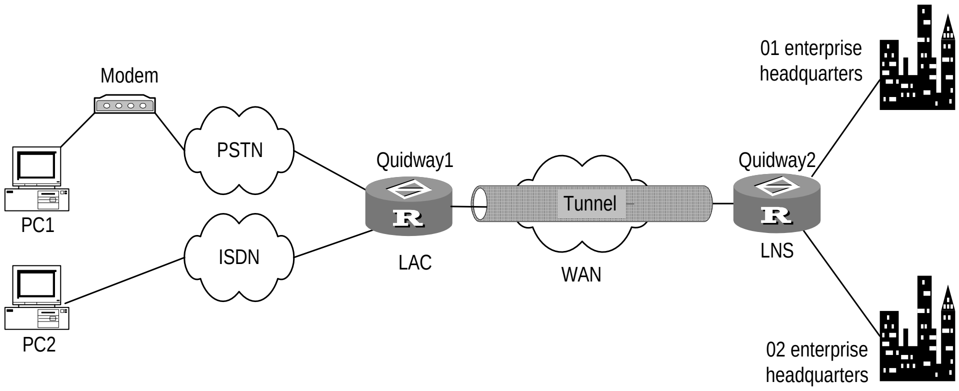


Figure 2-9 Network diagram of multi-instance-supported L2TP

III. Configuration procedure

1) Configuration at user side

Set up a dial network using the access number of 3Com1 Router, and accept addresses assigned by the LNS server to users. On PC1, the user should enter the user name vpdn1@263.net and the password 11111 in the pop-up Dial Terminal Window, supposing that the user name and password have been registered with the LNS.

On PC2, the user should enter the user name vpdn2@163.net and the password 22222 in the pop-up Dial Terminal Window, supposing that the user name and password have been registered with the LNS.

2) Configuration on 3Com1 Router (at LAC side)

# Set username and password.

```
<3Com1> system-view
[3Com1] local-user vpdn1.net
[3Com1-luser-vpdn1] password simple 11111
[3Com1-luser-vpdn1] service-type ppp
[3Com1-luser-vpdn1] quit
[3Com1] local-user vpdn2
[3Com1-luser-vpdn2] password simple 22222
```

```
[3Com1-luser-vpdn2] service-type ppp
[3Com1-luser-vpdn2] quit
```

# Apply local authentication to the domain user.

```
[3Com1] domain 263.net
[3Com1-isp-263.net] scheme local
[3Com1-isp-263.net] quit
[3Com1] domain 163.net
[3Com1-isp-163.net] scheme local
[3Com1-isp-163.net] quit
```

# Enable CHAP authentication on the interface that provides the access service to the dial-up users and configure IP address on BRI1/0/0.

```
[3Com1] interface bri1/0/0
[3Com1-bri1/0/0] ip address 202.38.160.1 255.255.255.0
[3Com1-bri1/0/0] ppp authentication-mode chap
[3Com1-bri1/0/0] ppp authentication-mode chap domain
[3Com1-bri1/0/0] quit
```

# Set two L2TP groups and configure the relevant attributes.

```
[3Com1] l2tp enable
[3Com1] l2tp-group 1
[3Com1-l2tp1] tunnel name LAC
[3Com1-l2tp1] start l2tp ip 202.38.161.2 domain 263.net
[3Com1-l2tp1] l2tp-group 2
[3Com1-l2tp2] tunnel name LAC
[3Com1-l2tp2] start l2tp ip 202.38.161.2 domain 163.net
```

# Enable tunnel authentication and set the password for it.

```
[3Com1-l2tp2] tunnel authentication
[3Com1-l2tp2] tunnel password simple 12345
[3Com1-l2tp2] l2tp-group 1
[3Com1-l2tp1] tunnel authentication
[3Com1-l2tp1] tunnel password simple 12345
```

3) Configuration on 3Com2 Router (at LNS side)

```
<3Com2> system-view
[3Com2] interface serial 1/0/0
[3Com2-Serial1/0/0] ip address 202.38.161.2 255.255.255.0
[3Com2-Serial1/0/0] quit
```

# Create two usernames and passwords.

```
[3Com2] local-user vpdn1
[3Com2-luser-vpdn1] password simple 11111
[3Com2-luser-vpdn1] service-type ppp
[3Com2] local-user vpdn2
```

```
[3Com2-luser-vpdn2] password simple 22222
[3Com2-luser-vpdn2] service-type ppp
[3Com2-luser-vpdn2] quit
```

# Configure the domain users to use local authentication.

```
[3Com2] domain 263.net
[3Com2-isp-263.net] scheme local
[3Com2-isp-263.net] ip pool 1 202.38.160.10 202.38.160.100
[3Com2-isp-263.net] quit
[3Com2] domain 163.net
[3Com2-isp-163.net] scheme local
[3Com2-isp-163.net] ip pool 2 202.38.160.10 202.38.160.100
[3Com2-isp-163.net] quit
```

# Create two vpn-instances.

```
[3Com2] ip vpn-instance vrf1
[3Com2–vpn-instance] route-distinguisher 100:1
[3Com2–vpn-instance] ip vpn-instance vrf2
[3Com2–vpn-instance] route-distinguisher 100:2
[3Com2-vpn-instance] quit
```

# Configure the Ethernet interface connected to 01 enterprise, and bind it with vrf1.

```
[3Com2] interface Ethernet2/0/0
[3Com2-Ethernet2/0/0] ip vpn-instance forwarding vrf1
[3Com2-Ethernet2/0/0] ip address 202.38.160.3 255.255.255.0
```

# Configure the Ethernet interface connected to 02 enterprise, and bind it with vrf2.

```
[3Com2-Ethernet2/0/0] interface Ethernet3/0/0
[3Com2-Ethernet3/0/0] ip vpn-instance forwarding vrf2
[3Com2-Ethernet3/0/0] ip address 202.38.160.4 255.255.255.0
[3Com2-Ethernet3/0/0] quit
```

# Create two virtual templates correspondingly, and bind them with vrf1 and vrf2 respectively.

```
[3Com2]interface virtual-template 1
[3Com2-Virtual-Template1] ip binding vpn-instance vpn-instance1
[3Com2-Virtual-Template1] ppp authentication-mode pap domain 263.net
[3Com2-Virtual-Template1] interface virtual-template 2
[3Com2-Virtual-Template2] ip binding vpn-instance vpn-instance2
[3Com2-Virtual-Template2] ppp authentication-mode pap domain 263.net
[3Com2-Virtual-Template2] quit
```

# Create two L2TP-groups correspondingly.

```
[3Com2] l2tp-group 3
[3Com2-l2tp3] tunnel authentication
```

```
[3Com2-l2tp3] allow l2tp virtual-template 1 remote LAC domain 263.net
[3Com2-l2tp3] tunnel password simple 12345
[3Com2-l2tp3] l2tp-group 4
[3Com2-l2tp4] tunnel authentication
[3Com2-l2tp4] allow l2tp virtual-template 2 remote LAC domain 163.net
[3Com2-l2tp4] tunnel password simple 12345
```

If the LSN side requires RADIUS authentication, you simply need to change the AAA configuration in the configurations described above.

2.5.5 Using LAC as L2TP Client

I. Network requirements

The LAC-side router functions as L2TP client, setting up permanent connection with LNS. All data from the connected private network is forwarded using the connection to the LNS.

II. Network diagram

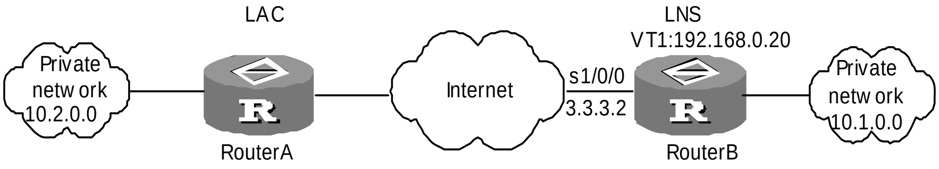


Figure 2-10 Network diagram for using LAC as the L2TP client

III. Configuration procedure

1) Configure Router A, or the LAC-side router

# Enable L2TP and create an L2TP group

```
[RouterA] l2tp enable
[RouterA] l2tp-group 1
```

# Configure the local tunnel name and the IP address of LNS

```
[RouterA-l2tp1] tunnel name LAC
[RouterA-l2tp1] start l2tp ip 3.3.3.2 fullusername vpdnuser
```

# Enable tunnel authentication and set the password

```
[RouterA-l2tp1] tunnel authentication
[RouterA-l2tp1] tunnel password simple 3Com
[RouterA-l2tp1] quit
```

# Configure virtual-template 1

```
[RouterA] interface virtual-template 1
```

```
[RouterA-virtual-template1] ip address ppp-negotiate
[RouterA-virtual-template1] ppp pap local-user vpdnuser password simple Hello
[RouterA-virtual-template1] ppp authentication-mode pap
[RouterA-virtual-template1] quit
```

# Configure static routing to private network 10.1.0.0

```
[RouterA] ip route-static 10.1.0.0 16 virtual-template 1
```

# Add a user name and password.

```
[RouterA] local-user vpdnuser
[RouterA-luser-vpdnuser] password simple Hello
[RouterA-luser-vpdnuser] service-type ppp
```

# Configure interface Serial 1/0/0.

```
[RouterA] interface serial1/0/0
[RouterA-Serial1/0/0] ip address 3.3.3.1 255.255.0.0
[RouterA-Serial1/0/0] quit
```

2) Configure Router B, or the LNS-side router

# Configure username and password

```
[RouterB] local-user vpdnuser
[RouterB-luser-vpdnuser] password simple Hello
[RouterB-luser-vpdnuser] service-type ppp
```

# Enable L2TP and set an L2TP group

```
[RouterB] l2tp enable
[RouterB] l2tp-group 1
```

# Configure virtual template 1

```
[RouterB] interface virtual-template 1
[RouterB-virtual-template1] ip address 192.168.0.20 255.255.255.0
[RouterB-virtual-template1] remote  address  pool 1
[RouterB-virtual-template1] ppp authentication-mode pap
[RouterB-virtual-template1] quit
```

# Configure domain information.

```
[RouterB] domain system
[3Com2-isp-system] scheme local
[3Com2-isp-system] ip pool 1 192.168.0.1 192.168.0.10
[3Com2-isp-system] quit
```

# Configure the local tunnel name and the remote name of the receive tunnel

```
[RouterB] l2tp-group 1
[RouterB-l2tp1] tunnel name LNS
[RouterB-l2tp1] allow l2tp virtual-template 1 remote LAC
```

# Enable tunnel authentication and set the password

```
[RouterB-l2tp1] tunnel authentication
[RouterB-l2tp1] tunnel password simple 3Com
[RouterB-l2tp1] quit
```

# Configure interface Serial 1/0/0.

```
[RouterB] interface serial1/0/0
[RouterB-Serial1/0/0] ip address 3.3.3.2 255.255.0.0
[RouterB-Serial1/0/0] quit
```

# Configure static routing to private network 10.2.0.0

```
[RouterB] ip route-static 10.2.0.0 16 virtual-template 1
```

3) Start L2TP connection

# Start L2TP connection in virtual template interface view on Router A

```
[RouterA] interface virtual-template 1
[RouterA-virtual-template1] l2tp-auto-client enable
```

Note:

LAC-side router and LNS-side router must be the gateways for their connected private networks respectively.

2.5.6 Complex Network Design

3Com Routers can serve as LAC and LNS at the same time, supporting multiple simultaneous incoming calls. L2TP can receive and originate multiple calls as long as memory and line resources are available. These complex networking requirements and their configurations can be implemented by referring to above cases.

Pay special attention to the configuration of static route, because many applications are based on routing to originate calls.

2.6 L2TP Troubleshooting

The VPN tunnel setup process is quite complicated; only several common cases are analyzed here. Before debugging VPN, please confirm that both LAC and LNS are connected to a public network, and are connected correctly.

Symptom 1: User's login fails.

Troubleshooting:

Failure causes are as follows:

- Fail to establish a tunnel because:

1) On LAC side, LNS addresses are improperly set.

2) On LNS side, L2TP group that can receive the remote end of the tunnel is not configured. For details, refer to the description of the **allow** command.

3) Tunnel authentication fails. If authentication is configured, make sure that the same tunnel authentication password is configured at both sides.

4) If the local end compulsorily disconnects the connection but the opposite end fails to receive the "Disconnect" packet due to some network transmission problem, originating tunnel setup request without delay will fail in this case. The reason is that both sides cannot detect the disconnected link within certain time, and the tunnel connections originated by two opposite ends with the same IP address are not allowed.

- PPP negotiation fails because :

5) Error occurs to username or password set on LAC side, or the corresponding users are not set on LNS side.

6) LNS cannot assign addresses, e.g. because the address pool is too small or no address pool is set at all.

7) The types of tunnel password authentication are inconsistent. The default authentication type of VPN connection created by Windows 2000 is MSCHAP. If the peer end does not support MSCHAP, CHAP is recommended for substitution.

Symptom 2: Data transmission fails. After the connection is established, no data can be transmitted, e.g. the peer end cannot be pinged.

Troubleshooting: Possible causes are as follows:

- The address set by the user is wrong: Generally, it is up to LNS to assign addresses, but a user can also designate his own address. If the designated address and the address assigned by LNS are not in the same network segment, this problem occurs. It is recommended that LNS assign addresses completely.
- Network congestion: Congestion occurs to the Internet backbone and packet loss is serious. L2TP uses User Datagram Protocol (UDP) for transmission. Because UDP lacks in error control mechanism, applying L2TP on an unstable line will result in **ping** failures.

Chapter 3 Configuration of GRE

3.1 Brief Introduction to GRE

I. GRE overview

Generic Routing Encapsulation protocol (GRE) can encapsulate datagrams of some network layer protocols (e.g. IP and IPX) and allow these encapsulated datagrams to be transferred in another network layer protocol (e.g. IP). GRE is a layer 3 tunnel protocol of VPN, adopting a technique called Tunnel between protocol layers. Each tunnel is a virtual point-to-point connection and can be regarded as a virtual interface only supporting point-to-point connection in actual situation. The interface provides a tunnel where encapsulated datagrams can be transmitted. And it can also encapsulate and de-encapsulate datagrams at both ends of the tunnel.

To move in a tunnel, a packet must undergo the processes of encapsulation and decapsulation, which are illustrated in Figure 3-1:

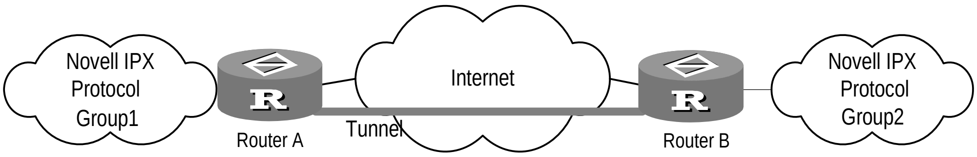


Figure 3-1 IPX network interconnection through GRE tunnel

1) The process of encapsulation

After receiving an IPX packet, the interface connected to Novell group1 first sends it to IPX for processing. IPX decides how to route it by examining the destination address field in its IPX header. If IPX finds that the packet should pass the network 1f (virtual network number of the tunnel) in order to reach the destination, it delivers the packet to the tunnel interface with the network number of 1f. After receiving the packet, the tunnel interface performs GRE encapsulation before forwarding it to the IP module for processing. After the IP header is encapsulated, the packet will be forwarded to the appropriate network interface according to its destination address and the routing table.

2) The process of decapsulation

The process of decapsulation is contrary to that of encapsulation. The system examines the destination address of each IP packet received from the tunnel interface; if it is this router, the system removes the IP header of the packet and sends it to the GRE module for processing (verifying key, checksum, and serial number of the packet, etc.). After completing all the works, the GRE module removes the GRE header of the packet and sends it to the IPX module where it is handled just as a common one.

When receiving a datagram needed encapsulating and routing, called payload, the system first add a GRE header to the datagram to form a GRE packet. This GRE packet is then encapsulated into an IP packet, thus allowing the IP layer to take full charge of the forwarding of the packet. The IP protocol in this particular case is called Delivery Protocol or Transport Protocol.

The format of an encapsulated tunnel packet is shown as follows:

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

Figure 3-2 Format of encapsulated tunnel packets

For instance, an IPX Delivery packet encapsulated in IP tunnel is as follows:

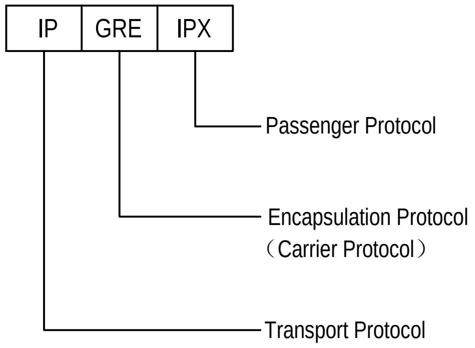


Figure 3-3 Format of Delivery packets in Tunnel

II. Application scope

GRE mainly provides services below:

1) Allowing a multi-protocol local network to make transmission through a single-protocol backbone

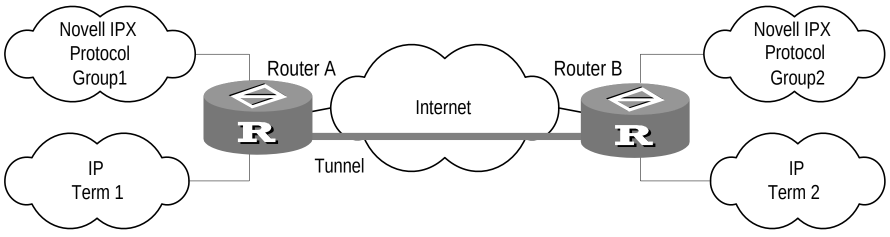


Figure 3-4 Multi-protocol local network that makes transmission through a single-protocol backbone

In the above figure, Group1 and Group2 are the local networks employing the Novell IPX protocol; Term1 and Term2 are the local networks running IP. By setting up a GRE tunnel between Router A and Router B, you can allow Group1 to communicate with Group2 and Term1 with Term2 without interfering with each other.

2) Expanding the operating area of networks running hop-limited protocols (e.g. IPX)

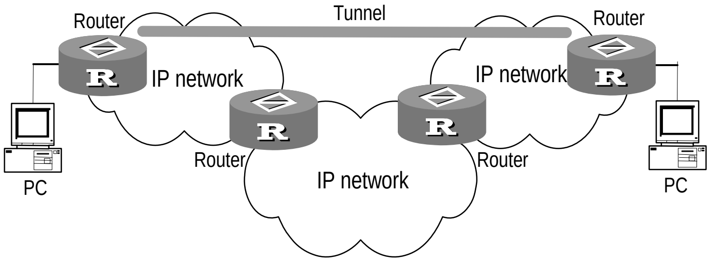


Figure 3-5 Expanding network operating area

If the hop count between two terminals in the above figure is more than 15, the two terminals cannot communicate with each other. By setting up a tunnel across the network, some hops can be hidden, thus expanding the operating area of the network.

3) Connecting some discontinuous sub-networks to establish VPN

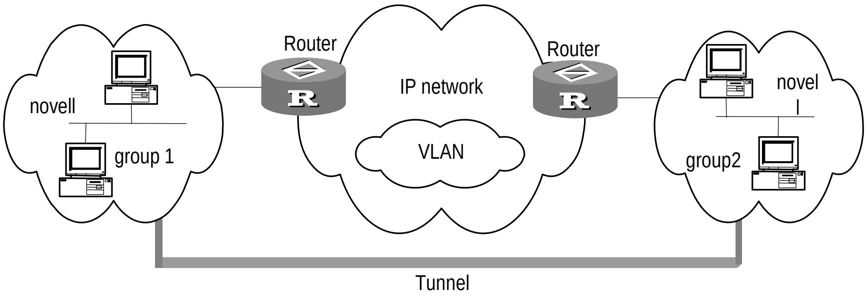


Figure 3-6 Tunnel connecting discontinuous sub-networks

Sub-networks group1 and group2 running Novell IPX are in different cities but they can form a VPN over WAN by using a tunnel.

4) The use in conjunction with IPSec

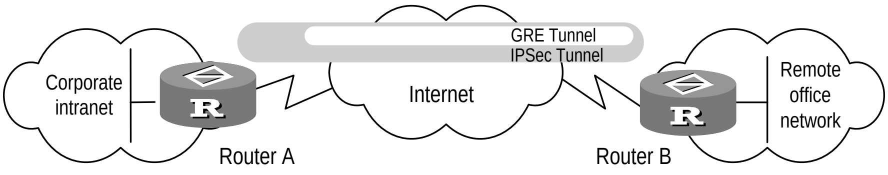


Figure 3-7 GRE-IPSec tunnel application

As illustrated in the above figure, GRE can encapsulate multicast data and transmit the data through the GRE tunnel. As provisioned, IPSec can only protect unicast data at present. When transmitting such multicast data as routing protocol, voice and image in an IPSec tunnel, you can set up a GRE tunnel, encapsulate the multicast data with GRE, and then encrypt the encapsulated data using IPSec. Thus, data secrecy in transmission can be achieved.

In addition, GRE also supports users to select and record identification key of tunnel interface, and supports the end-to-end check of encapsulated message.

Due to the influence of such factors as encapsulation and decapsulation between GRE sender and receiver and data increase caused by encapsulation, the use of GRE may somewhat decrease the data forwarding efficiency of routers.

3.2 GRE Configuration

Among all the configuration tasks, virtual tunnel interface must be created first before other function features can be configured on it. Deleting a virtual tunnel interface deletes all configurations on it.

GRE configuration tasks include:

- Create virtual tunnel interface (required)
- Set encapsulation mode (optional)
- Specify source end of tunnel (required)
- Specify destination end of tunnel (required)
- Set network address of tunnel interface (required)
- Configure end-to-end verification on both ends of tunnel (optional)
- Set identification key of tunnel interface (optional)
- Configure routing via tunnel (optional)

3.2.1 Creating Virtual Tunnel Interface

Virtual tunnel interface should be created so that other parameters of GRE can be configured on it. These configurations are required to be performed on both ends of the tunnel.

Perform the following configuration in system view.

Table 3-1 Create virtual tunnel interface

Operation	Command
Create a virtual tunnel interface.	**interface tunnel** *number*
Delete a virtual tunnel interface.	**undo interface tunnel** *number*

By default, no virtual tunnel interface is created.

The device adopts distributed structure, on which interfaces are represented in a three-dimension way, i.e, *slot/card/port*. The parameter *slot* represents slot number of the specified universal interface module; *card* represents the number of the installed card, which can take on the value of 0 or 1; *port* represents the number of the specified interface, ranging from 0 to 1023, but the actual number of created tunnels depends on the total number of interfaces and available memory.

On creating Tunnel interface, it is recommended that the parameter *slot* should keep in line with the slot of source end interface configured by the **source** command. In other words, slot number specified by *slot* is the same as that of the actual physical interface forwarding GRE packets, thus improving the forwarding efficiency.

3.2.2 Setting Encapsulation Mode

Encapsulation protocol and delivery protocol are to be configured on tunnel interface. You may choose not to configure them on both ends of the tunnel, but if you do configure them, make sure to use the same encapsulation mode on both ends (by far, only GRE is available).

Perform the following configuration in tunnel interface view.

Table 3-2 Set encapsulation mode

Operation	Command
Set encapsulation mode on the tunnel interface.	**tunnel-protocol gre**
Delete the encapsulation mode on the tunnel interface.	**undo tunnel-protocol**

By default, encapsulation protocol is GRE, and delivery protocol is IP.

3.2.3 Specifying Tunnel Source

After the creation of a tunnel interface, the source address of the tunnel, that is, the actual physical interface address where GRE packets are forwarded also needs to be specified. A tunnel is uniquely identified by one source address and one destination address. These configurations are required on both ends of the tunnel, with the source address at one end being the destination address at the other end and vice versa.

Perform the following configuration in tunnel interface view.

Table 3-3 Specify source address or source interface of the tunnel

Operation	Command
Specify source address or source interface of the tunnel.	**source** { *ip-addr* | *interface-type interface-num* }
Delete the source address or source interface of the tunnel.	**undo source**

🕮 **Note:**

- The same source address and destination address cannot be configured on two or more tunnel interfaces encapsulated with the same protocol.
- The **source** command configures actual physical interface address or actual physical interface. In addition, the network address of tunnel interface also needs configuring by using the **ip address** command in tunnel interface view.

3.2.4 Specifying Tunnel Destination

After the creation of a tunnel interface, the destination address of the tunnel, that is, IP address of the actual physical interface receiving GRE packets, also needs to be specified. A tunnel is uniquely identified by one source address and one destination address. These configurations are required on both ends of the tunnel, with the source address at one end being the destination address at the other end and vice versa.

Perform the following configuration in tunnel interface view.

Table 3-4 Specify destination address of the tunnel

Operation	Command
Set destination address of the tunnel.	**destination** *ip-addr*
Delete the destination address of the tunnel.	**undo destination**

🕮 **Note:**

The **destination** command sets IP address of actual physical interface. In order to support dynamic routing protocols, network address of tunnel interface also needs configuring.

3.2.5 Assigning Network Address to Tunnel Interface

You must assign addresses to the interfaces at the ends of a tunnel. The assigned addresses can be private ones but they must belong to the same network segment.

Perform the following configuration in Tunnel interface view.

Table 3-5 Assign network address to a tunnel interface

Operation	Command
Assign an IP address to the tunnel interface.	**ip address** *ip-addr mask*

Operation	Command
Delete the IP address of the tunnel interface.	**undo ip address**

By default, network address of tunnel interface is not configured.

3.2.6 Configuring End-to-End Verification on Both Ends of Tunnel

As RFC1701 provisioned, if the Checksum Present bit in GRE header is set to 1, then the checksum field is present and contains valid information. The sender calculates the checksum according to GRE header and payload information and sends the packet containing the checksum information to the peer end. The receiver calculates the checksum of the received packet and compares it with the one in the packet. If they are consistent, the packet that may be discarded otherwise will be further processed.

Checksum can be enabled or disabled on the two ends of a tunnel as needed. If checksum is enabled only at the local end, the local end will calculate the checksum of each transmitted packet but will ignore the checksum of received packets; on the contrary, if checksum is enabled only at the remote end, the local end will verify the checksum of each received packet but will ignore the checksum of transmitted packets.

Perform the following configuration in tunnel interface view.

Table 3-6 Enable/disable end-to-end verification on both ends of a tunnel

Operation	Command
Enable end-to-end verification on both ends of the tunnel.	**gre checksum**
Disable end-to-end verification on both ends of the tunnel.	**undo gre checksum**

By default, end-to-end verification is disabled on both ends of tunnel.

3.2.7 Setting Identification Key of Tunnel Interface

RFC1701 provisions that if the Key Present bit in the GRE header of a packet is set to 1, the tunnel identification key carried by the packet will be verified between the sender and the receiver. The verification will fail if different identification keys are used, and the packet will be discarded.

Perform the following configuration in tunnel interface view.

Table 3-7 Set identification key of the tunnel interface

Operation	Command
Set identification key of the tunnel interface.	**gre key** *key-number*
Cancel the identification key of tunnel interface.	**undo gre key**

The *key-number* parameter is an integer in the range 0 to 4294967295.

By default, tunnel does not use KEY.

3.2.8 Configuring Routing via Tunnel

Tunnel route, either static or dynamic, must exist on both the source router and the destination router, so that GRE packets can be forwarded properly.

I. Configuring static routing

You may manually configure a route to the destination address, which is the destination address of the packet without GRE encapsulation rather than the destination address of the tunnel, with the next hop being the address of the remote tunnel interface address. This configuration is required at both ends of the tunnel. For details about this configuration, refer to the part “Static Routing Configuration” of this manual. For detailed descriptions on the configuration commands, refer to the *Command Manual* accompanying this manual.

II. Configuring dynamic routing

If dynamic routing protocol is running on the router, you may simply enable this protocol on both the tunnel interface and the router interface directly connected to the private network. This configuration is required on both ends of the tunnel. For details about this configuration, refer to the part “Dynamic Routing Configuration” of this manual. For detailed descriptions on the configuration commands, refer to the *Command Manual* accompanying this manual.

3.2.9 Configuring the keepalive function

Perform the following configuration in tunnel interface view.

Table 3-8 Configure the keepalive function

Operation	Command
Enable the keepalive function of GRE.	**keepalive** *interval times*
Disable the keepalive function of GRE.	**undo keepalive** [*seconds*] [*times*]

By default, the keepalive function of GRE is disabled; *seconds* is set to 10 and *times* to 3.

3.3 Displaying and Debugging GRE

Upon the completion of the above configurations, execute the **display** command in any view to view their running state and to verify the effect of the configurations. The **debugging** command can be used in user view.

Table 3-9 Display and debug GRE

Operation	Command
Display operating state of tunnel interfaces.	**display interface tunnel** *number*
Enable tunnel information debugging.	**debugging tunnel**

3.4 Typical Configuration Examples of GRE

I. Network requirements

Two subnets running IP, Group1 and Group2, are interconnected by using GRE between the routers of 3Com1 and 3Com2.

II. Network diagram

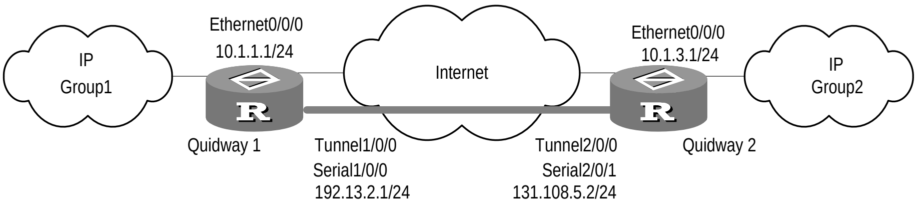


Figure 3-8 Network diagram of GRE application

III. Configuration procedure

1) Configure 3Com1:

# Configure interface Ethernet 0/0/0.

```
[3Com1] interface ethernet 0/0/0
[3Com1-Ethernet0/0/0] ip address 10.1.1.1 255.255.255.0
[3Com1-Ethernet0/0/0] quit
```

# Configure interface Serial 0/0/0 (physical interface of tunnel).

```
[3Com1] interface serial 1/0/0
[3Com1-Serial1/0/0] ip address 192.13.2.1 255.255.255.0
```

```
[3Com1-Serial1/0/0] quit
```

# Create interface Tunnel 1/0/0.

```
[3Com1] interface tunnel 1/0/0
```

# Configure IP address of interface Tunnel 1/0/0.

```
[3Com1-Tunnel1/0/0] ip address 10.1.2.1 255.255.255.0
```

# Configure encapsulation mode of tunnel.

```
[3Com1-Tunnel1/0/0] tunnel-protocol gre
```

# Configure source address of interface Tunnel1/0/0 (IP address of Serial1/0/0).

```
[3Com1-Tunnel1/0/0] source 192.13.2.1
```

# Configure destination address of interface Tunnel1/0/0 (IP address of Serial2/0/1 on 3Com2).

```
[3Com1-Tunnel1/0/0] destination 131.108.5.2
[3Com1-Tunnel1/0/0] quit
```

# Configure static route from 3Com1 to Group2 on interface Tunnel1/0/0.

```
[3Com1] ip route-static 10.1.3.0 255.255.255.0 tunnel 1/0/0
```

2) Configure Router 3Com2:

# Configure interface Ethernet 0/0/0.

```
[3Com2] interface ethernet 0/0/0
[3Com2-Ethernet0/0/0] ip address 10.1.3.1 255.255.255.0
[3Com2-Ethernet0/0/0] quit
```

# Configure interface Serial 2/0/1 (physical interface of Tunnel).

```
[3Com2] interface serial 1/0/1
[3Com2-Serial2/0/1] ip address 131.108.5.2 255.255.255.0
[3Com2-Serial2/0/1] quit
```

# Create interface Tunnel 2/0/0.

```
[3Com2] interface tunnel 2/0/0
```

# Configure IP address of interface Tunnel2/0/0.

```
[3Com2-Tunnel2/0/0] ip address 10.1.2.2 255.255.255.0
```

# Configure encapsulation mode of the tunnel.

```
[3Com2-Tunnel2/0/0] tunnel-protocol gre
```

# Configure source address of interface Tunnel 2/0/0 (IP address of Serial 2/0/1).

```
[3Com2-Tunnel2/0/0] source 131.108.5.2
```

# Configure destination address of interface Tunnel 2/0/0 (IP address of Serial 1/0/0 on Router 3Com1).

```
[3Com2-Tunnel2/0/0] destination 192.13.2.1
[3Com2-Tunnel2/0/0] quit
```

Configure static route from 3Com2 to Group 1 via interface Tunnel2/0/0.

```
[3Com2] ip route-static 10.1.1.0 255.255.255.0 tunnel 2/0/0
```

3.5 GRE Troubleshooting

GRE configuration is relatively simple, except that you should pay more attention to the consistency. Most errors can be located by executing the **debugging tunnel** command. Here, only one type of error is analyzed, as shown in the following figure:

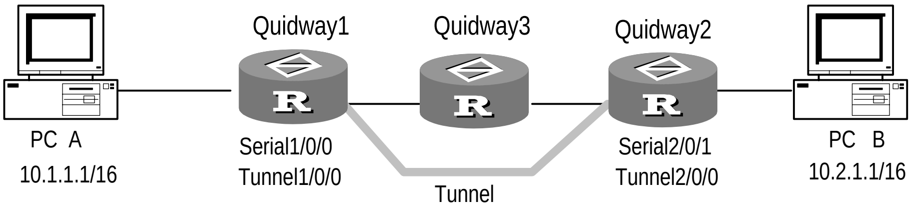


Figure 3-9 Troubleshooting example of GRE

Symptom 1: The interfaces at both ends of the tunnel are correctly configured and both ends of the tunnel can “ping” each other successfully, but PC A and PC B fail to do so.

Troubleshooting: Perform the following steps:

- In user view, perform the **display ip route** command on 3Com1 and 3Com2 respectively, making sure there is the route from interface Tunnel1/0/0 to 10.2.0.0/16 on Router 3Com1, and the route from interface Tunnel 2/0/0 to 10.1.0.0/16 on Router 3Com2.
- If the needed static route do not exist in the output information of the above step, perform the **ip route** command in system view to add it. Taking Router 3Com1 for example, make the following configuration:

```
[3Com1] ip route-static 10.2.0.0 255.255.0.0 tunnel 1/0/0
```

Chapter 4 DVPN

4.1 DVPN Overview

4.1.1 Introduction to DVPN

Dynamic virtual private network (DVPN) technology is a kind of technology that establishes virtual private networks (VPNs) by dynamically acquiring information about the peers. Adopting a non-broadcast multiple access (NBMA) tunneling mechanism, DVPN enables devices to encapsulate and transmit DVPN packets with virtual tunnel interfaces as the end points of DPVN tunnels, and enables devices to learn private network routes through tunnel interfaces dynamically.

DVPN also adopts a client-server model to overcome the drawbacks that the traditional VPN technology suffers from. By registering with a server, clients store their information on the server. Therefore, a registered client can acquire information about other registered clients through the redirect function of the server and then establish separate sessions with those clients. By registering with the same server, multiple DVPN-enabled access devices can form a DVPN domain, implementing the interconnection of the VPNs behind the access devices.

4.1.2 Basic DVPN Concepts

I. DVPN domain

A set of private networks and their routers that are interconnected using DVPN.

II. DVPN access device

A router for building DVPNs across networks. Any router that supports DVPN can be a DVPN access device.

III. DVPN server

The DVPN access device that acts as the server in a DVPN domain. The other DVPN access devices must register with the DVPN server before they can access the DVPN domain. A DVPN sever has these functions:

- Store and maintain registration information about DVPN clients.
- Authenticate clients that apply for accessing the DVPN domain.
- Forward packets between clients with no sessions established, and send redirect packets to source clients.
- Encrypt packets using IPSec.

IV. DVPN client

A DVPN access device that operates as a client in a DVPN domain. A client must successfully register with the DVPN server to access a DVPN domain. A DVPN client does these things:

- Initiate registration with the DVPN server to join a DVPN domain.
- Establish sessions with the DVPN server for data transmission.
- Establish sessions with other DVPN clients in the DVPN domain automatically.
- Encrypt packets using IPSec.

V. DVPN ID

The unique identifier of a DVPN domain. A DVPN access device can belong to multiple DVPN domains and therefore have multiple DVPN IDs.

VI. Map

A registration channel, called map, is established between a DVPN client and a DVPN server when the DVPN client attempts to register with the DVPN server. After the client gets registered, the map remains there until the DVPN client exits the DVPN domain or the network. Both the client and the server keep information about the map, including the ID of the DVPN domain, the private and public IP addresses of the peer, the UDP port used, and the status, type, and control ID of the map.

VII. Session

DVPN tunnel for data transmission. In a DVPN domain, sessions are established between pairs of DVPN access devices for connecting private networks. Similar to map information, session information includes the ID of the DVPN domain, the private and public IP addresses of the peer, the UDP port used, the status of the session, and the type of the session.

VIII. Redirect

Packet redirect mechanism. For two clients with no session, communications between them rely on the DVPN server. Before forwarding packets between two clients, the DVPN server determines whether a separate session can be established between the two clients. If possible, the DVPN server sends a redirect packet carrying information about the destination client to the initiating client so that they may set up a session directly.

IX. Active side and passive side

For the two ends of a session, one end must be the active side, and the other must be the passive side. If a session is established between a client and a server, the client acts as the active side and the server acts as the passive side. If a session is established between two clients, the one that initiates the session is the active side and the other is the passive side.

4.1.3 Operation of DVPN

Each DVPN access device in a DVPN domain runs the proprietary DVPN protocol. The DVPN server holds information about all registered clients, and each client holds information about all sessions it has established, including the private IP address of the destination device (the IP address of the tunnel interface), the public IP address of the destination device (the IP address of the WAN interface), the UDP port of the destination device (when employing UDP), and the status of the session.

The following is a brief description of the interactive operations between the server and a client in three phases.

I. Registration phase

For a client with the interface properties and server address configured, when its interfaces come up, it registers with the server, completing processes including algorithm negotiation, key negotiation, authentication (optional), information registration, and policy issuing.

During the registration phase, a map is created between the client and the server. All the activities in this phase depend on the map. Throughout the lifetime of the client, the client and the server hold a corresponding map respectively; the maps are removed only when the client exits the DVPN domain. Once a map is removed, the client releases all resources that it occupies (including all sessions) and goes back to the initial state.

Figure 4-1 demonstrates the registration procedure. Any error coming forth during the procedure can terminate the procedure and put the client back to the initial state.

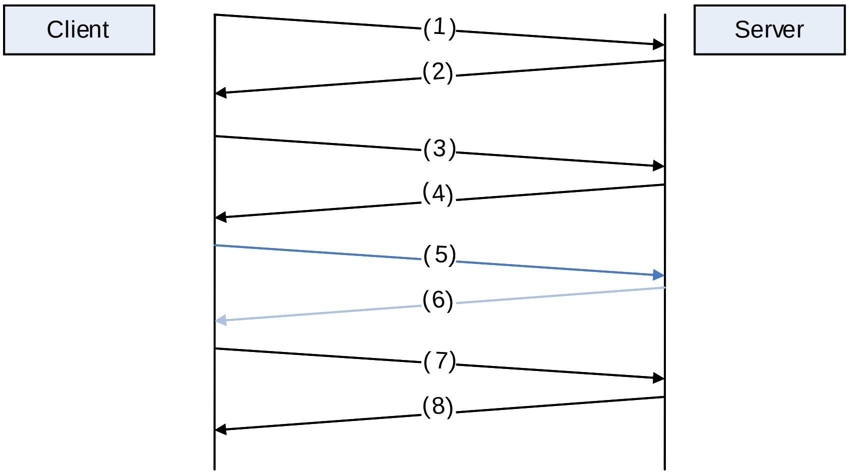


Figure 4-1 DVPN registration procedure

1) The client sends an algorithm negotiation request message to the server.
2) The server sends an algorithm negotiation response message to the client.

3) The client sends key negotiation request and server authentication request to the server.
4) The server sends a key negotiation response message, a client authentication message, and a server authentication response message to the client.
5) The client sends its own authentication information to the server.
6) The server sends the authentication result to the client.
7) The client sends a registration request message to the server, which includes all information about the client.
8) The server sends the registration response information to the client, among which are items such as data encryption policy, key, and DVPN ID.

📖 **Note:**

A DVPN server allows up to 5000 clients to register with it. A DVPN domain can accommodate up to 1024 registered clients.

II. Session establishment phase

Upon successful registration, the client immediately establishes a session with the DVPN server to transmit packets using DVPN. If the server receives a packet destined for a network other than the local private network, it forwards the packet and sends a next hop redirect notification message to the source client, informing the client of information about the destination. Once receiving the redirect message, the client sends a session establishment request to the peer client. After the two clients go through session establishment negotiation (including the negotiation of the IPSec SA for the session), a separate session is established between the two clients. Since then, the two clients can communicate with each other directly without the server.

Before a session is removed, a judgment is made about whether the session is coupled with a registration map. If not, the session is removed directly. Otherwise, the map must be removed at first.

III. Data transmission phase

Data transmission phase starts after a session is established between clients. All data is transmitted among the clients and server over sessions. The data being transmitted is secured using IPSec, with DES as the encryption algorithm and MD5 as the authentication algorithm.

During this phase, all data transmitted is protected by the previously mentioned algorithms by default. You do not need to perform any configuration.

4.1.4 Basic Network Structure

DVPN adopts a client/server model. Among all the access devices in a DVPN domain, only one can be the server and uses a fixed public IP address, whereas the others operate as clients. You must configure information about the server manually on each client to enable the client to register with the server. A session is automatically established between a client and the server after the client successfully registers with the server. By sending redirect packets, the server can provide a client with information about other clients to establish sessions between clients. In this way, the DVPN domain becomes a fully meshed topology.

Both DVPN control packets and data packets are encapsulated using UDP. Therefore, DVPN tunnels can be established across NAT gateways to allow clients using private IP addresses to communicate.

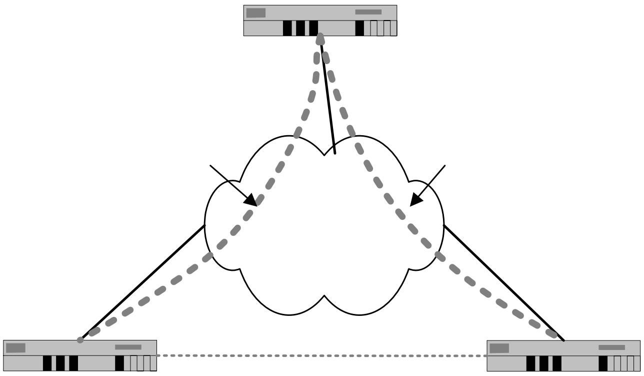


Figure 4-2 A simple DVPN network diagram

4.1.5 Traditional VPN versus DVPN

I. Drawbacks of the traditional VPN

The current VPN solutions commonly use generic routing encapsulation (GRE) or multiprotocol label switching/border gateway protocol (MPLS/BGP), and the VPNs constructed by using either technology suffer from the following drawbacks:

- Complicated in networking and configuration. Layer 3 VPN technologies employs point-to-point tunneling schemes. To establish a fully meshed VPN when the number of access points is N, the number of point-to-point VPN tunnels to be manually configured is N * (N-1)/2.
- Inconvenient in maintenance and expansion. To add a node or change the configuration of a node in an established VPN, you must reconfigure all other nodes, which results in high maintenance cost.
- GRE cannot traverse NAT gateways. For VPN tunnels that are established using GRE and have network address port translation (NAPT) gateways deployed at

egresses, you must map each private IP address to a unique public IP address. This leads to the requirement for a large amount of public IP addresses. Therefore, GRE is not applicable for scenarios with NAT gateways. VPNs established using early versions of IPSec does not support NAT traversal either. NAT traversal is implemented by encapsulating IPSec packets in UDP packets now.

- GRE is not applicable for scenarios with dynamic IP addresses. VPN tunnels established using GRE are based on fixed IP addresses. Using GRE, you cannot establish VPNs for dial-up subscribers at all.
- Not secure. Layer 2 tunneling protocol (L2TP) and GRE do not encrypt the transmitted packets. Whereas, IPSec provides the most secure protection for packets forwarded across IPSec VPNs.
- IPSec VPN does not support dynamical routes. VPN tunnels that are established using GRE and L2TP are interface-based, whereas those that are established using IPSec are flow-based. Therefore, route learning is not possible between private networks interconnected using IPSec VPN tunnels, which is contradictory to dynamic network planning.

II. Advantages of DVPN

DVPN provides all the advantages from which traditional VPN benefits and overcomes lots of problems that traditional VPN faces. It is more suitable for modern and future networks. DVPN has the following features:

- Easy to configure. Instead of configuring one logical interface as the tunnel end for each tunnel, you need only to configure one logical tunnel interface for a DVPN access device to establish sessions with multiple other DVPN access devices. This simplifies DVPN configuration remarkably and improves network maintainability and extensibility. In addition, to add a private network to an existing DVPN domain, you only need to configure information about the DVPN server of the DVPN domain on the DVPN access device(s) of the private network.
- Supporting NAT traversal. UDP-encapsulated DVPN packets can traverse NAT gateways. This enables VPN connections to be established between the internal DVPN access devices and the public network DVPN access devices, making the private networks connected to the NAT gateways form a VPN together with the external private networks.
- Supporting to establish dynamic IP address-based VPNs. For a DVPN client to establish a tunnel in a DVPN domain, it requires only to be configured with the IP address of the DVPN server; it even does not need to know what IP address it is using. This makes DVPN perfect for applications using dynamical IP addresses, such as applications based on plain dial-up and xDSL.
- Capable of establishing tunnels automatically. A DVPN server maintains information about all DVPN access devices in the DVPN domain. The redirect function enables a DVPN client to acquire information about any other DVPN client in the DVPN domain from the DVPN server and then establish a session

with the client. A DVPN client requires only being configured with information about itself and the DVPN server; it does not need any information about other clients. This remarkably eases the network maintenance and administration burden.

- Encrypted registration. When registering with a DVPN server, a client first negotiates with the server for the algorithm suite and keys, which are used to encrypt the key registration information (such as the user name and password) for security and to verify the registration messages.
- Authentication. When registering with a DVPN server, a client can authenticate the server using a pre-shared key to make sure the DVPN server is valid. The DVPN server, in turn, can authenticate the clients that want to access the DVPN domain using AAA to ensure that only authenticated DVPN clients can access the DVPN domain.
- Unified policy management. The DVPN server issues the policy of the DVPN domain to each registered client, and therefore all sessions in a DVPN domain share the same policy. A policy includes the algorithm suite used in session negotiation, the keepalive time of session, the idle timeout time of session, the IPSec encryption algorithm, the renegotiation time of IPSec SA, and so on.
- Encryption during session negotiation. In the course of session negotiation, all the session control packets are IPSec-encrypted using the algorithm suite issued by the DVPN server. That is, when negotiating with the DVPN server about the IPSec SA for data communications over the session, the client employs the encryption and authentication algorithms issued by the DVPN server. Diffie-Hellman (DH) is used for negotiating the key for the IPSec SA. Data to be transmitted through this session can be encrypted as needed using the IPSec SA negotiated in the course of the session establishment and then forwarded through the DVPN domain. The IPSec SA of a session can be renegotiated. You can specify an IPSec SA renegotiation interval to improve the security of data.
- Support for multiple DVPN domains. A single DVPN device can serve multiple DVPN domains. For example, a router can belong to both DVPN domain A and DVPN domain B simultaneously, and a DVPN device can be a client in DVPN domain A and the DVPN server in DVPN domain B at the same time. A DVPN device can serve up to 200 DVPN domains and can be the DVPN server of up to 200 DVPN domains at a time. This not only improves networking flexibility remarkably, but also enables you to make full use of network devices, and therefore can reduce user investment. For a single DVPN device to serve multiple DVPN domains, you must isolate these DVPN domains using private network routes.
- Support for dynamic routes. In a DVPN domain, route packets that need to be transmitted through tunnel interfaces can be broadcast over all sessions to enable automatic route learning in the DVPN domain. Together with dynamic routing protocols, DVPN can simplify the planning of private networks that need to access

a DVPN domain and the configuration of the entire network, dramatically improving network maintainability and automation degree.

4.1.6 Extended DVPN Function

Along with RADIUS server, DVPN server can implement accounting of DVPN users.

When completing authentication/authorization of a DVPN client, the DVPN server records the user information of the DVPN client. After a session is established between the DVPN client and the DVPN server, the DVPN server encapsulates information such as the user name and the login time into the accounting start request, and sends the request to the configured RADIUS server. Upon receiving the accounting start request, the RADIUS server starts accounting and sends an accounting start response to the DVPN server.

When the DVPN client logs out, the DVPN server sends an accounting stop request to the RADIUS server. Upon receiving the accounting stop request, the RADIUS server stops accounting and responds with an accounting stop acknowledgement.

After the RADIUS server starts accounting, accounting stop requests may fail to reach the RADIUS server due to line or device failure, resulting in incomplete user accounting information. To solve this problem, the DVPN server sends real time accounting packets to the RADIUS server at a specified interval after the RADIUS server starts accounting. The RADIUS server records the DVPN client information in the real time accounting packets and responds to the DVPN server accounting acknowledgements. If the DVPN server receives no response to the real time accounting packet, it retransmits the packet at an interval. When the DVPN server has transmitted the packet for the specified maximum attempts, if accounting optional is enabled on the DVPN server, the DVPN server does not send the real time accounting packet any more but maintains the DVPN connection. If accounting optional is not enabled on the DVPN server, the DVPN server will tear down the DVPN connection.

Note:

- You can configure the interval for sending real time accounting packets on the RADIUS server using the **timer realtime-accounting** command. By default, the interval is 12 minutes. For detailed configuration information, refer to the “Security” part of the manual.
- If the DVPN server receives no response to the real time accounting packet from the RADIUS server, it retransmits the packet for the maximum times specified by using the **retry realtime-accounting** command. The default maximum number for sending the real time accounting packet is 5. For details, refer to the “Security” part of the manual.

4.2 DVPN Configuration

DVPN configuration comprises client configuration and server configuration.

I. Client configuration

DVPN client configuration includes basic configuration, tunnel interface configuration, and DVPN class configuration.

1) Basic configuration

Basic client configuration tasks are described in the following sections:

- Enabling/disabling DVPN
- Configuring the registration interval
- Configuring the maximum number of registration
- Configuring the dumb interval

2) Tunnel interface configuration

Tunnel interface configuration tasks are described in the following sections:

- Configuring the encapsulation format
- Configuring the type of the tunnel interface
- Configuring the source address of the tunnel interface
- Applying the DVPN class to the tunnel interface (for the client only)
- Configuring the DVPN domain to which the tunnel interface belongs
- Configuring the data stream to be encrypted using IPSec
- Configuring the registration type of a client (optional)

3) DVPN class configuration

You can use the commands in DVPN class view to configure parameters that are necessary for a client to register with a DVPN server, and to provide information used in negotiation. DVPN class configuration tasks are described in the following sections:

- Creating a DVPN class and entering its view
- Configuring the public IP address of the DVPN server
- Configuring the private IP address of the DVPN server (optional)
- Configuring the algorithm suite used during registration (Optional. Defaults to des-md5-dh1.)
- Specifying how the client authenticates the DVPN server (optional)
- Configure the pre-shared key of the DVPN server (optional)
- Configuring the user name and password of the client (optional)

II. Server configuration

DVPN server configuration includes basic configuration, tunnel interface configuration, and DVPN policy suite configuration.

1) Basic configuration

Basic server configuration tasks are described in the following sections:

- Enabling/disabling DVPN
- Configuring the pre-shared key (optional)
- Configuring the map aging time
- Configuring how to authenticate a client
- Configuring a local user for a client (optional)
- Configure a service for the user to use (optional)

2) Tunnel interface configuration

Tunnel interface configuration tasks are described in the following sections:

- Configuring the encapsulation format
- Configuring the type of the tunnel interface
- Configuring the DVPN domain to which the tunnel interface belongs
- Configuring the source address of the tunnel interface
- Configuring the data stream to be encrypted using IPSec
- Applying the DVPN policy to the tunnel interface (for the server only) (optional)

3) DVPN policy suite configuration

DVPN policy suite configuration tasks are described in the following sections:

- Creating a DVPN policy and entering its view
- Configuring how the DVPN server authenticates the clients (Optional. Defaults to NONE.)
- Configuring an encryption algorithm suite for sessions (Optional. Defaults to des-md5-dh1.)
- Configuring the idle timeout period for the sessions (Optional. Defaults to 300 seconds.)
- Configuring the interval for sending keepalive packets (Optional. Defaults to 10 seconds)
- Configuring the session request interval (Optional. Defaults to 10 seconds.)
- Configuring the IPSec algorithm suite (Optional. Defaults to des-md5-dh1.)
- Configuring the lifetime of the IPSec SA (Optional. Defaults to 3,600 seconds.)

Since some commands must be configured on both the server and the clients, the following describes the configuration tasks by category: basic configuration for the server, basic configuration for the clients, tunnel interface configuration, DVPN class configuration, and DVPN policy configuration.

4.2.1 Configuring a DVPN Server (Basic Configuration)

I. Enabling/disabling DVPN

Use these commands to enable/disable DVPN on a device. If you disable DVPN on a DVPN server, the existing DVPN sessions are removed after they time out.

Perform the following configuration in system view on a DVPN server.

Table 4-1 Enable/disable DVPN

Operation	Command
Enable DVPN	**dvpn service enable**
Disable DVPN	**dvpn service disable**

DVPN is enabled by default.

II. Configuring the pre-shared key

Use these commands to configure/remove identity authentication information (that is, the pre-shared key) on a DVPN server. For a client to authenticate the server using a pre-shared key, you must configure the pre-shared-key used by the DVPN server on the client. Note that the same pre-shared key must be configured on the client and server.

Perform the following configuration in system view on a DVPN server.

Table 4-2 Configure a pre-shared key for a DVPN server

Operation	Command
Configure a pre-shared key for a DVPN server	**dvpn server pre-shared-key** *key*
Remove the pre-shared key of a DVPN server	**undo dvpn server pre-shared-key**

No pre-shared key is configured by default.

III. Configuring how to authenticate a client

A DVPN server can authenticate a client attempting to access the DVPN domain. The currently supported authentication methods are password authentication protocol (PAP) authentication and challenge authentication protocol (CHAP) authentication. After you specify the method for authenticating clients on a DVPN server, the DVPN server authenticates the clients with the specified method if no DVPN policy is configured.

Perform the following configuration in system view on a DVPN server.

Table 4-3 Configure how to authenticate a client

Operation	Command
Configure how to authenticate a client	**dvpn server authentication-client method** { **none** | **chap** | **pap** }

A DVPN server does not authenticate clients by default.

IV. Configuring the map aging time

You can configure a map aging time on the DVPN server, so that the server can delete maps related to unsuccessful registration. If a client successfully registers with the server, the map for the client and the server coexists with the created session.

Perform the following configuration in system view.

Table 4-4 Configure the map aging time

Operation	Command
Configure the map aging time	**dvpn server map age-time** *time*
Restore the default map aging time	**undo dvpn server map age-time**

The default map aging time is 30 seconds.

V. Configuring a local user for a client

On a DVPN server that is configured to authenticate clients, you must configure a local user and a password for each client. When registering with a DVPN server of this kind, a client can pass the authentication only when the user name and password it provides match those configured on the DVPN server.

Perform the following configuration in system view.

Table 4-5 Configure the user name and password for a client to use when registering

Operation	Command
Create a local user	**local-user** *user-name*
Remove a local user	**undo local-user** { **user-name** | **all** }
Set a password for the local user (in local user view)	**password** { **cipher** | **simple** } *password*
Remove the password of the local user (in local user view)	**undo password**
Configure a service for the user to use	**service-type** { **telnet** | **ssh** | **terminal** | **pad** | **dvpn** }
Disable a service the user uses	undo service-type { telnet | ssh | terminal | pad | dvpn }

4.2.2 Configuring a Client (Basic Configuration)

I. Enabling/disabling DVPN

Use these commands to enable/disable DVPN on a device. If you disable DVPN on a DVPN server, the existing DVPN sessions are removed after they time out.

Perform the following configuration in system view on a client or a DVPN server.

Table 4-6 Enable/disable DVPN

Operation	Command
Enable DVPN	**dvpn service enable**
Disable DVPN	**dvpn service disable**

DVPN is enabled by default.

II. Configuring the registration interval

If a client fails one registration with a DVPN server, it can retry after a specified interval. Use this command to configure the registration interval of a client.

Perform the following configuration in system view on a client.

Table 4-7 Configure the registration interval

Operation	Command
Configure the registration interval	**dvpn client register-interval** *time-interval*
Restore the default registration interval	**undo dvpn client register-interval**

The default registration interval is 10 seconds.

III. Configuring the maximum number of registration attempts

When registering with the DVPN server, a client can try for a specified number of times. If all attempts fail, the client turns to the dumb state. Use this command to configure the maximum number of times for which a client can try during a registration round.

Perform the following configuration in system view on a client.

Table 4-8 Configure the maximum number of registration attempts

Operation	Command
Configure the maximum number of registration attempts	**dvpn client register-retry** *times*
Restore the default maximum number of registration attempts	**undo dvpn client register-retry**

The default maximum number of registration attempts is 3.

IV. Configuring the dumb interval

When registering with the DVPN server, a client can try for a specified number of times. If all attempts fail, the client turns into the dumb state. A client in the dumb state cannot register with the DVPN server. After a specified interval called the dump interval elapses, the client becomes active and can register with the DVPN server again. Use this command to specify the dumb interval.

Perform the following configuration in system view on a client.

Table 4-9 Configure the dumb interval

Operation	Command
Configure the dumb interval	**dvpn client register-dumb** *time*
Restore the default dumb interval	**undo dvpn client register-dumb**

The default dumb interval is 300 seconds.

4.2.3 Configuring the Tunnel Interface

I. Configuring the encapsulation format

Before configuring other DVPN parameters, be sure to configure the encapsulation format of UDP DVPN on the tunnel interface.

Perform the following configuration in tunnel interface view on a client or a server.

Table 4-10 Configure the encapsulation format

Operation	Command
Set the encapsulation format to UDP DVPN	**tunnel-protocol udp dvpn**

A tunnel interface uses the GRE encapsulation format by default.

II. Configuring the type of the tunnel interface

Configure the type of the tunnel interface as server on a DVPN server, and as client on a DVPN client.

Perform the following configuration in tunnel interface view on a client or a server.

Table 4-11 Configure the type of the tunnel interface

Operation	Command
Configure the type of the tunnel interface	**dvpn interface-type** { **client** | **server** }

The type of the tunnel interface is client by default.

III. Configuring the DVPN domain to which the tunnel interface belongs

Use this command to configure the ID of the DVPN domain to which the tunnel interface belongs. Tunnel interfaces belonging to the same DVPN domain must be configured with the same DVPN ID.

Perform the following configuration in tunnel interface view on a client or a server.

Table 4-12 Configure the DVPN domain to which the tunnel interface belongs

Operation	Command
Configure the DVPN domain to which the tunnel interface belongs	**dvpn dvpn-id** d*vpn-id*
Remove the configured DVPN ID	**undo dvpn dvpn-id**

A tunnel interface is not configured with a DVPN ID by default.

IV. Configuring the source address of the tunnel interface

The source address or source interface of a tunnel interface refers to the address of the physical interface DVPN packets are sourced from. A source address and destination address pair uniquely identifies a tunnel. You must configure the source address and destination address for a tunnel on both the server and the client. Note that the source address of a tunnel on the server is the destination address of the tunnel on the client, and vice versa.

Perform the following configuration in tunnel interface view on a client or a server.

Table 4-13 Configure the source address of the tunnel interface

Operation	Command
Configure the source address or source interface of the tunnel interface	**source** { *ip-address* | *interface-type interface-number* }
Remove the source address or source interface of the tunnel interface	**undo source**

V. Applying the DVPN class to the tunnel interface (for the client only)

After configuring the DVPN server in DVPN class view on the client, use the following command to apply a DVPN class.

Perform the following configuration in tunnel interface view on the client.

Table 4-14 Apply a DVPN class to the tunnel interface

Operation	Command
Apply a DVPN class to the tunnel interface	**dvpn server** *dvpn-class-name*

Operation	Command
Disable a DVPN class on the tunnel interface	**undo dvpn server** *dvpn-class-name*

A tunnel interface has no DVPN class applied by default.

VI. Applying the DVPN policy to the tunnel interface (for the server only)

After configuring the policy in DVPN policy view on the server, use the following command to apply it to the DVPN domain.

Perform the following configuration in tunnel interface view on the server.

Table 4-15 Apply the DVPN policy to the tunnel interface

Operation	Command
Apply the DVPN policy to the tunnel interface	**dvpn policy** *dvpn-policy-name*
Disable the DVPN policy applied to the tunnel interface	**undo dvpn policy** *dvpn-policy-name*

A tunnel interface does not have a DVPN policy applied by default.

VII. Configuring the data stream to be encrypted using IPSec

Packets forwarded in a DVPN domain are encrypted using IPSec by default. You can have packets that match specified ACLs not encrypted by performing the following operations.

Note:

This command must be configured in combination with the **acl** and **rule** commands, and the **rule** command must be configured with the **deny** keyword, which specifies packets denied by the **rule** command are not encrypted using IPSec. Otherwise, this command does not take effect.

Perform the following configuration in tunnel interface view.

Table 4-16 Configure the data stream to be encrypted using IPSec

Operation	Command
Specify the data streams to be excluded from IPSec encryption	**dvpn security acl** *acl-number*

Operation	Command
Restore the default encryption mode of data streams	**undo dvpn security acl**

All packets that pass through the tunnel interface are encrypted using IPSec by default.

VIII. Configuring the registration type of a client

The registration packets a client sends to the DVPN server can carry additional information, which can be of the forward type, or the undistributed type. The DVPN server determines whether to send redirect packets according to the additional information.

If you configure the additional information of a client as the forward type, the client will not be able to establish any session with any other clients in the DVPN domain. If you configure the additional information of a client as the undistributed type, the DVPN server notifies no client in the DVPN domain of the redirect packets about the client; however, the DVPN server still notifies the client of redirect packets about other clients. So the client can still establish sessions with other clients.

Perform the following configuration in tunnel interface view.

Table 4-17 Configure the registration type of a client

Operation	Command
Configure the registration type	**dvpn register-type** { **forward** | **undistributed** }*
Restore the default registration type	**undo dvpn register-type** { **forward** | **undistributed** }*

A DVPN server forwards redirect packets by default.

4.2.4 Configuring a DVPN Class

In DVPN class view, you can configure the parameters related to the specified DVPN server, such as the private IP address, public IP address, and user name. A client needs these parameters for registering with the DVPN server. Note that the parameters must be consistent with those configured on the server.

Note:

To have the DVPN class configuration modified after a map has been created take effect, you must re-create the map by performing the **shutdown tunnel** and **undo shutdown tunnel** commands or by performing the **reset dvpn map** command.

I. Creating a DVPN class and entering its view

Use these commands to create a DVPN class and enter its view, or remove an existing DVPN class. Note that a DVPN class in use cannot be removed.

Perform the following configuration in system view.

Table 4-18 Create a DVPN class

Operation	Command
Create a DVPN class and enter its view	**dvpn class** *dvpn-class-name*
Remove a DVPN class	**undo dvpn class**

No DVPN class is configured by default.

II. Configuring the public IP address of the DVPN server

The public IP address here refers to the fixed public IP address assigned to the DVPN server.

Perform the following configuration in DVPN class view.

Table 4-19 Configure the public IP address of the DVPN server

Operation	Command
Configure the public IP address of the DVPN server	**public-ip** *ip-address*
Remove the public IP address of the DVPN server	**undo public-ip** *ip-address*

No public IP address of the DVPN server is configured by default.

III. Configuring the private IP address of the DVPN server

The private IP address here refers to the IP address of the tunnel interface through which the DVPN server accesses a DVPN domain. This configuration is optional. During registration, when a client configured with the private IP address of the DVPN server receives a registration response message from the server, it compares the private IP address of the server contained in the response message with that configured on it. If the two private IP addresses are not the same, the client tears down the connection.

Perform the following configuration in DVPN class view.

Table 4-20 Configure the private IP address of the DVPN server

Operation	Command
Configure the private IP address of the DVPN server	**private-ip** *ip-address*

Operation	Command
Remove the private IP address of the DVPN server	**undo private-ip**

No private IP address of the DVPN server is configured by default.

IV. Configuring the algorithm suite used during registration

DVPN registration control packets must be encrypted for security. The encryption algorithm, authentication algorithm, and key negotiation algorithm used during registration are called as a whole the algorithm suite.

Perform the following configuration in DVPN class view.

Table 4-21 Configure the algorithm suite used during registration

Operation	Command
Configure the algorithm suite used during registration	**algorithm-suite** *suite-number*
Restore the default algorithm suite	**undo algorithm-suite**

The algorithm suite 1, DES-MD5-GROUP1, is used by default. Refer to the related contents in *V 2.41 3.4 Command Manual* for the information about other algorithm suites.

V. Specifying how the client authenticates the DVPN server

A client can authenticate the DVPN server that it wants to access by using a pre-shared key. Use this command to configure the pre-shared key. Note that the pre-shared key specified here must be identical to the one that the DVPN server holds for the client to successfully register with the DVPN server.

Perform the following configuration in DVPN class view.

Table 4-22 Specify how the client authenticates the DVPN server

Operation	Command
Specify to authenticate the DVPN server using the pre-shared key	**authentication-server method pre-share**
Specify not to authenticate the DVPN server	**authentication-server method none**

A client does not authenticate the DVPN server by default.

Table 4-23 Configure the pre-shared key of the DVPN server

Operation	Command
Configure the pre-shared key of the DVPN server	**pre-shared-key** *key*
Remove the configured pre-shared key	**undo pre-shared-key**

No pre-shared key of the DVPN server is configured by default.

VI. Configuring the user name and password of the client

When registering with a DVPN server that authenticates clients, a client must provide its user name and password. Use this command to configure the user name and password of the client.

Perform the following configuration in DVPN class view.

Table 4-24 Configure the user name and password of the client

Operation	Command
Configure the user name and password of the client	**local-user** *username* **password** { **simple** | **cipher** } *password*
Remove the user name and password of the client	**undo local-user** *username*

A client is not configured with a user name and password by default.

4.2.5 Configuring a DVPN Policy

In DVPN policy view, you can configure the DVPN policy information, such as session algorithm, IPSec algorithm for data, and time parameters. A DVPN server issues the DVPN policy used in the DVPN domain to the registered clients.

⚠ **Caution:**

To modify or apply a configured policy, you must reboot the router or configure the **shutdown/undo shutdown** command on the tunnel interface. Otherwise, the new policy will not take effect.

I. Creating a DVPN policy and entering its view

Use these commands to create a DVPN policy and enter its view, enter an existing DVPN policy view, or remove an existing DVPN policy. To remove a DVPN policy that is in use, you must disable the policy first.

Perform the following configuration in system view.

Table 4-25 Create a DVPN policy and enter its view

Operation	Command
Create a DVPN policy and enter its view	**dvpn policy** *dvpn-policy-name*
Remove a DVPN policy	**undo dvpn policy** *dvpn-policy-name*

No DVPN policy is configured by default.

II. Configuring how the DVPN server authenticates the clients

A DVPN server can authenticate the clients that want to access the DVPN domain. At present, the supported authentication methods are PAP authentication and CHAP authentication.

Perform the following configuration in DVPN policy view.

Table 4-26 Configure how the DVPN server authenticates the clients

Operation	Command
Configure how the DVPN server authenticates the clients	**authentication-client method** { **none** | **chap** | **pap** }

A DVPN server does not authenticate the clients by default.

III. Configuring an encryption algorithm suite for sessions

DVPN supports the following algorithms for control packets in session negotiation: DES, 3DES, and AES encryption algorithms, MD5 and SHA1 authentication algorithms, and DH-GROUP1 and DH-GROUP2 key negotiation algorithms. Use these commands to specify the algorithm suite for the sessions between the server and the clients.

Perform the following configuration in DVPN policy view.

Table 4-27 Configure an encryption algorithm suite for the sessions

Operation	Command
Configure the encryption algorithm suite for sessions between the server and the clients	**session algorithm-suite** *suite-number*

Operation	Command
Restore the default encryption algorithm suite for sessions between the server and the clients	**undo session algorithm-suite**

By default, the algorithm suite 1 for session control packets is used, which comprises encryption algorithm DES, authentication algorithm MD5, and key negotiation algorithm DH-GROUP1.

IV. Configuring the idle timeout period for the sessions

A session is torn down if no packet passes through it during a specified interval known as the idle timeout period.

Perform the following configuration in a DVPN policy view.

Table 4-28 Configure the idle timeout period for the sessions

Operation	Command
Configure the idle timeout period for the sessions	**session idle-timeout** *time-interval*
Restore the default idle timeout period for the sessions	**undo session idle-timeout**

The default idle timeout period for the sessions is 300 seconds.

V. Configuring the interval for sending keepalive packets

After a session is established, the active side sends keepalive packets regularly to check the connection status of the session if no data passes through the session. If the active side receives no keepaliveack packet after sending three successive keepalive packets, it assumes that the session is disconnected.

Perform the following configuration in DVPN policy view.

Table 4-29 Configure the interval for sending keepalive packets

Operation	Command
Configure the interval for sending keepalive packets	**session keepalive-interval** *time-interval*
Restore the default interval for sending keepalive packets	**undo session keepalive-interval**

The default interval for sending keepalive packets is 10 seconds.

VI. Configuring the session request interval

If a session is not successfully established, the initiator sends a request again to try to establish the session after a specified interval. If three successive session establishment attempts end up with failure, the initiator concludes that the session cannot be established.

Perform the following configuration in a DVPN policy view.

Table 4-30 Configure the session request interval

Operation	Command
Configure the session request interval	**session setup-interval** *time-interval*
Restore the default session request interval	**undo session setup-interval**

The default session request interval is 10 seconds.

VII. Configuring the IPSec algorithm suite

Data packets transmitted in a DVPN domain are IPSec-encrypted for security. At present, the supported encryption algorithms include DES, 3DES, and AES, and the supported authentication algorithms are MD5 and SHA1. Use the following commands to specify the algorithm suite for the IPSec SA to use for forwarding packets.

Perform the following configuration in DVPN policy view.

Table 4-31 Configure the IPSec algorithm suite

Operation	Command
Configure the IPSec algorithm suite	**data algorithm-suite** *suite-number*
Restore the default IPSec algorithm suite	**undo data algorithm-suite**

The algorithm suite 1 for data packets are used by default, which comprises encryption algorithm DES and authentication algorithm MD5.

VIII. Configuring the lifetime of the IPSec SA

The lifetime of the IPSec SA used to encrypt data packets is part of the DVPN policy. Perform the following configuration in DVPN policy view.

Table 4-32 Configure the lifetime of the IPSec SA

Operation	Command
Configure the lifetime of the IPSec SA	**data ipsec-sa duration time-base** *time-interval*

Operation	Command
Restore the default lifetime	**undo data ipsec-sa duration time-base**

The default lifetime of the IPSec SA is 3,600 seconds.

4.2.6 Displaying and Debugging DVPN

Execute the **display** commands in any view to display how DVPN operates.

Execute the **reset** commands in user view to clear sessions, maps, statistics, or initialize a DVPN domain.

Execute the **debugging** command in user view to debug DVPN.

Table 4-33 Display and debug DVPN

Operation	Command
Enable/disable debugging for DVPN	[**undo**] **debugging dvpn** { **all** | **error** | **event** { **all | register | session | misc** } | **hexadecimal** | **packet** { **all | control | data | ipsec** } }
Display statistics about all DVPN domains or information about a specified DVPN domain	**display dvpn info** { **dvpn-id** d*vpn-id* | **global** }
Display information about maps in a DVPN domain	**display dvpn map** { **all** | **dvpn-id** d*vpn-id* | **public-ip** *public-ip* }
Display information about sessions in a DVPN domain	**display dvpn session** { **all** | **dvpn-id** d*vpn-id* [**private-ip** *private-ip*] }
Display information about one or all IPSec SAs in a DVPN domain	**display dvpn ipsec-sa** { **all** | **dvpn-id** d*vpn-id* }
Display information about online DVPN users	**display dvpn online-user**
Initialize a DVPN domain	**reset dvpn all** *dvpn-id*
Clear a specified map	**reset dvpn map** *ip-address port* [*control-id*]
Clear a specified session	**reset dvpn session** *dvpn-id private-ip*
Clear DVPN statistics	**reset dvpn statistics**

4.3 Configuration Example

4.3.1 Configuration Example for DVPN with NAT Traversal

I. Network requirements

As Figure 4-3 shows, Branch A and Branch B establish DVPN connections with the headquarters respectively. Since the private network of Branch A is connected to the private network of the headquarters through NAT, DVPN NAT traversal is required. Detailed configuration requirements are as follows:

- Specify to use the default algorithm suite (algorithm suite 1) during registration and sessions, that is, use DES for encryption, MD5 for authentication, and DH-GROUP1 for key negotiation.
- Specify to perform IPSec encryption on data using algorithm suite 6, that is, use 3DES for encryption, MD5 for authentication, and DH-GROUP2 for key negotiation.

Note:

Data transmitted over DVPN sessions is IPSec-encrypted by default using algorithm suite 1. That is, by default, the system uses DES for encryption, MD5 for authentication, and DH-GROUP1 for key negotiation.

II. Network diagram

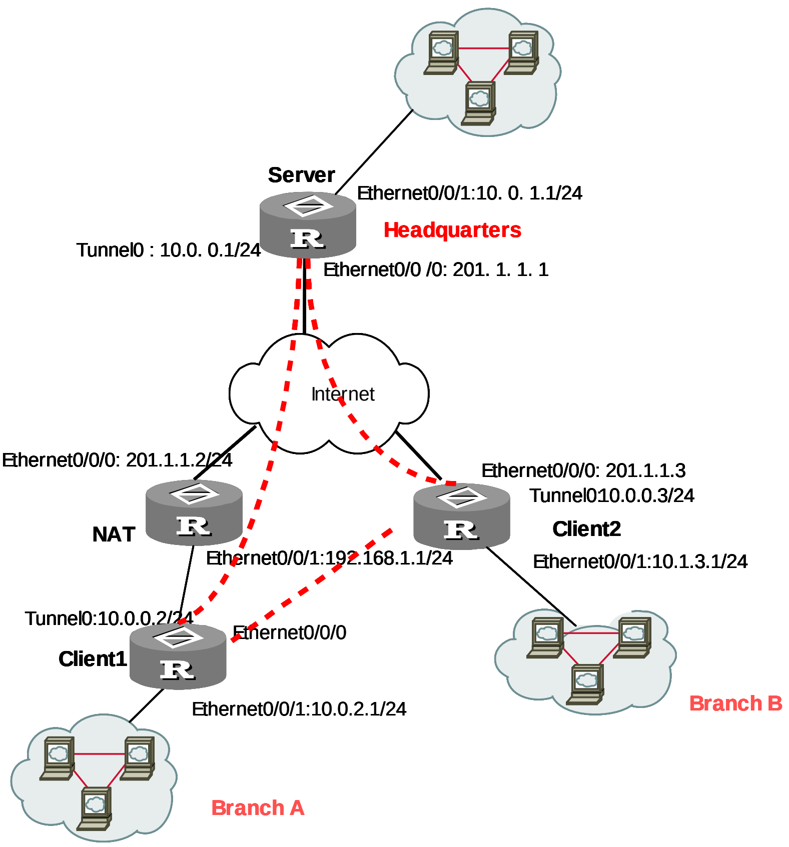

Server
Ethernet0/0/1:10. 0. 1.1/24
Headquarters
Tunnel0 : 10.0. 0.1/24
Ethernet0/0 /0: 201. 1. 1. 1
Internet
Ethernet0/0/0: 201.1.1.2/24
Ethernet0/0/0: 201.1.1.3
Tunnel010.0.0.3/24
NAT
Client2
Ethernet0/0/1:192.168.1.1/24
Ethernet0/0/1:10.1.3.1/24
Tunnel0:10.0.0.2/24
Ethernet0/0/0
Client1
Ethernet0/0/1:10.0.2.1/24
Branch B
Branch A

Figure 4-3 Network diagram for DVPN with NAT traversal

III. Configuration procedure

1) Configure Server

# Enable DVPN.

```
<Server> system-view
[Server] dvpn service  enable
```

# Configure interface Ethernet0/0/0.

```
[Server] interface Ethernet0/0/0
[Server-Ethernet0/0/0] ip address 201.1.1.1 255.255.255.0
[Server-Ethernet0/0/0] quit
```

# Create a DVPN policy and specify to use IPSec algorithm suite 5.

```
[Server] dvpn policy 1
[Server-dvpn-policy-1] data algorithm-suite 5
```

# Configure interface Ethernet0/0/1.

```
[Server] interface Ethernet0/0/1
[Server-Ethernet0/0/1] ip address 10.0.1.1 255.255.255.0
```

```
[Server-Ethernet0/0/1] quit
```

# Configure interface Tunnel0.

```
[Server] interface tunnel 0
[Server-Tunnel0] tunnel-protocol udp dvpn
[Server-Tunnel0] dvpn interface-type server
[Server-Tunnel0] ip address 10.0.0.1 255.255.255.0
[Server-Tunnel0] source Ethernet0/0/0
[Server-Tunnel0] dvpn dvpn-id 1
[Server-Tunnel0] dvpn policy 1
[Server-Tunnel0] quit
```

# Configure static routes.

```
[Server] ip route-static 10.0.2.0  255.255.255.0  10.0.0.2
[Server] ip route-static 10.1.3.0  255.255.255.0  10.0.0.3
```

2) Configure the NAT device

# Configure interface Ethernet0/0/0.

```
[Nat] interface Ethernet0/0/0
[Nat-Ethernet0/0/0] ip address 201.1.1.2 255.255.255.0
[Nat-Ethernet0/0/0] nat outbound 3000
[Nat-Ethernet0/0/0] quit
```

# Configure interface Ethernet0/0/1.

```
[Nat] interface Ethernet0/0/1
[Nat-Ethernet0/0/1] ip address 192.168.1.1 255.255.255.0
[Nat-Ethernet0/0/1] dhcp select interface
[Nat-Ethernet0/0/1] quit
```

# Configure an ACL.

```
[Nat] acl number 3000
[Nat-Acl-Adv-3000] rule permit ip
```

3) Configure Client1

# Enable DVPN.

```
<Client1> system-view
[Client1] dvpn service enable
```

# Configure interface Ethernet0/0/0 to obtain an IP address through DHCP.

```
[Client1] interface Ethernet0/0/0
[Client1-Ethernet0/0/0] ip address dhcp-alloc
[Client1-Ethernet0/0/0] quit
```

# Configure interface Ethernet0/0/1.

```
[Client1] interface Ethernet0/0/1
[Client1-Ethernet0/0/1] ip address 10.0.2.1 255.255.255.0
```

```
[Client1-Ethernet0/0/1] quit
```

# Configure the DVPN class.

```
[Client1] dvpn class testserver
[Client1-dvpn-class-testserver] public-ip 201.1.1.1
[Client1-dvpn-class-testserver] quit
```

# Configure interface Tunnel0.

```
[Client1] interface tunnel 0
[Client1-Tunnel0] ip address 10.0.0.2 255.255.255.0
[Client1-Tunnel0] tunnel-protocol udp dvpn
[Client1-Tunnel0] source Ethernet0/0/0
[Client1-Tunnel0] dvpn interface-type client
[Client1-Tunnel0] dvpn server testserver
[Client1-Tunnel0] dvpn vpn-id 1
[Client1-Tunnel0] quit
```

# Configure static routes.

```
[Client1] ip route-static 10.0.1.0  255.255.255.0  10.0.0.1
[Client1] ip route-static 10.1.3.0  255.255.255.0  10.0.0.3
```

4) Configure Client2

# Enable DVPN.

```
<Client2> system-view
[Client2] dvpn service  enable
```

# Configure interface Ethernet0/0/0.

```
[Client2] interface Ethernet0/0/0
[Client2-Ethernet0/0/0] ip address 201.1.1.3 255.255.255.0
[Client2-Ethernet0/0/0] quit
```

# Configure interface Ethernet0/0/1.

```
[Client2] interface Ethernet0/0/1
[Client2-Ethernet0/0/1] ip address 10.1.3.1 255.255.255.0
[Client2-Ethernet0/0/1] quit
```

# Configure the DVPN class.

```
[Client2] dvpn class testserver
[Client2-dvpn-class-testserver] public-ip 201.1.1.1
[Client2-dvpn-class-testserver] quit
```

# Configure interface Tunnel0.

```
[Client2] interface tunnel 0
[Client2-Tunnel0] ip address 10.0.0.3 255.255.255.0
[Client2-Tunnel0] tunnel-protocol udp dvpn
[Client2-Tunnel0] source Ethernet0/0/0
```

```
[Client2-Tunnel0] dvpn interface-type client
[Client2-Tunnel0] dvpn server testserver
[Client2-Tunnel0] dvpn vpn-id 1
[Client2-Tunnel0] quit
```

# Configure static routes.

```
[Client2] ip route-static 10.0.1.0  255.255.255.0  10.0.0.1
[Client2] ip route-static 10.0.2.0  255.255.255.0  10.0.0.2
```

4.3.2 Configuration Example for DVPN in Combination with GRE

I. Network requirements

As Figure 4-4 shows, the headquarters, Branch A and Branch B form a VPN, which comprises a DVPN established between the headquarters and Branch A and a VPN established between the headquarters and Branch B using GRE. Detailed requirements are as follows:

- Server can communicate with Client 1 and Client 2.
- Authentication is performed between Server and Client1 by using a pre-shared key.
- Client 1 and Client 2 communicate with each other through Server.

II. Network diagram

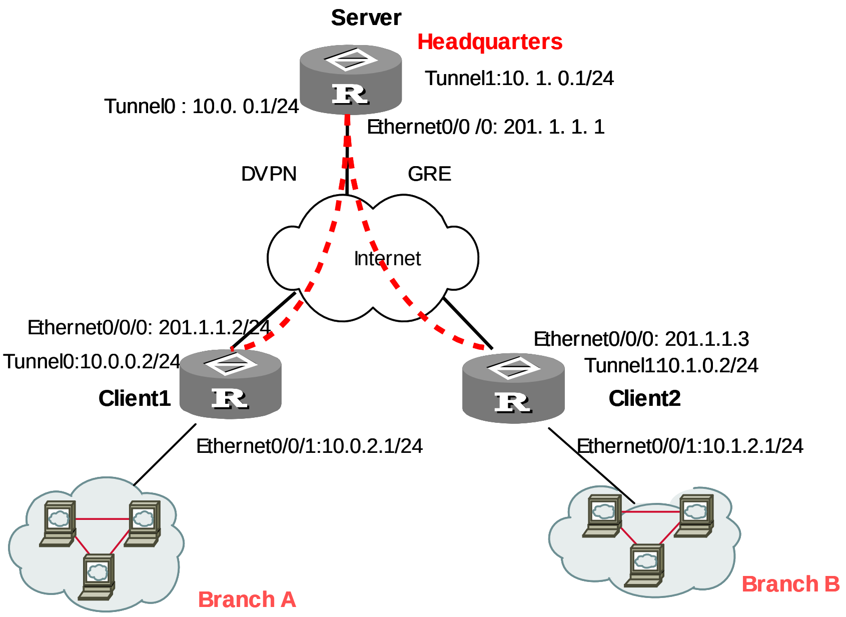


Figure 4-4 Network diagram for DVPN in combination with GRE

III. Configuration procedure

1) Configure Server

# Enable DVPN.

```
<Server> system-view
[Server] dvpn service  enable
```

# Configure interface Ethernet0/0/0.

```
[Server] interface Ethernet0/0/0
[Server-Ethernet0/0/0] ip address 201.1.1.1 255.255.255.0
[Server-Ethernet0/0/0] quit
```

# Configure interface Ethernet0/0/1.

```
[Server] interface Ethernet0/0/1
[Server-Ethernet0/0/1] ip address 10.0.1.1 255.255.255.0
[Server-Ethernet0/0/1] quit
```

# Configure the pre-shared key of the server.

```
[Server] dvpn server pre-shared-key 123456
```

# Configure the DVPN policy.

```
[Server] dvpn policy testpolicy
[Server-dvpn-Policy-testpolicy]  authentication-client  method  chap  domain
dvpn
[Server-dvpn-Policy-testpolicy] data algorithm-suite 7
[Server-dvpn-Policy-testpolicy] session algorithm-suite 12
[Server-dvpn-Policy-testpolicy] quit
```

# Configure the DVPN authentication domain and specify to authenticate locally.

```
[Server] domain dvpn
[Server-isp-domain] scheme local
[Server-isp-domain] state active
[Server-isp-domain] quit
```

# Configure a local DVPN user.

```
[Server] local-user dvpnuser
[Server-luser-dvpnuser] password simple dvpnuser
[Server-luser-dvpnuser] service-type dvpn
[Server-luser-dvpnuser] quit
```

# Configure the Tunnel0 interface used by DVPN.

```
[Server] interface tunnel 0
[Server-Tunnel0] tunnel-protocol udp dvpn
[Server-Tunnel0] dvpn interface-type server
[Server-Tunnel0] ip address 10.1.0.2 255.255.255.0
[Server-Tunnel0] source Ethernet0/0/0
[Server-Tunnel0] dvpn dvpn-id 1
[Server-Tunnel0] dvpn policy testpolicy
[Server-Tunnel0] quit
```

# Configure the Tunnel1 interface used by GRE.

```
[Server] interface tunnel 1
[Server-Tunnel1] ip address 10.1.0.1 255.255.255.0
[Server-Tunnel1] destination 211.1.1.3
[Server-Tunnel1] source Ethernet0/0/0
[Server-Tunnel1] quit
```

# Configure static routes.

```
[Server] ip route-static 10.1.2.0  255.255.255.0  10.1.0.2
[Server] ip route-static 10.0.2.0  255.255.255.0  10.0.0.2
```

2) Configure Client1

# Enable DVPN.

```
<Client1> system-view
[Client1] dvpn service  enable
```

# Configure interface Ethernet0/0/0 to obtain an IP address through DHCP.

```
[Client1] interface Ethernet0/0/0
[Client1-Ethernet0/0/0] ip address dhcp-alloc
[Client1-Ethernet0/0/0] quit
```

# Configure interface Ethernet 0/0/1.

```
[Client1] interface Ethernet0/0/1
[Client1-Ethernet0/0/1] ip address 10.0.2.1 255.255.255.0
[Client1-Ethernet0/0/1] quit
```

# Configure the DVPN class.

```
[Client2] dvpn class testserver
[Client1-dvpn-class-testserver] public-ip 201.1.1.1
[Client1-dvpn-class-testserver] authentication-server method pre-share
[Client1-dvpn-class-testserver] pre-shared-key 123456
[Client1-dvpn-class-testserver] local-user dvpnuser password simple dvpnuser
[Client1-dvpn-class-testserver] quit
```

# Configure interface Tunnel0.

```
[Client1] interface tunnel 0
[Client1-Tunnel0] ip address 10.0.0.2 255.255.255.0
[Client1-Tunnel0] tunnel-protocol udp dvpn
[Client1-Tunnel0] source Ethernet0/0/0
[Client1-Tunnel0] dvpn interface-type client
[Client1-Tunnel0] dvpn server testserver
[Client1-Tunnel0] dvpn vpn-id 1
[Client1-Tunnel0] quit
```

# Configure static routes.

```
[Client1] ip route-static 10.0.1.0  255.255.255.0  10.0.0.1
```

```
[Client1] ip route-static 10.1.2.0  255.255.255.0  10.0.0.1
```

3) Configure Client2

# Enable DVPN.

```
<Client2> system-view
[Client2] dvpn service  enable
```

# Configure interface Ethernet0/0/0.

```
[Client2] interface Ethernet0/0/0
[Client2-Ethernet0/0/0] ip address 201.1.1.3 255.255.255.0
[Client2-Ethernet0/0/0] quit
```

# Configure interface Ethernet0/0/1.

```
[Client2] interface Ethernet0/0/1
[Client2-Ethernet0/0/1] ip address 10.1.2.1 255.255.255.0
[Client2-Ethernet0/0/1] quit
```

# Configure interface Tunnel0.

```
[Client2] interface tunnel 0
[Client2-Tunnel0] ip address 10.1.0.2 255.255.255.0
[Client2-Tunnel0] tunnel-protocol gre
[Client2-Tunnel0] source Ethernet0/0/0
[Client2-Tunnel0] quit
```

# Configure static routes.

```
[Client2] ip route-static 10.0.1.0  255.255.255.0  10.1.0.1
[Client2] ip route-static 10.0.2.0  255.255.255.0  10.1.0.1
```

📖 **Note:**

In this example, as Client 1 is connected to Server using DVPN and Client 2 is connected to Server using GRE, they cannot establish a session between them. Communications between the two are forwarded by Server. Therefore, the next hops of the routes configured on Client 1 and Client 2 are the corresponding tunnel interfaces of Server, that is, the Tunnel0 interface and Tunnel1 interface.

Quality of Service

Table of Contents

Chapter 1 QoS Overview

1.1 Introduction

Quality of Service (QoS) measures the service performance of service providers in terms of client satisfaction. Instead of giving accurate marks, QoS emphasizes analyzing what good or imperfect services are, and they come in what kind of circumstances, so as to provide a cutting edge improvement.

In the Internet, QoS evaluates service performance for network packet transmission. Due to various services offered by the network, the evaluation for QoS will be based on different aspects accordingly. Generally QoS evaluates the service performance for those network core requirements during packet transmission process, such as: delay, jitter and packet loss ratio.

1.2 Traditional Packets Transmission Application

On traditional IP networks, the routers treat all packets identically and handle them with the first in, first out (FIFO) policy, assigning forwarding resources by arrival sequence of packets.

All the packets share the resources of the network. How many resources the packets can obtain will completely depend on the time they arrive. This service policy is called Best-effort, which delivers the packets to their destination as it can, without any assurance and guarantee for delivery delay, jitter, packet loss ratio, reliability and so on.

The traditional Best-Effort service policy is only suitable for applications insensitive to bandwidth and delay, such as WWW, file transfer and e-mail.

1.3 New Requirements Caused by New Applications

With the fast development of the network, more and more networks access the Internet. The Internet has been expanded in terms of its scale, coverage and users quantities. More and more users use Internet as their data transmission platform to implement various applications. And service providers expect to increase their income with new applications.

Apart from traditional applications of WWW, e-mail and FTP, network users try to expand some new applications, such as tele-education, telemedicine, video telephone, videoconference and Video-on-Demand (VoD), on the Internet. And the enterprise users expect to connect their regional branches together to develop some operational applications through VPN technology, for instance, to access the database of the company or monitor their remote equipment via Telnet.

Those new applications have one thing in common, i.e. high requirements for bandwidth, delay, and jitter. For instance, videoconference and VOD need the assurance of wide bandwidth, low delay and jitter. As for mission-critical applications, such as transaction and Telnet, they may not require wide bandwidth but do require lower delay and be handled by priority during congestion.

The new emerging applications demand higher requirements for service performance of IP network. Better network services during packets transmission are required other than simply delivering the packets to their destination, such as providing user-specific bandwidth, reducing packet loss ratio, avoiding congestion, regulating network traffic, setting priority of the packets. To meet those requirements, the network should be provided with better service capability.

1.4 Congestion: Causes, Impact, and Countermeasures

Network congestion is a key factor to degrade the service quality of the traditional network. Congestion refers to such a fact that the service rates are decreased due to relative deficiency of the resources supply (leading to extra delay).

1.4.1 Causes

Congestion will easily occur in complex packet switching circumstances in the Internet, with two cases illustrated in the following Figure:

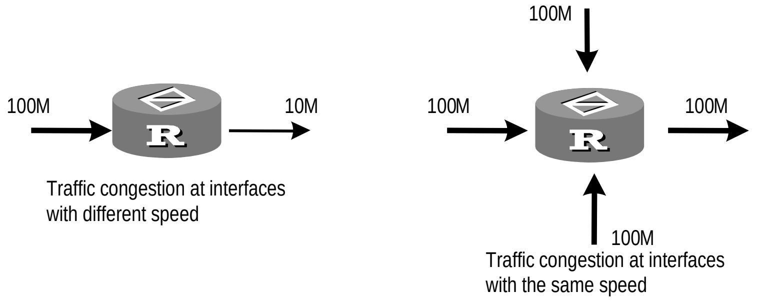

100M
10M
Traffic congestion at interfaces with different speed
100M
100M
100M
100M
Traffic congestion at interfaces with the same speed

Figure 1-1 Diagram for traffic congestion

1) The packet streams enter a router from a high speed link and are forwarded via a low speed link;
2) Packet streams enter to a router from several interfaces with a same speed and are forwarded through an interface with the same speed as well;

When traffic arrives at wire speed, congestion may occur for network resource bottleneck.

Besides the bottleneck of link bandwidth, congestion will also be caused by resources deficiency in normal packet forwarding, such as the deficiency of assignable processor time, buffer and memory. In addition, congestion may occur if the arrival traffic is not managed efficiently and the assignable network resources are inadequate.

Impact

Congestion may cause the following negative effects:

- Increase the delay and jitter of packet transmission
- Packet re-transmission caused by high delay
- Decrease the efficient throughput of network and waste the network resources
- Intensified congestion can occupy too many network resources (especially in memory), and the irrational assignment of resources even can lead to resource block and breakdown for the system.

It is obvious that congestion will make the traffics unable to obtain the resources in time and degrade the service performance accordingly. No one wants congestion, but it occurs frequently in complex environments where packet switching and multi-users applications coexist. So it needs to be treated cautiously.

1.4.2 Countermeasure

A direct way to solve resources deficient problem is to increase the bandwidth of network; however, it cannot resolve all the problems concerning congestion.

A more effective method to solve the problem of QoS is to enhance the functions of traffic control and resource allocation at network layer, and to provide differentiated services for applications with different service requirement in order to allocate and use resources rightly. During the process of resources allocation and traffic control, the direct or indirect factors that might cause network congestion should be controlled with best effort to reduce the probability of congestion. As congestion occurs, resource allocation should be balanced according to features and demands of applications, to minimize the effects on QoS by congestion.

1.5 Traffic Control Technologies

Traffic classification, traffic policing, traffic shaping, congestion management, congestion avoidance, and physical-interface LR are the foundations for a network to provide differentiated services. Mainly they implement the following functions:

- Traffic classification: It is a prerequisite for differentiated service, to identify the interested objects based on a certain matching rule.
- Traffic policing: polices the specification of particular traffics entering the router. When the traffics exceed the specification then some restriction or punishment measures can be taken to protect the commercial benefits of carriers and to prevent network resources from being damaged. Traffic policing is implemented at the IP layer.
- Congestion management: handles resource competition during network congestion. Generally, it stores the packets in the queue first, and then takes a dispatching algorithm to assign the forwarding sequence of packets.

- Congestion avoidance: Exceeding congestion consumes network resources. Congestion avoidance can monitor the usage status of network resources, and as congestion becomes worse actively take the policy of dropping packets through adjusting traffic, to resolve the overloading of the network.
- Traffic shaping: A traffic control measure of actively adjusting the output speed of traffics, generally it can enable the traffic to adapt to the network resources supplied by the downstream router, to prevent the unwanted packet dropping and congestion. Same as traffic policing, traffic shaping is implemented at the IP layer.
- Physical-interface LR: Unlike traffic policing, which can handle only packets that are processed at the IP layer, LR restricts all packets on physical interfaces and thus is well suited to the situation where rate limiting on all packets is desired.

Among those traffic management technologies, traffic classification is the basis. It is a prerequisite for differentiated service, which identifies the interested packet with certain matching rule. As for traffic policing, traffic shaping, congestion management and congestion avoidance, they implement management to network traffic and allocated resources from different aspects respectively to realize the differentiated service.

Normally, QoS provides the following functions:

- Traffic classification
- Traffic policing and shaping
- Congestion management
- Congestion avoidance

Chapter 2 Traffic Classification, Policing, and Shaping

2.1 Traffic Classification

Traffic classification is the prerequisite and foundation for differentiated service, which uses certain rules to identify the packets with certain features.

To discriminate flows, you can set traffic classification rules using the priority bits of ToS (type of service) field in the IP packet header, or using cell loss priority (CLP), the last bit in the fourth byte of the ATM cell header. Alternatively, the network administrator may define a traffic classification policy, for instance, integrating information such as source IP address, destination IP address, MAC address, IP, or port number of the applications to classify the traffic. In general, it can be a narrow range defined by a quintuple (source IP address, source port number, destination IP address, destination port number and the Transport Protocol), or can be all packets to a network segment.

In general, while packets being classified on the network border, the precedence bits in the ToS byte of IP header are set so that IP precedence can be used as a direct packet classification standard within the network. The queuing technologies, such as WFQ, can use IP precedence to handle the packets. Downstream network can receive the packets classification results from upstream network selectively, or re-classify the packets with its own standard.

Traffic classification is used to provide differentiated service, so it must be associated with certain kinds of traffic policing or resource-assignment mechanisms. To adopt what kind of traffic policing action will depend on the current stage and load status of the network. For example, to police the packets according to the committed rate when they enter the network, to make traffic shaping before they flow out the nodes, to do queuing in the event of congestion and to employ congestion avoidance when congestion becomes worse.

2.2 Traffic Policing and Traffic Shaping

If no restrictions are imposed on the traffics from the users, bursting data sent by mass users continuously will make the network become more congested. Thus for more efficient network function and better network service for more users, the traffics from the users must be restricted, for example, to restrict a traffic can only acquire the specific assigned resources in certain time interval so as to prevent the network congestion caused by excess burst.

Traffic policing and traffic shaping is a traffic monitoring policy to adjust the traffic and resources through comparing with the traffic specification. To know whether the traffic exceeds the specification or not is a prerequisite for traffic policing or shaping. Then based upon the evaluation result you can implement a regulation policy. Usually Token Bucket is used to value the traffic specification.

2.2.1 Traffic Evaluation and Token Bucket

I. Token bucket features

Token Bucket can be regarded as a container to reserve Token, which has certain capacity. The system will put Tokens into the Bucket at a defined rate. In case the Bucket is full, the extra Tokens will overflow and no more Tokens will be added.

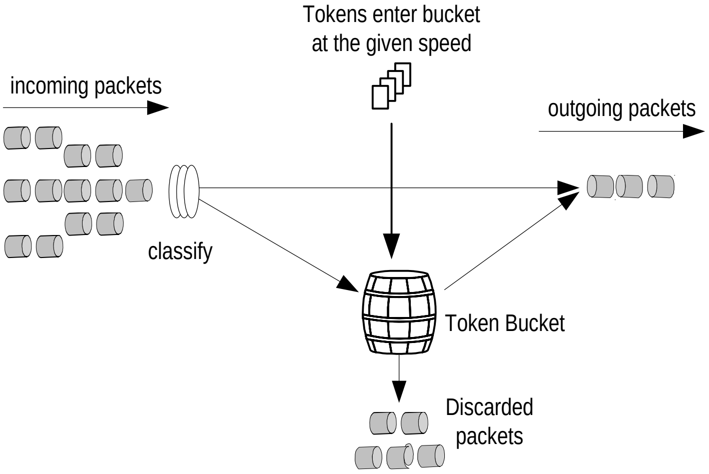


Figure 2-1 Measuring the traffic with Token Bucket

II. Measuring the traffic with Token Bucket

Whether or not the token quantity of the Token Bucket can satisfy the packets forwarding is the basis for Token Bucket to measure the traffic specification. If enough tokens are available for forwarding packets, traffic is regarded conforming the specification (Generally one token is associated to the forwarding ability of one bit) otherwise, non-conform or excess.

When measuring the traffic with Token Bucket, these parameters are included:

- Mean rate: The rate of putting Token into Bucket, i.e. average rate of the permitting traffic. Generally set as CIR (Committed Information Rate).
- Burst size: Token Bucket’s capability, i.e. the maximum traffic size of every burst. Generally, it is set as CBS (Committed Burst Size), and the bursting size must be greater than the maximum packets size.

A new evaluation will be made when a new packet arrives. If there are enough tokens in bucket for each evaluation, it shows that traffics are within the bound, and at this time the amount of tokens appropriate for the packets forwarding rights, need to be taken out. Otherwise, it shows that too much tokens have been used, and traffic specifications are exceeded.

III. Complicated evaluation

Two Token Buckets can be configured to evaluate conditions that are more complex and to implement more flexible regulation policy. For example, Traffic Policing (TP) has three parameters, as follows:

- CIR (Committed Information Rate)
- CBS (Committed Burst Size)
- EBS (Excess Burst Size)

It uses two Token Buckets with the token-putting rate of every bucket set as CIR equally, but with different capabilities: CBS and EBS (CBS < EBS, called C Bucket and E Bucket), which represents different bursting class permitted. In each evaluation, you may use different traffic control policies for different situations, such as "C bucket has enough tokens"; "Tokens of C bucket are deficient, but those of E bucket are enough"; "Tokens of C bucket and E bucket are all deficient".

2.2.2 Traffic Policing

Typically, traffic policing is used to monitor the specification of certain traffic entering the network and keep it within a reasonable bound, or it will make “penalty” on the exceeding traffic so as to protect network resources and profits of carriers. For example, it can restrict HTTP packets to occupy network bandwidth of no more than 50%. Once finding the traffic of a connection exceeds, it may drop the packets or reset the precedence of packets.

Traffic policing allows you to define match rules based on IP precedence or DiffServ code point (DSCP). It is widely used by ISP to police the network traffic. TP also includes the traffic classification service for the policed traffics, and depending upon the different evaluation results, it will implement the pre-configured policing actions, which are described as the following:

- Forward: For example, continue to forward the packets evaluated as “conform”.
- Drop: for example, dropping the packets evaluated as “not conform”.
- Reset precedence and forward: For example, for packets evaluated “partly conform”, to sign another priority then forward them.
- Enter the policing of the next level: Traffic policing can stack gradually with each class caring and policing objects that are more specific.

2.2.3 Traffic Shaping

Traffic shaping is an active way to adjust the traffic output rate. A typical application is to control the output traffic with TP index based upon downstream network nodes.

The main difference between traffic shaping and traffic policing is: The packets to be dropped in traffic policing will be stored during traffic shaping — generally they will be put into buffer or queues (Also called Traffic Shaping – TS; see Figure 2-2). Once there are enough tokens in Token Bucket, those stored packets will be evenly sent. The traffic size fluctuates around the CIR rate within a range specified by CBS. Another difference is that traffic shaping may intensify delay, yet traffic policing seldom does so.

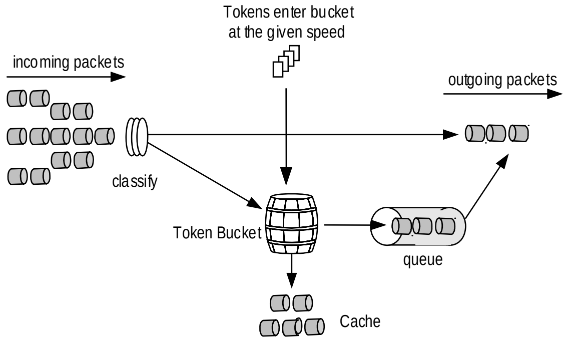


Figure 2-2 TS diagram

As shown in the figure below, Router A sends packets to Router B. And Router B implements TP on those packets, and directly drops exceeding traffic.

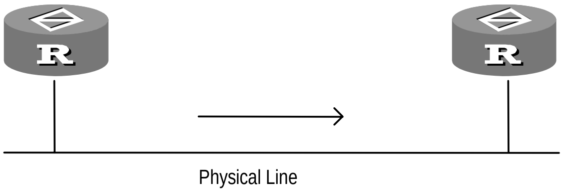


Figure 2-3 Traffic shaping application

To reduce packets dropping, GTS can be used for the packets on the egress interface of Router A. The packets beyond the traffic features of GTS will be stored in Router A. While sending the next set of packets, GTS will take out those packets from buffer or queues and send them. So that all the packets sent to Router B accord with the traffic regulation of Router B.

2.2.4 Line Rate on Physical Port

On a physical interface, you can enforce line rates below the physical line rate to limit the overall transmitting rate (including the rate sending critical packets).

LR also uses Token Bucket for traffic control. If LR is configured on an interface of a router, all packets to be sent via the interface will be firstly handled by Token Bucket of LR. If there are enough tokens in Token Bucket, then those packets can be forwarded; otherwise, those packets will be put into QoS queues for congestion management, so that the packet traffics through the physical port can be managed.

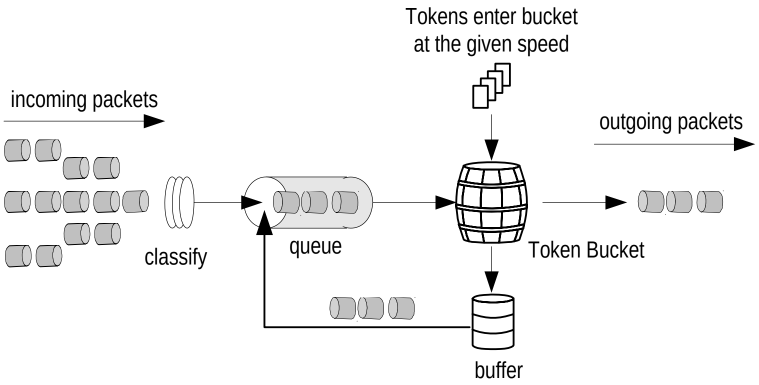


Figure 2-4 LR processing diagram

If Token Bucket is used to control the traffics, when there are tokens in Token Bucket, the packets can be sent in burst; if no tokens are available, packets will not be sent until new tokens generate in the Token Bucket. Thus, the traffic of packets is restricted under the generating rate of new token to achieve the goal of restricting the traffics while allowing bursting traffic overpass.

Compared with TP, LR can restrict all packets via physical port. TP is realized at IP layer implementing no function for packets not through IP layer. If users demand to limit the rate of all packets, LR is easier to be implemented.

2.3 Traffic Policing and Traffic Shaping Configuration

Traffic policing configuration includes:

- Configure CAR list
- Apply CAR policy

Traffic shaping configuration includes:

- Set shaping parameters for a certain kind of traffic
- Set shaping parameters for all traffics

LR on physical port configuration includes:

- Set LR on physical port

2.3.1 Configuring Traffic Policing

The traffic-policing configuration is divided into two tasks: one is to define the characters of the packets that need traffic policing; the other is to define the policing policy.

I. Configuring CAR list

CAR list can be regard as a particular class of access control list (ACL), which is to define the rules of matching packets. For different *carl-index*, the repeat execution of the command will create several CAR lists; for the same *carl-index*, the repeat execution of the command will modify the parameters of CAR list, i.e. the CAR list just configured will replace the one, which already exists using the same *carl-index*.

Perform the following configuration in system view.

Table 2-1 Configure CAR list

Operation	Command
Create/modify CAR List	**qos carl** *carl-index* { **precedence** *precedence-value* **|** **mac** *mac-address* **|** **dscp** *dscp-value* }
Delete CAR List	**undo qos carl** *carl-index*

You may specify up to eight IP precedence or DSCP values. In case the same value is specified multiple times, only one is regarded valid. If the IP precedence or DSCP value of a packet matches one of the specified values, the system regards that a match is found.

II. Applying CAR Policy

You may repeatedly perform this command to configure several CAR policies on the interface. Except IP packets, this command will not handle other data packets.

Please set the following configuration in interface view.

Table 2-2 Apply CAR policy

Operation	Command
Apply CAR policy	**qos car** { **inbound** **|** **outbound** } { **any** **|** **acl** *acl-number*| **carl** *carl-index* } **cir** *committed-information-rate* **cbs** *committed-burst-size* **ebs** *excess-burst-size* **green** *action* **red** *action*
Delete CAR policy	**undo qos car** { **inbound** **|** **outbound** } { **any** **|** **acl** *acl-number* **|** **carl** *carl-index* } **cir** *committed-information-rate* **cbs** *committed-burst-size* **ebs** *excess-burst-size*

The defined CIR value should not exceeds CBS x 20.

The action taken on a packet can be:

- **continue**: to have it dealt with by the next CAR strategy.
- **discard**: to dicard the data packet.
- **pass**: to send the data packet.

- **remark-prec-continue** *new-precedence*: to specify a new IP priority *new-precedence* and execute the next CAR strategy. The value range is 0~7.
- **remark-prec-pass** *new-precedence*: to specify a new IP priority *new-precedence* and send the packet. The value range is 0~7.

CAR policy can be used on an ingress or egress interface.

2.3.2 Configuring Traffic Shaping

The command in the following table is used to set the shaping parameters for a category of traffic or all the traffic and start the shaping as well.

You can configure the **qos gts acl** command to set the shaping parameters for the traffic matching some ACL and use different ACLs to set the shaping parameters for different categories of traffic.

You can use the **qos gts any** command to set the traffic parameters for all the traffic. If you use the command repeatedly, the latest configuration will replace the previous one.

The commands **qos gts acl** and **qos gts any** cannot be used together.

Please set the following configurations in interface view.

Table 2-3 Set shaping parameters for a certain kind of traffic

Operation	Command
Set shaping parameters for a certain kind of traffic	**qos gts** { **any** | **acl** *acl-number* } **cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size* [**queue-length** *queue-length*]]]
Remove shaping for a certain kind of traffic	**undo qos gts** { **any** | **acl** *acl-number* }

2.3.3 Configuring Interface LR

You can limit the rate at which a physical or tunnel interface sends out data.

You can use this command on a tunnel interface to limit its interface rate and implement congestion management along with other queue scheduling algorithms.

Before configuring queuing on the tunnel interface, you must configure the **qos lr** command. Before deleting the **qos lr** command on the interface, however, you must delete the queuing configuration.

Perform the following configuration in interface (including the MFR interface) view.

Table 2-4 Configure interface LR

Operation	Command
Configure interface LR	**qos lr cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]]
Disable interface LR	**undo qos lr**

2.4 Traffic Policing and Shaping Display and Debug

2.4.1 Displaying CAR Rule

After the above configuration, execute the **display** command in any view to display the running of a certain rule or all the access rules of TP configuration, and to verify the effect of the configuration.

Table 2-5 Display TP rule

Operation	Command
Display TP rule	**display qos carl** [*carl-index*]

2.4.2 Displaying CAR Information on Each Interface

After the above configuration, execute the **display** command in any view to display the running of the TP configuration information and running statistic information on each interface, and to verify the effect of the configuration.

Table 2-6 Display the TP information at each interface

Operation	Command
Display the TP information on each interface	**display qos car interface** [*interface-type interface-number*]

2.4.3 Displaying GTS Configuration and Statistics on Interface

After the above configuration, execute the **display** command in any view to display the running of GTS configuration and statistics in certain interface or all interfaces, and to verify the effect of the configuration.

Table 2-7 Display GTS configuration and statistics on the interface

Operation	Command
Display GTS configuration and statistics in the interface	**display qos gts interface** [*interface-type interface-number*]

2.4.4 Displaying LR Configuration and Statistics on Interface

After the above configuration, execute the **display** command in any view to display the running of LR configuration and statistics in certain interface or all interfaces, and to verify the effect of the configuration.

Table 2-8 Display LR configuration and statistics in the interface

Operation	Command
Display LR configuration and statistics in the interface	**display qos lr interface** [*interface-type interface-number*]

2.5 Traffic Policing and Shaping Configuration Example

I. Configuration requirement

As shown in Figure 2-5, the interface ethernet0/0/0 of the router 3Com1 is connected with the interface ethernet1/0/0 of the router 3Com2. Server, PC1 and PC2 can access the Internet via 3Com1 and 3Com2. Server, PC1 and the interface ethernet0/0/0 of the router 3Com1 are in the same network segment while PC2 and the interface ethernet2/0/0 of the router 3Com1 are in the same network segment. The traffics from Server and PC1 received by the interface ethernet1/0/0 require to be controlled on the router 3Com2.

The traffic restriction from Server is 54000bps. The traffic less than this restriction can be transmitted normally. When the traffic exceeds this restriction, the preference of the ultra-long packet will be set to 0 before transmission.

The limit on the traffic from PC1 is 80000 bps. Traffic within this limit is transmitted normally. When the traffic exceeds this limit, the packets are dropped.

In the meantime, there are the following requirements for the interfaces ethernet1/0/0 and ethernet0/0/0 on the router 3Com2:

- The restriction of the total traffic received by the interface ethernet1/0/0 on 3Com2 is 0.5Mbps and when the traffic exceeds this restriction, the ultra-long packet will be dropped.
- The restriction of the traffic entering the Internet via the interface ethernet0/0/0 on 3Com2 is 1Mbps and when the traffic exceeds this restriction, the ultra-long packet will be dropped.

II. Network diagram

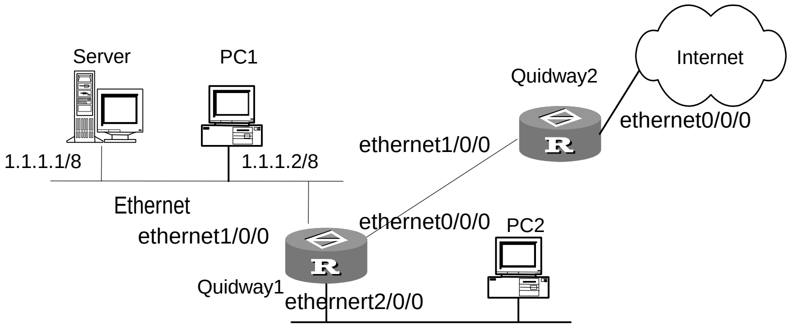


Figure 2-5 Network diagram of traffic policing and shaping

III. Configuration procedure

1) Configure the router 3Com1:

# Configure GTS on the interface ethernet0/0/0 of 3Com1 to shape the traffic transmitted from the interface (shaping the traffic exceeding 0.5Mbps) so as to reduce the packet drop rate of the interface ethernet1/0/0 of 3Com2.

```
[3Com1] interface ethernet0/0/0
[3Com1-Ethernet0/0/0] qos gts any cir 500000
```

2) Configure the router 3Com2:

# Configure the ACL to match the packets from Server and PC1.

```
[3Com2] acl number 2001
[3Com2-acl-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[3Com2-acl-basic-2001] quit
[3Com2] acl number 2002
[3Com2-acl-basic-2002] rule permit source 1.1.1.2 0.0.0.0
[3Com2-acl-basic-2002] quit
```

# Configure TP on the interface ethernet1/0/0 to perform the corresponding traffic control on the different traffics received by the interface ethernet1/0/0.

```
[3Com2] interface ethernet1/0/0
[3Com2-Ethernet1/0/0] qos car inbound acl 2001 cir 54000 cbs 54000 ebs 0 green
pass red remark-prec-pass 0
[3Com2-Ethernet1/0/0] qos car inbound acl 2002 cir 8000 cbs 8000 ebs 0 green
pass red discard
[3Com2-Ethernet1/0/0] qos car inbound acl 1 cir 500000 cbs 500000 ebs 0 green
pass red discard
```

# Configure TP on the interface ethernet0/0/0 to perform traffic control on the traffic transmitted on the interface ethernet0/0/0. The traffic should not exceed 1Mbps and the ultra-long packets will be dropped.

```
[3Com2] interface ethernet0/0/0
```

```
[3Com2-Ethernet0/0/0] qos car acl 2 outbound cir 1000000 cbs 1000000 ebs 0 green
pass red discard
```

2.6 MFR Interface LR Configuration Example

I. Network requirements

Router A and Router are connected through MFR interfaces formed by serial interfaces.

Configure LR on the MFR interface on Router A, setting CIR to 10000 bps, CBS to 15000 bit, and EBS to 0 bits.

II. Network diagram

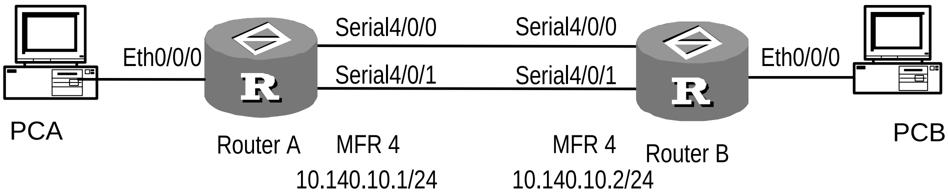


Figure 2-6 Network diagram for LR configuration on MFR interfaces

III. Configuration procedure

1) Configure Router A

# Create and configure interface MFR 4.

```
[3Com] interface mfr 4
[3Com-MFR4] ip address 10.140.10.1 255.255.255.0
[3Com-MFR4] fr interface-type dte
[3Com-MFR4] fr dlci 100
[3Com-fr-dlci-MFR4-100] quit
[3Com-MFR4] fr map ip 10.140.10.2 100
[3Com-MFR4] qos lr cir 10000 cbs 15000 ebs 0
[3Com-MFR4] quit
```

# Assign interfaces Serial 4/0/0 and Serial 4/0/1 to MFR 4.

```
[3Com] interface serial 4/0/0
[3Com-Serial4/0/0] link-protocol fr mfr 4
[3Com-Serial4/0/0] interface serial 4/0/1
[3Com-Serial4/0/1] link-protocol fr mfr 4
```

2) Configure Router B

# Create and configure interface MFR 4.

```
[3Com] interface mfr 4
[3Com-MFR4] ip address 10.140.10.2 255.255.255.0
```

```
[3Com-MFR4] fr interface-type dce
[3Com-MFR4] fr dlci 100
[3Com-fr-dlci-MFR4-100] quit
[3Com-MFR4] fr map ip 10.140.10.1 100
[3Com-MFR4] quit
```

# Assign interfaces Serial 4/0/0 and Serial 4/0/1 to MFR 4.

```
[3Com] interface serial 4/0/0
[3Com-Serial4/0/0] link-protocol fr mfr 4
[3Com-Serial4/0/0] interface serial 4/0/1
[3Com-Serial4/0/1] link-protocol fr mfr 4
```

When PCA transmits traffic to PCB, you can view traffic statistics with the **display qos lr interface** command on Router A.

```
<RouterA> display qos lr interface
Interface: MFR1
 CIR 10000 (Bps), CBS 15000 (bit), EBS 0 (bit)
 Passed : 1006/72112 (Packets/Bytes)
 Delayed: 933/70766 (Packets/Bytes)
 Active Shaping:  NO
```

Chapter 3 Congestion Management

3.1 Brief Introduction to Congestion Management

As to a network device, congestion will occur on the interface where the arrival rate of packets is faster than the sending rate. If there is no enough buffer capacity to store those packets and then a part of them will be lost, which may cause the packet retransmission from the hosts or Router because of timeout, and lead to a vicious circle.

The key to congestion management is how to define a dispatching policy for resources to decide the forwarding order of packets when congestion occurs.

3.1.1 Congestion Management Policies

In general, congestion management adopts queuing technology. The system classifies traffics using a kind of queuing algorithm, and then it will send out them with a certain preference algorithm. Each queuing algorithm is used to handle a particular network traffic problem and has great impacts on bandwidth resource assignment, delay, and jitter.

We will introduce several common queue-scheduling mechanisms here.

I. FIFO (First In,First Out) queuing

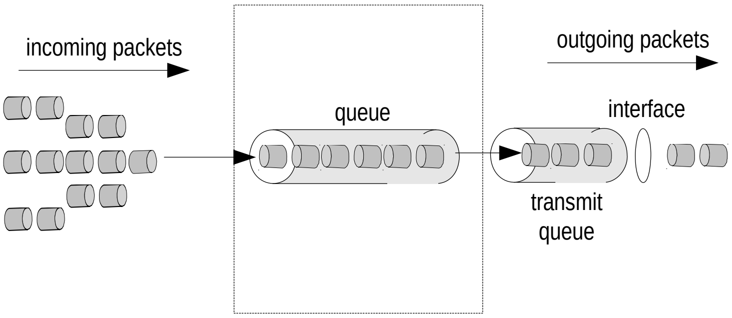


Figure 3-1 FIFO queuing

As shown in above figure, FIFO designs the forwarding order of packets depending upon their arrival time. On a router, the resources assigned for data traffic of users are based on the arrival time of packets and the current load status of the network. Best-Effort services use FIFO queuing policy.

If there is only one FIFO-based output/input queue on router’s interface, malicious applications may occupy all network resources and seriously affect mission-critical data.

Within each queue, the sending (sequence) of packets is defaulted as FIFO.

II. PQ (Priority Queuing)

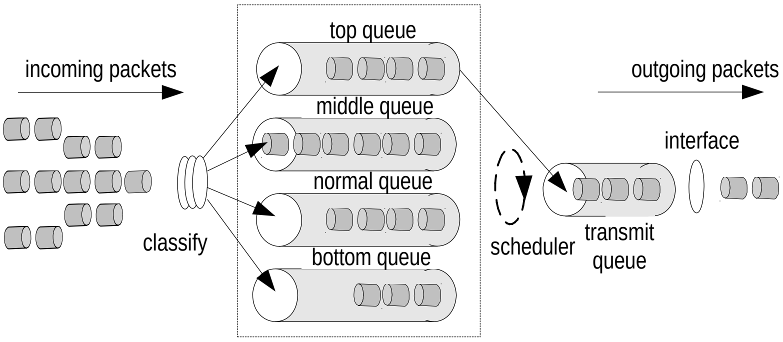


Figure 3-2 Priority queuing

Priority queuing is designed for mission-critical applications. Those applications have an important feature, i.e. when congestion occurs they require preferential service to reduce the response delay. PQ can flexibly design priority sequence according to different network protocols (e.g. IP and IPX), interface receiving packets, packet length, source/destination IP address etc. Priority queuing classifies the packets into four different types: top, middle, normal and bottom, in descending order. By default, the data flow enters the normal queue.

During queues dispatching, PQ strictly comply with the priority sequence from high to low, and it will send packets in the high-priority queue first. When that queue is empty, PQ will begin to send packets in lower priority queue. The system then put packets of mission-critical application in higher priority queue, and packets of normal application in lower priority queue. It guarantees that the packets of mission-critical application are sent with priority, and the packets of normal application are sent at the free interval of operating mission-critical application.

The disadvantage of PQ is that packets in the lower queues will be neglected if there are packets in the higher queues for a long time.

III. CQ (Custom Queuing)

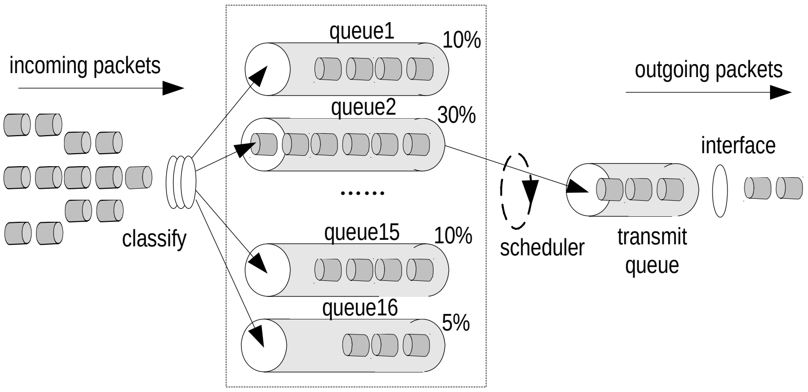


Figure 3-3 Custom queuing

CQ classifies packets into 17 classes in accordance with certain rules (corresponding to 17 queues). Based on their own classes, packets will enter the corresponding custom queues with FIFO policy.

Of these 17 queues, queue 0 is a system queue (not shown) which is not configurable and queues 1 through 16 are user queues, as shown in the above figure. User can set the rules of traffic classification and assign the proportions on occupying interface bandwidth for those 16 user queues. During dispatching, packets in system queue are sent preferentially till the queue is empty. Then with polling method a certain number of packets, taken from No.1-16 user queues under the bandwidth-occupying proportion set in advance, are sent out. In this way, packets of different application can be assigned with different bandwidth. Therefore, it will not only ensure mission-critical application to get more bandwidth but also prevent normal application from obtaining no bandwidth at all. By default, the data flow enters the No.1 queue.

Another advantage of custom queuing is that bandwidth can be assigned according to the busyness of applications, which is suitable for those applications having special requirement for bandwidth. Though the dispatching for 16 user queues is polling, the service time for each queue is not fixed. So when there are no packets of certain classes, the CQ dispatching mechanism can automatically increase bandwidth occupied by the packets of current existing class.

IV. WFQ (Weighted Fair Queuing)

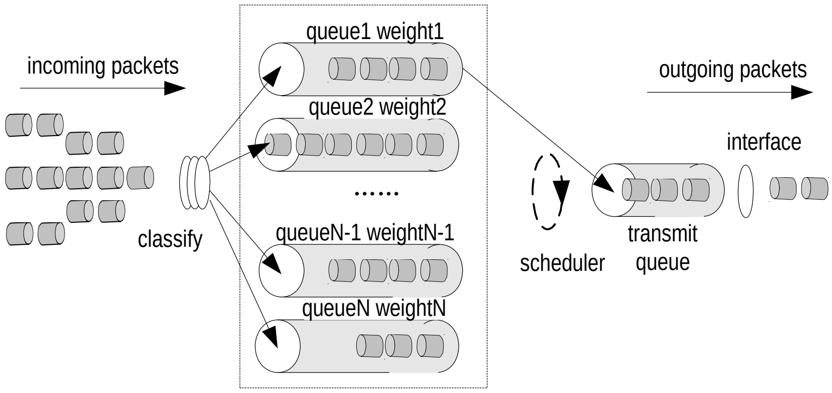


Figure 3-4 WFQ diagram

Before further to Weighted Fair Queuing, FQ (Fair Queue) is to be introduced first. FQ is designed for fairly sharing network resources, which will try to reduce the delay and jitter of all traffics to their optimum levels. It has taken all the aspects into consideration, which has the following features:

- Different queues have fair opportunity of dispatching to equilibrate the delay of each stream on the whole.
- Short packets and long packets are treated fairly while dequeuing: if there are long packets in a queue and short packets in another queue waiting simultaneously to be send out, the short packets should also be cared, and statistically the short packets should be treated preferentially, and the jitter between packets of every traffic will be reduced on the whole.

Compared with FQ, WFQ considers priority in addition when calculating the dispatching sequence of packets. Statistically, with WFQ, high priority traffic takes priority over low priority packets in dispatching. WFQ can automatically classify traffic according to the “session” information of traffic (protocol type, source/destination TCP or UDP port number, source/destination IP address, preference bits of ToS field, etc), and try to provide more queues so that each traffic will be equably put into different queues and equilibrate the delay of every traffic on a whole. While dequeuing, WFQ can assign the bandwidth of egress interfaces occupied by each flow according to IP precedence or DSCP. The bigger the numerical value of the precedence is, the more bandwidth can be obtained. At last, when sending packets, WFQ polls each queue and picks out packets based on bandwidth ratio.

For example: Now if there are five traffics on the interface, and their precedence levels are 0, 1, 2, 3, 4, respectively, then the total bandwidth quota will be: the sum of total (precedence of traffic +1), i.e.

1+2+3+4+5=15

The bandwidth-occupying proportion for each traffic is: (priority + 1)/total quota of bandwidth, i.e. Bandwidth available for each traffic: 1/15, 2/15, 3/15, 4/15, 5/15.

Because WFQ can balance the delay and jitter of every flow when congestion occurs, it is effectively applied in particular fields. For instance, in the assured services using the RSVP (resource reservation protocol), generally, WFQ will be used as the dispatching policy. And also in GTS, WFQ is used to dispatch buffered packets.

V. CBQ (Class-Based Queuing)

CBQ is the extension of WFQ, which supports user-defined classes. CBQ allocates an independent FIFO reserved queue for each user-defined class to buffer data of the same class. In case of network congestion, CBQ matches output packets according to user-defined class rules and enables them to enter corresponding queues. It is necessary to check the congestion avoidance mechanism (tail drop or WRED) and bandwidth restriction before the packets enter queues. WFQ is performed to the packets in the queue corresponding to each class when they go out of the queue.

If CBQ treats queues of all classes in weighted fair mode, delay sensitive data streams like voice packets may not be serviced timely. This is why the PQ feature is introduced. This feature provides an emergency queue, which adopts FIFO scheduling mode and bears no bandwidth restrict and therefore is capable of providing service of strict priority (SP) to sensitive packets such voice packets. CBQ providing an emergency queue is called low latency queuing (LLQ).

LLQ combines SP mechanism with CBQ. The user can set a class to use SP service when defining the class. Such a class is known as priority class. All packets of the priority class will enter the same priority queue. It is necessary to check bandwidth restriction of packets before they enter queues. When packets go out of queues, the packets in priority queue get transmitted first. Then packets in other queues are transmitted in weighted fair mode.

In order that packets in other queues will not be delayed too long, maximum available bandwidth can be specified to each priority class when using LLQ. The bandwidth value is used to monitor traffic in case of congestion. If no congestion happens, the priority class is allowed to use the bandwidth exceeding the allocated value. If congestion happens, the packets of the priority class exceeding the allocated bandwidth will be discarded. LLQ can also specify burst-size.

The system will always match the priority class first and then the other classes when matching rules for packets. Multiple priority classes are matched in the configuration sequence. It is the same with other classes. Multiple rules in a class are matched in the configuration sequence.

VI. RTP (Real-time Transport Protocol) priority queuing

RTP priority queuing technology is used to solve the QoS problems of real-time service (including audio and video services). Its principle is to put RTP packets carrying audio or video into high-priority queue and send it first, thus minimizing delay and jitter and ensuring the quality of audio or video service which is sensitive to delay.

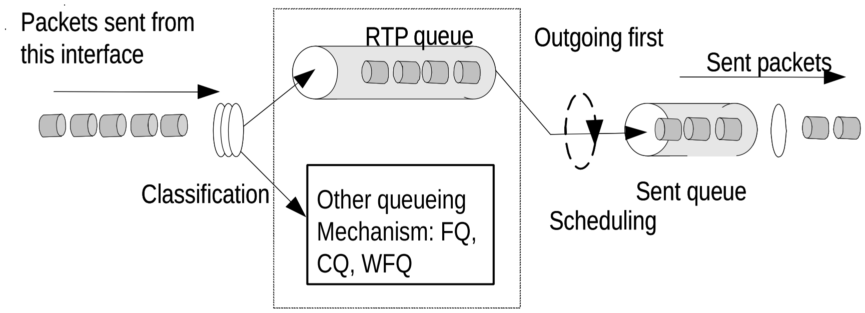

Packets sent from this interface
RTP queue
Outgoing first
Sent packets
Classification
Other queueing Mechanism: FQ, CQ, WFQ
Sent queue
Scheduling

Figure 3-5 RTP queuing diagram

As shown in the above figure, an RTP packet is sent into a high priority queue. RTP packet is the UDP packet whose port number is even. The range of the port number is custom. RTP priority queue can be used along with any queue (e.g., FIFO, PQ, CQ, WFQ and CBQ), while it has the highest priority. Since LLQ of CBQ can also be used to solve real-time service, it is recommended not to use RTP together with CBQ.

3.1.2 Comparisons among Congestion Management Technologies

3Com routers will provide several congestion management technologies. Breaking through the single congestion management policy of FIFO for traditional IP equipment, they provide strong QoS ability, which meets the demands of different service quality required by different applications. For efficient use of congestion management technologies, the following table compares the available queuing technologies.

Table 3-1 Congestion management technologies

Type	Queue No.	Advantages	Disadvantages
FIFO	1	• No need for configuration, easy to use • Easy operation, low delay	• All packets are treated equally. The available bandwidth, delay and drop probability are decided by the arrival order of the packets. • No restriction on the unmatched data sources (that is, flows without flow control mechanism, UDP for example), resulting bandwidth loss of matched data sources such as TCP. • No guarantee to the delay of time-sensitive real-time application, such as VoIP
PQ	4	• Provide service of absolute preference to data of different applications, and capable of ensuring the low delay for real-time applications (VoIP) • Provide absolute preference to the packets of preferential business on their bandwidth-occupying	• Need to be configured; generate great system overhead • If there are no restriction on bandwidth-occupying of packets with high preference, the packets with low preference won’t obtain the required bandwidth
CQ	17	• Capable of assigning the bandwidth-occupying proportion according to packets with different applications • If packets of certain classes do not exist, it can increase the bandwidth for existing packets	Need to be configured, generate great system overhead

Type	Queue No.	Advantages	Disadvantages
WFQ	Configurable	● Easily configured ● Capable of ensuring the bandwidth-occupying for data sources (e.g. TCP packets sending) used for interactive purpose ● Capable of reducing jitter ● Capable of reducing the delay for interactive application with small data ● Capable of assigning different bandwidth for traffics with different priorities ● When the amount of the traffics decreased, it can automatically increase the bandwidth for existing traffics.	The system overhead is greater than that of FIFO but smaller than that of PQ and CQ
CBQ	Configurable (0 to 64)	● Capable of classifying data according to flexible, various rules, providing different queue dispatching mechanism for the expedited forwarding (EF), assured forwarding (AF) and best-effort (BE) services. ● Capable of providing highly precise bandwidth assurance for the AF service and ensuring that the queue dispatching is performed according to a certain weight proportion among various AF services. ● Capable of providing absolutely preferential queue dispatching for the EF service so as to ensure the real-time data delay. In the mean time, it can overcome the disadvantage that the PQ of low preference will "extinct due to too little data flow" since it restricts the data flow of high preference. ● Capable of providing WFQ dispatching for the default data of best-effort forwarding.	The system overhead is large.

3.2 Configuring FIFO Queue

FIFO queue configuration includes:

- Configure the length of FIFO queue

3.2.1 Configuring FIFO Queue Length

FIFO is the queue scheduling mechanism for interface by default, and the length of the queue can be changed by configuration command.

Please set the following configuration in interface view.

Table 3-2 Configure FIFO queue length

Operation	Command
Configure the length of FIFO queue	**qos fifo queue-length** *queue-length*
Restore the default length of FIFO queue	**undo fifo queue-length**

The default length for FIFO queue is 75.

3.3 Priority Queuing Configuration

PQ configuration includes:

- Configure priority-list
- Apply priority-group on the interface

3.3.1 Configuring Priority-list

I. Configuring Priority-list under network layer protocol

The packets will be classified into different queues based on different protocol types. For a same *pql-index*, repeatedly using this command can set several rules for it.

The system will match the packets according to the sequence of configured rules. Once finding the packets match a certain rule, the system will stop searching.

Please set the following configurations in system view.

Table 3-3 Priority-list configuration based on network layer protocol

Operation	Command
Configure priority-list according to network layer protocol	**qos pql** *pql-index* **protocol** *protocol-name queue-key key-value* **queue** { **top** | **middle** | **normal** | **bottom** }
Delete the relative classifying rules in group-number	**undo qos pql** *pql-index* **protocol** *protocol-name* [*queue-key key-value*]

II. Configuring Priority-list based on interfaces on which packets are received

Classify the packets based on the ingress interfaces of Routers, and send them into different queues.

Perform the following configuration in system view.

Table 3-4 Configure Priority-list based on interfaces on which packets are received

Operation	Command
Configure Priority-list based on interfaces on which packets are received	**qos pql** *pql-index* **inbound-interface** *interface-type interface-number* **queue** { **top** | **middle** | **normal** | **bottom** }
Delete the relative classifying rules in group-number	**undo qos pql** *pql-index* **inbound-interface** *interface-type interface-number*

III. Configuring default queue

A default queue is designated for the packets that do not match any rules.

Perform the following configuration in system view.

Table 3-5 Configure default queue

Operation	Command
Configure default queue	**qos pql** *pql-index* **default-queue** { **top** | **middle** | **normal** | **bottom** }
Restore the default value of default queue	**undo qos pql** *pql-index* **default-queue**

You may define multiple rules for a priority-list group and apply these rules to an interface. When a packet that needs to be forwarded out the interface arrives at the interface, the system compares it against the rule chain. If a match is found, the packet is put into the corresponding queue and the match operation is complete; if no match is found, the packet is put into the default queue.

The default value for default queue is **normal**.

IV. Configuring the Length of Queue

Configure the length of each queue (i.e. the capability of queue).

Perform the following configuration in system view.

Table 3-6 Configure length of the queue

Operation	Command
Configure Length of the queue	**qos pql** *pql-index* **queue** { **top** | **middle** | **normal** | **bottom** } **queue-length** *queue-length*
Recover the default length value of each queue	**undo qos pql** *pql-index* **queue** { **top** | **middle** | **normal** | **bottom** } **queue-length**

The following table lists the default length of each queue.

Table 3-7 Default length of each queue

Queue	Length
top	20
middle	40
normal	60
bottom	80

3.3.2 Applying Priority-list Queue on the Interface

Apply a group of Priority-list on the interface; to use this command repeatedly will set a new priority-list for the same interface.

Perform the following configuration under interface view.

Table 3-8 Apply priority-list group on the interface

Operation	Command
Apply priority-list group on the interface	**qos pq pql** *pql-index*
Cancel using PQ on the interface	**undo qos pq**

Not PQ but FIFO is employed on the interface by default.

⚠ **Caution:**

Except for interfaces encapsulated with X.25 or LAPB, all physical interfaces can use PQ.

You can apply PQ to a dialer interface. Before that, make sure the queuing configuration on its physical interfaces is the default.
In addition, if these physical interfaces have had connections with their respective connected devices, the applied queuing configuration cannot update to them immediately. Instead, the configuration updates to the physical interfaces the next time they set up connections.

3.3.3 Displaying and Debugging Priority Queue

After the above configuration, execute **display** commands in any view to display the running of the priority queue configuration, and to verify the effect of the configuration.

Table 3-9 Display priority queue status and application on the interfaces

Operation	Command
Display the status of priority queue	**display qos pql** [*pql-index*]
Display priority queue configuration status on the interface	**display qos pq interface** [*interface-type interface-number*]

3.4 Custom Queuing Configuration

Customize queuing configuration includes:

- Configure custom queuing list (CQL)
- Apply custom-group on the interface

3.4.1 Configuring CQL

There are 16 groups (called custom-groups) of CQLs (1 through 16), each specifying packet queuing rule, length of each queue, and bytes to be sent continuously for each queue during a poll. You may apply only one custom-group on an interface.

I. Configuring custom-list under network layer protocol

Packets can be classified under different protocols, and enter different queues. But V 2.41 can only classify IP and MPLS packets by far.

Perform the following configuration in system view.

Table 3-10 Configure custom-list under network layer protocol

Operation	Command
Configure custom-list under network layer protocol	**qos cql** *cql-index* **protocol** *protocol-name queue-key key-value* **queue** *queue-number*
Delete the relative classifying rule of group-number	**undo qos cql** *cql-index* **protocol** *protocol-name* [*queue-key key-value*]

II. Configuring custom-list according to the ingress interfaces of packets

Set an interface-based classifying rule. Repeatedly using this command can add rules to a *cql-index*.

Perform the following configuration in system view.

Table 3-11 Configure custom-list based on interface

Operation	Command
Configure custom-list based on the incoming interface of packets	**qos cql** *cql-index* **inbound-interface** *interface-type interface-number* **queue** *queue-number*
Delete the relative classifying rule of group-number	**undo qos cql** *cql-index* **inbound-interface** *interface-type interface-number*

III. Configuring default queue

Designate a default queue for those packets matching no rules.

Perform the following configuration in system view.

Table 3-12 Configure default queue

Operation	Command
Configure default queue	**qos cql** *cql-index* **default-queue** *queue-number*
Restore the default value of default queue	**undo qos cql** *cql-index* **default-queue**

We can define several rules for a custom-list and apply the rules to an interface. When a packet is treated by the interface (the packet needs to be sent out via this interface), the system will match this packet along rule chain; if it matched with a certain rule, then it will enter the corresponding queue and the matching is finished, otherwise, the packet will enter default queue.

The default value of default queue is 1.

IV. Configuring length of the queue

Designate length for a custom queue (i.e. Capacity of the queue).

Perform the following configuration in system view.

Table 3-13 Configure the length of the queue

Operation	Command
Configure the length of the queue	**qos cql** *cql-index* **queue** *queue-number* **queue-length** *queue-length*
Restore the default length of each queue	**undo qos cql** *cql-index* **queue** *queue-number* **queue-length** *queue-length*

The *queue-length* argument specifies the maximum queue length; it defaults to 20.

V. Configuring the queue continuously sending bytes

Configure the bytes of packets sent by polling of each queue.

Perform the following configuration in system view.

Table 3-14 Configure the queue continuously sending bytes

Operation	Command
Configure the queue continuously sending bytes	**qos cql** *cql-index* **queue** *queue-number* **serving** *byte-count*
Recover the default value of sending bytes	**undo qos cql** *cql-index* **queue** *queue-number* **serving**

In which:

byte-count: When Router dispatches user queue of CQ, it will continuously pick out the packets to send from this queue till the sending bytes are no less than value of *byte-count* configured for this queue or the queue is empty, then it will dispatch another user queue of CQ. So the value of *byte-count* will affect the proportion of interface bandwidth occupied by every user queue of CQ, and also determine the time interval of dispatching another queue of CQ by the Router. The default byte number of *byte-count* is 1500.

If the value of *byte-count* is too small, since the router won't treat the packets in the next queue unless at least one packet in the former one is sent out, the actual acquired bandwidth of a queue would be far from that expected. If *byte-count* is too large, it may cause great switch delay between different queues.

3.4.2 Applying Custom-list on the Interface

Perform the following configuration in interface view.

Table 3-15 Apply custom-list on the interface

Operation	Command
Apply Custom-list on the interface	**qos cq cql** *cql-index*
Cancel using CQ on the interface	**undo qos cq**

Not CQ but FIFO is employed on the interface by default.

⚠ **Caution:**

Except for interfaces encapsulated with X.25 or LAPB, all physical interfaces can use CQ.

You can apply CQ to a dialer interface. Before that, make sure the queuing configuration on its physical interfaces is the default.
In addition, if these physical interfaces have had connections with their respective connected devices, the applied queuing configuration cannot update to them immediately. Instead, the configuration updates to the physical interfaces the next time they set up connections.

3.4.3 Displaying and Debugging Custom-list Queue

After the above configuration, execute **display** commands in any view to display the running of the custom-list queue configuration, and to verify the effect of the configuration.

Table 3-16 Display custom-list queue status and application on the interfaces

Operation	Command
Display custom-list queue status	**display qos cql**
Display custom-list queue application status on the interfaces	**display qos cq interface** [*interface-type interface-number*]

3.5 WFQ Configuration

Configuring WFQ (Weighted Fair Queuing) includes:

- Use WFQ or modify WFQ parameters

3.5.1 Using WFQ or Modifying WFQ Parameters

WFQ classifies packets based on traffic. For IP networks, packets belong to the same stream if they have the same quintuple (source IP address, destination IP address, source port, destination port, and IP protocol) and IP precedence/DSCP value.

Usually, on access networks, traffic classification involves IP precedence and IP quintuple, while on distribution networks, DSCP and IP quintuple. You can select as needed.

In case there is no WFQ employed on the interface, this command can be used to employ WFQ and designate the parameter for WFQ, otherwise, this command can be used to modify the parameters of WFQ.

Perform the following configuration in interface view.

Table 3-17 Use WFQ or modify WFQ parameters

Operation	Command
Use WFQ or modify WFQ parameters	**qos wfq** [**precedence** | **dscp**] [**queue-length** *max-queue-length* [**queue-number** *total-queue-number*]]
Remove WFQ setting	**undo qos wfq**

FIFO instead of WFQ is employed on the interface by default.

⚠ **Caution:**

Except for interfaces encapsulated with X.25 or LAPB, all physical interfaces can use WFQ.

You can apply WFQ to a dialer interface. Before that, make sure the queuing configuration on its physical interfaces is the default.

In addition, if these physical interfaces have had connections with their respective connected devices, the applied queuing configuration cannot update to them immediately. Instead, the configuration updates to the physical interfaces the next time they set up connections.

3.5.2 Displaying and Debugging WFQ

After the above configuration, execute the **display** command in any view to display the running of the configuration and statistics information of WFQ on one or interfaces, and to verify the effect of the configuration.

Table 3-18 Display the configuration and statistics of WFQ on one or all interfaces

Operation	Command
Display the configuration and statistics information of WFQ on interfaces	**display qos wfq interface** [*interface-type interface-number*]

3.6 Class-based Queuing Configuration

The class-based queuing CBQ configuration includes:

- Configure the maximum available bandwidth on the interface
- Define the class and define a group of traffic classification rules in the class view.
- Define traffic behavior, and define a group of QoS features in the traffic behavior view.
- Define the policy, and define the corresponding traffic behavior for the class in use in the policy view.
- Apply QoS policy in the interface or ATM PVC view.

The system pre-defines some classes, traffic behaviors and policies. The detailed description is given below.

I. Pre-defined classes

The system pre-defines some classes and defines general rules for them. The user can use the pre-defined classes when defining the policy. The classes include:

1) Default class: default-class, matching the default data flow.
2) DSCP-based pre-defined class: ef, af1, af2, af3, af4, matching IP DSCP values of ef, af1, af2, af3, af4 respectively.
3) IP priority-based pre-defined class: ip-prec0, ip-prec1, ip-prec7: matching IP priorities of 0, 1, and 7 respectively.
4) MPLS EXP-based pre-defined class: mpls-exp0, mpls-exp1, …mpls-exp7: matching MPLS EXP values of 0, 1, …7.

II. Pre-defined traffic behaviors

The system pre-defines some traffic behaviors and defines QoS features for them.

1) ef: Defines a feature of input EF queue, occupying 20% of the available bandwidth of the interface.
2) af: Defines a feature of input AF queue, occupying 20% of the available bandwidth of the interface.
3) be: Defines no features.

III. Pre-defined policies

The system pre-defines a policy, and specifies the pre-defined class for the policy and specifies the pre-defined behavior for the class. The policy is named default, with the default CBWFQ behavior.

The detailed rules of the default policy are as follows.

1) Pre-defined class ef, adopting pre-defined traffic behavior of ef.
2) Pre-defined classes af1 to af4, adopting pre-defined traffic behavior of af.
3) default-class, adopting pre-defined traffic behavior of be.

3.6.1 Configuring the Maximum Available Bandwidth on the Interface

The bandwidth discussed here refers to the maximum interface bandwidth used when CBQ enqueues packets, rather than the actual bandwidth of the physical interface.

Perform the following configurations in interface view.

Table 3-19 Configure bandwidth of the interface

Operation	Command
Configure the bandwidth of the interface.	**qos max-bandwidth** *bandwidth*
Restore the default bandwidth.	**undo qos max-bandwidth**

The *bandwidth* argument indicates the available bandwidth of the interface. It is in kbps (1 to 1000000). By default, this value is the actual interface baud rate or speed for a physical interface, the total bandwidth of the channel set for a logical serial interface that is formed by bundling in T1/E1 or MFR, or 64 kbps for a logical interface like virtual template or VE.

The maximum available bandwidth of an interface is preferred to be smaller than the real available bandwidth of the physical interfaces or the logical links. For a serial interface, the value defaults to 64 kbps. To modify it, you can change the interface rate using the **baudrate** command to 2.048 Mbps for example, and then set a new value, 115.2 kbps for example.

3.6.2 Configuring Matching Rules of a Class

Before you can define a class, you must first create its class name. Then you can configure matching rules in this class view. The rules come in many types, and many of them have restrictions on packet types, for example:

- destination-mac, source-mac, and dot1p-cos are effective only for Ethernet packets.
- mpls-exp is effective in the inbound direction only for MPLS packets.

- mpls-exp (in the outbound direction), ip-precedence, dscp, rtp, and acl are effective for IP and MPLS packets.
- fr-de, atm-clp, protocol, inbound-interface, any, and classifier are effective for all packets.

When packets of a certain class do not meet the packet type restrictions of a rule, the rule is senseless and regarded as ineffective, and the system will neglect it when performing process by class.

I. Defining a class and enter the class view

Perform the following configuration in system view.

Table 3-20 Define a class and enter the class view

Operation	Command
Define a class and enter the class view	**traffic classifier** *tcl-name* [**operator** { **and | or** }]
Delete a class	**undo traffic classifier** *tcl-name*

The user-defined class name *tcl-name* should not be that of the classes pre-defined by the system.

By default, the class is defaulted to **and**. That is, the relation between respective matching rules in the class view is logic AND.

II. Defining/deleting the rule matching all packets

Perform the following configurations in class view.

Table 3-21 Define/delete the rule matching all packets

Operation	Command
Define the rule matching all packets	**if-match** [**not**] **any**
Delete the rule matching all packets	**undo if-match** [**not**] **any**

III. Defining/deleting classifier match rule

Perform the following configurations in class view.

Table 3-22 Define/delete classifier match rule

Operation	Command
Define classifier match rule	**if-match** [**not**] **classifier** *tcl-name*
Delete classifier match rule	**undo if-match** [**not**] **classifier** *tcl-name*

This command cannot be used circularly. For example, traffic classifier A defines the rules to match traffic classifier B but traffic classifier B cannot define a rule match traffic classifier A directly or indirectly.

IV. Defining/deleting ACL match rule

Perform the following configurations in class view.

Table 3-23 Define/delete ACL match rule

Operation	Command
Define ACL match rule	**if-match** [**not**] **acl** *access-list-number*
Delete ACL match rule	**undo if-match** [**not**] **acl** *access-list-number*

V. Defining/deleting match rule of MAC address

Perform the following configurations in class view.

Table 3-24 Define/delete MAC address match rule

Operation	Command
Define MAC address match rule	**if-match** [**not**] { **destination-mac** | **source-mac** } *mac-address*
Delete MAC address match rule	**undo if-match** [**not**] { **destination-mac** | **source-mac** } *mac-address*

This command applies to only Ethernet interface. The match rules of the destination MAC address are only meaningful for policies in the outbound direction. The match rules of the source MAC address are only meaningful for policies in the inbound direction.

VI. Defining/deleting input-interface match rule of a class

Perform the following configurations in class view.

Table 3-25 Define/delete input-interface match rule of a class

Operation	Command
Define input-interface match rule of a class	**if-match** [**not**] **inbound-interface** *type number*
Delete input-interface match rule of a class	**undo if-match** [**not**] **inbound-interface** *type number*

The rule will be deleted automatically when the matched interface is deleted.

VII. Defining/deleting DSCP match rule

DSCP (Differentiated Services Code Point) is a refined field from the 6 high bits of ToS bytes in IP header by IETF DiffServ workgroup. In the solution submitted by DiffServ, services are classified and traffic is controlled according to service requirements at network ingress. Simultaneously, DSCP is set. In the network, packets are classified with services like resource allocation and packet discard policy according to their DSCP values.

The user can set classified matching rules using DSCP values.

Perform the following configurations in class view.

Table 3-26 Define/delete DSCP match rule

Operation	Command
Define DSCP match rule	**if-match** [**not**] **dscp** *dscp-value*
Delete DSCP match rule	**undo if-match** [**not**] **dscp** *dscp-value*

VIII. Defining/deleting ip precedence match rule

Perform the following configurations in class view.

Table 3-27 Define/delete ip precedence match rule

Operation	Command
Define ip precedence match rule	**if-match** [**not**] **ip-precedence** *ip-precedence-value*
Delete ip precedence match rule	**undo if-match** [**not**] **ip-precedence**

The configuration of the **if-match ip precedence** command will overwrite the previous configurations.

IX. Defining/deleting RTP port match rule

Perform the following configurations in class view.

Table 3-28 Define/delete RTP port match rule

Operation	Command
Define RTP port match rule	**if-match** [**not**] **rtp** **start-port** *starting-port-number* **end-port** *end-port-number*
Delete RTP port match rule	**undo if-match** [**not**] **rtp**

Because the RTP queue has a higher priority than CBQ, the RTP will take effect when both the RTP queue and the CBQ queue based on the class matching RTP are configured.

X. Defining/deleting protocol match rule

Perform the following configurations in class view.

Table 3-29 Define/delete protocol match rule

Operation	Command
Define protocol match rule	**if-match** [**not**] **protocol** *protocol-name*
Delete protocol match rule	**undo if-match** [**not**] **protocol** *protocol-name*

protocol-name: Only the IP protocol is used.

XI. Defining/deleting an ATM CLP bit match rule

In ATM cell headers, CLP bit is used for traffic control. When network congestion occurs, ATM cells with CLP bit set to 1 are dropped first.

Perform the following configuration in class view.

Table 3-30 Define/delete an ATM CLP bit match rule

Operation	Command
Define an ATM CLP bit match rule (CLP bit set to 1 or 0)	**if-match** [**not**] **atmclp**
Delete the configured ATM CLP bit match rule	**undo if-match** [**not**] **atmclp**

Use the **if-match atmclp** command to create a cell loss priority (CLP) bit match rule defining that ATM cells with CLP bit set to 1 are matched.

Use the **if-match not atmclp** command to create a CLP bit match rule defining that ATM cells with CLP bit set to 0 are matched.

XII. Defining/deleting a CoS field match rule for VLAN packets

Perform the following configuration in class view.

Table 3-31 Define/delete a CoS field match rule for VLAN packets

Operation	Command
Define a CoS field match rule for VLAN packets	**if-match** [**not**] **dot1p-cos** *cos-value*
Delete the specified CoS field match rule for VLAN packets	**undo if-match** [**not**] **dot1p-cos** *cos-value*

XIII. Defining or deleting an FR DE matching rule

Perform the following configuration in class view.

Table 3-32 Define or delete an FR DE matching rule

Operation	Command
Define an FR DE matching rule	**if-match [not] fr-de**
Delete the FR DE matching rule	**undo if-match [not] fr-de**

The **if-match fr-de** command matches packets with the FR DE bit set to 1, while the **if-match not fr-de** command matches packets with the FR DE bit left as 0.

XIV. Defining or deleting an outbound subinterface matching rule

Perform the following configuration in class view.

Table 3-33 Define or delete an outbound subinterface matching rule

Operation	Command
Define an outbound subinterface matching rule	**if-match [not] outbound-subinterface** *interface-type interface-number.subinterface-number*
Delete an outbound subinterface matching rule	**undo if-match [not] outbound-subinterface** *interface-type interface-number.subinterface-number*

The interface specified in this command must support subinterfaces. At present, it can be GE, FE, FR, or MFR only.

In addition, a policy containing a rule defined using this command must be applied to the main interface where the specified subinterface is located. If the policy is applied to a subinterface or to a PVC created on the main interface, the rule cannot take effect.

3.6.3 Configuring Features of a Traffic Behavior

To define a traffic behavior, you should first create a traffic behavior name and then configure attributes for it in the new traffic behavior view.

I. Defining a traffic behavior and Entering traffic behavior view

Perform the following configuration in system view.

Table 3-34 Define a traffic behavior and enter traffic behavior view.

Operation	Command
Define a traffic behavior and enter traffic behavior view.	**traffic behavior** *behavior-name*
Delete a traffic behavior	**undo traffic behavior** *behavior-name*

behavior-name: Name of the traffic behavior. It is not the name of the traffic behavior pre-defined by the system.

II. Configuring AF and minimum available bandwidth

Perform the following configurations in traffic behavior view.

Table 3-35 Configure AF and minimum available bandwidth

Operation	Command
Configure AF and minimum available bandwidth	**queue af bandwidth** { *bandwidth* | **pct** *percentage* }
Delete the configuration	**undo queue af**

This behavior can apply only in output direction of an interface or ATM PVC.

The same traffic behavior must use the same standard to configure **queue ef** and **queue af**, either bandwidth or percentage.

When the service traffic sent to the network from an application is below the specified value, AF ensures a low drop priority. AF has four classes, each containing up to three levels of drop precedence.

III. Configuring ef and maximum bandwidth

Perform the following configurations in traffic behavior view.

Table 3-36 Configure ef and maximum bandwidth

Operation	Command
Configure ef and maximum bandwidth	**queue ef bandwidth** { *bandwidth* [**cbs** *committed-burst-size*] | **pct** *percentage* [**cbs_ratio** *ratio*] }
Delete the configutation	**undo queue ef**

In traffic behavior view, this command cannot be used along with **queue af**, **queue-length** and **wred**.

This command cannot be used for default-class.

The same traffic behavior must use the same standard to configure **queue ef** and **queue af**, either bandwidth or percentage.

EF applies to the applications that support low drop ratio, low delay, and assured bandwidth.

IV. Configuring weight fair queuing (WFQ)

Perform the following configuration in traffic behavior view.

Table 3-37 Configure WFQ

Operation	Command
Configure WFQ	**queue wfq** [**queue-number** *total-queue-number*]
Delete the configured	**undo queue wfq**

Configure that the traffic behavior of the feature can only be associated with the default class.

V. Configuring maximum queue length

Configure maximum queue length and the drop type is tail drop.

Perform the following configurations in traffic behavior view.

Table 3-38 Configure maximum queue length

Operation	Command
Configure maximum queue length	**queue-length** *queue-length*
Delete the configuration	**undo queue-length**

This command can be used only after the **queue af** command and **queue wfq** command have been configured.

Execute the **undo queue af** command and **undo queue wfq** command, then **queue-length** will be deleted as well.

For the default-class, this command can be used only after the **queue af** or **queue wfq** command has been configured.

VI. Configuring the drop type as WRED

Perform the following configurations in traffic behavior view.

Table 3-39 Configure the discarding mode as WRED

Operation	Command
Configure the discarding mode as WRED	**wred** [**dscp | ip-precedence**]

Operation	Command
Restore the default setting	**undo wred**

dscp indicates that the dscp value is used to calculate drop proportion of a packet.

Ip-precedence indicates that the IP precedence value is used to calculate discard proportion of a packet, which is the default setting.

This command can be used only after the **queue af** command and **queue wfq** command have been configured. The **wred** and **queue-length** are mutually exclusive. Other configurations under the random drop will be deleted when this command is deleted. When a QoS policy included WRED is applied on an interface, the original WRED configuration on interface will be ineffective.

The default-class can only be associated with the traffic behavior configured the WRED drop based on the IP precedence.

VII. Configuring exponential of average queue length calculated by WRED

Perform the following configurations in traffic behavior view.

Table 3-40 Configure exponential of average queue length calculated by WRED

Operation	Command
Configure exponential of average queue length calculated by WRED	**wred weighting-constant** *exponent*
Delete the configuration	**undo wred weighting-constant**

This command can be used only after the **queue af** command has been configured and the **wred** command has been used to enable WRED.

VIII. Configuring DSCP lower-limit, upper-limit and discard probability of WRED

Perform the following configurations in traffic behavior view.

Table 3-41 Configure DSCP lower-limit, upper-limit and discard probability of WRED

Operation	Command
Configure DSCP lower-limit, upper-limit and discard probability of WRED	**wred dscp** *dscp-value* **low-limit** *low-limit* **high-limit** *high-limit* [**discard-probability** *discard-prob*]
Delete the configuration	**undo wred dscp** *dscp-value*

The *dscp-value* is in the range of 0 to 63, which can be any of the following keys: **ef**, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, or **default**.

The DSCP based WRED drop type has been enabled via the **wred dscp** command.

When the configuration of **wred** is deleted, the **wred dscp** will be deleted at the same time.

When the configuration of **queue af** is deleted, the configuration of discarding parameters is deleted also.

IX. Configuring lower-limit, upper-limit and discard probability of WRED precedence

Perform the following configurations in traffic behavior view.

Table 3-42 Configure lower-limit, upper-limit and discard probability of WRED precedence

Operation	Command
Configure lower-limit, upper-limit and discard probability of WRED precedence	**wred ip-precedence** *precedence* **low-limit** *low-limit* **high-limit** *high-limit* [**discard-probability** *discard-prob*]
Delete the configuration	**undo wred ip-precedence** *precedence*

Precedence based WRED has been enabled via the **wred ip-precedence** command.

When the configuration of **wred** is deleted, the **wred ip-precedence** will also be deleted.

When the configuration of **queue af** is deleted, the configuration of discarding parameters will also be deleted.

X. Using/removing traffic policing

Perform the following configurations in traffic behavior view.

Table 3-43 Use/remove traffic policing

Operation	Command
Use traffic policing	**car cir** *committed-information-rate* [**cbs** *committed-burst-size* **ebs** *excess-burst-size*] [**green** *action* [**red** *action*]]
Remove traffic policing	**undo car**

The defined CIR value should not exceed CBS x 20.

In the command, action is a behavior conducted to the packets, which includes the following types:

- **discard**: Drops the packet
- **remark-dscp-pass** *new-dscp*: Sets new-dscp and transmit the packet.
- **remark-prec-pass** *new-precedence*: Sets new-precedence of IP and transmit the packet.
- **remark-mpls-exp-pass** *new-exp*: Sets the new MPLS EXP and transmit the packet.
- **pass**: Transmits the packet.

The policy in which TP is used in traffic behavior on an interface can be used in the input or output of the interface.

The policy in which TP is used in traffic behavior on an interface will cause the previous **qos car** command ineffective on the interface.

If this command is frequently configured on the class of the same behavior, the last configuration will replace the previous one.

The traffic configured with shaping and policing but without AF or EF behavior can be sent if it passes the detection of policing or shaping. However, in case of congestion, the traffic will enter the default queue.

XI. Configuring/deleting TS

Perform the following configurations in traffic behavior view.

Table 3-44 Configure/delete TS

Operation	Command
Configure traffic shaping	**gts cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size* [**queue-length** *queue-length*]]]
Delete traffic shaping	**undo gts**

When behavior including TS is used in the policy, it can only be used in the egress interface.

When the policy with behavior including TS is applied on the interface, the **qos gts** command configured on the interface will become invalid.

If this command is frequently configured on the same behavior, the last configuration will replace the previous one.

The traffic configured with shaping and policing but without AF or EF behavior can be sent if it passes the detection of policing or shaping. However, in case of congestion, the traffic will enter the default queue.

XII. Configuring/disabling LR

Perform the following configuration in traffic behavior view.

Table 3-45 Configure/disable LR

Operation	Command
Configure LR	**lr cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] or **lr percent cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]]
Disable LR	**undo lr**

The policy that contains LR behaviors can only be applied to the outgoing direction of interfaces.

The LR configured using the **lr** or **lr percent** command will replace the previous LR configuration, if there is any.

When configuring LR with policy embedding, observe the following rules:

- For a parent policy, you can configure queuing in its child policy only when it has been configured with LR using the **lr** or **lr percent** command. In this case, the queue length in the child policy applies. (You can configure queue length using the **qos gts** command.) If the child policy has no queuing configuration, traffic is put in a FIFO queue whose length is fixed to 200. You cannot delete the LR setting in the parent policy after queuing is configured in the child policy.

When configuring LR on an ATM or FR interface, consider the following:

- LR can be applied to ATM PVCs but not to ATM interfaces.
- On FR PVCs, you can configure the **lr** command but not the **lr percent** command.
- On an FR interface configured with the **fr traffic-shaping** command, you cannot configure LR.
- LR cannot be configured in a child policy.

XIII. Remarking DSCP value

Perform the following configuration in traffic behavior view.

Table 3-46 Remark DSCP value for packets

Operation	Command
Remark DSCP value for packets	**remark dscp** *dscp-value*
Disable remarking DSCP value for packets	**undo remark dscp**

XIV. Remarking IP precedence value

Perform the following configuration in traffic behavior view.

Table 3-47 Remark IP precedence value

Operation	Command
Remark IP precedence value for packets	**remark ip-precedence** *ip-prec-value*
Disable remarking IP precedence value for packets	**undo remark ip-precedence**

XV. Remarking the 802.1p preference of VLAN packets

Perform the following configurations in traffic behavior view.

Table 3-48 Remark the 802.1p preference of VLAN packets

Operation	Command
Remark VLAN packets with the specified 802.1p preference value.	**remark dot1p** *cos-value*
Disable remarking the 802.1p preference of VLAN packets.	**undo remark dot1p**

XVI. Remarking DE value for FR packets

Perform the following configuration in traffic behavior view.

Table 3-49 Remark DE value for FR packets

Operation	Command
Remark DE value for FR packets	**remark fr-de** *fr-de-value*
Disable remarking DE value for FR packets	**undo remark fr-de**

XVII. Remarking the cell loss priority (CLP) bit of ATM packets

Perform the following configuration in traffic behavior view.

Table 3-50 Remark the CLP bit of ATM packets

Operation	Command
Remark the CLP bit of ATM packets.	**remark atmclp** *atmclp-value*

Operation	Command
Disable remarking the CLP bit of ATM packets.	**undo remark atmclp**

This behavior applies only in the outbound direction of interfaces and ATM PVCs.

XVIII. Configuring/disabling policy embedding

After defining a class using the **traffic classifier** command, you can have it perform the associated behavior defined in its policy and in addition, use a child policy to further classify the class, having it perform the behavior defined in the child policy. You can thus implement policy embedding. To understand how policy embedding works, refer to the section 3.8.5 "Integrated QoS Policy Embedding and LR Configuration Example".

Perform the following configuration in traffic behavior view.

Table 3-51 Configure/disable policy embedding

Operation	Command
Associate a child policy to the behavior	**traffic-policy** *policy-name*
Disable policy embedding	**undo traffic-policy**

When embedding a child policy in a policy, note that:

- Policy embedding is two-tier only.
- If both of them are configured with the remark behavior, only the remark setting in the child policy is executed. If both of them are configured with CAR or GTS, the two CAR or GTS settings are executed, but the one in the child policy is executed first. If both of them are configured with queuing (LR is mandatory for the policy in this case), the packets that conform to the LR setting are enqueued according to the policy and the nonconforming packets are enqueued according to the child policy.
- Make sure that LR is applied to the class associated with the parent policy before embedding a child policy configured with the **queue ef**, **queue af**, or **queue wfq** behavior.
- Policy embedding can be applied to physical interfaces, subinterfaces, FR PVCs, and ATM PVCs.
- Policy embedding can be applied in both inbound and outbound directions of an interface or PVC. However, you cannot configure the child policy with LR, CBQ, GTS, FR DE remark, or CLP remark in the inbound direction, or configure FR DE remark or ATM CLP remark in the outbound direction. In addition, for the child policy, 802.1p remark is valid only on Ethernet interfaces (excluding virtual Ethernet interfaces) and CBQ is valid on the interfaces except for ATM physical

interfaces, virtual Ethernet interfaces, and subinterfaces. Note that CBQ can be configured on ATM PVCs.

- LR cannot be configured in a child policy.
- *committed-information-rate* can be less than 8000 in an embedded child policy

3.6.4 Configuring Policy

I. Defining the Policy and entering the Policy View

Policy mapping defines the traffic behavior of each class in the policy. Each traffic behavior is composed of a group of features, including EF, AF, WFQ, TP, TS, WRED and label.

Perform the following configurations in the system view.

Table 3-52 Define the policy and enter the policy view

Operation	Command
Define the policy and enter the policy view	**qos policy** *policy-name*
Delete the specified policy	**undo qos policy** *policy-name*

The policy name should not be that of the policies pre-defined by the system.

When creating the policy, the default has the default-class as the default class, which associates with be behavior.

If this policy is applied on an interface, it cannot be deleted. The user must remove the application of this policy on the interface and then delete the policy with the **undo qos policy** command.

II. Specifying the Traffic Behavior for the Class in the Policy

Perform the following configurations in the policy view.

Table 3-53 Specify the traffic behavior for the class in the policy

Operation	Command
Specify the traffic behavior for the class in the policy	**classifier** *tcl-name* **behavior** *behavior-name*
Remove the application of the specified class in the policy	**undo classifier** *tcl-name*

tcl-name: Class name. It must be that of the defined class, the system-defined or user-defined class.

behavior-name: It must be that of the defined behavior, the system-defined or user-defined behavior.

3.6.5 Applying Policy

The **qos apply policy** command maps a policy to an interface. One policy can be applied on multiple interfaces.

Perform the following configuration in interface, subinterface, or ATM PVC view.

Table 3-54 Apply a policy to the interface or ATM PVC

Operation	Command
Apply a policy to the interface or ATM PVC	**qos apply policy** *policy-name* { **inbound** | **outbound** [**dynamic**] }
Delete the policy from the interface or ATM PVC	**undo qos apply policy** { **inbound** | **outbound** }

dynamic applies only to the dial or VT interface configured with MP for dynamic policy application. Before applying a QoS policy to such a dial or VT interface, use the **qos max-bandwidth** command to configure adequate bandwidth for running the policy.

I. Applying a QoS policy in interface (except for ATM interface) view

- CBQ could not be applied to an interface encapsulated with X.25 or LAPB.
- The VT interface referenced by common physical port and MP can apply the policy configured with various features, including remark, car, gts, queue af, queue ef, queue wfq, wred, etc.
- The policy configured with TS (e.g. gts) and queue (e.g. queue ef, queue af, queue wfq) features cannot be applied on the inbound interface as the input direction policy.
- The subinterface does not support queue (e.g. queue ef, queue af, queue wfq) feature but support TS (e.g. gts) and TP (e.g. car). The policy configured with TS and TP can be applied on the sub-interface.

II. Applying a QoS policy in subinterface view

When configuring an LR or CBQ policy for a subinterface, consider the following:

- All QoS restrictions applied to the main interface take effect on the subinterface.
- When policy embedding is used, CBQ must be configured in the child policy instead of the parent policy.
- In a QoS policy, LR cannot be configured using the **lr percent** command.
- If queuing is configured on the main interface, it can be FIFO only.
- The policy configured on the main interface cannot include LR behaviors.
- The sum of the LRs configured for all subinterfaces cannot exceed the available bandwidth of the main interface. (Available interface bandwidth refers to the interface bandwidth configured using the **qos max-bandwidth** command or the physical interface bandwidth when command is not configured.)

- For an FR subinterface, FR traffic shaping must be disabled on its main interface.

When configuring a QoS policy for a main interface, consider the following:

- You can configure CQ, PQ, WFQ, CBQ, or RTPQ on the main interface only when LR is not configured on its subinterfaces;
- You can configure an LR policy on the main interface only when no LR policy is configured on its subinterfaces.

During your configuration, you can see prompts if above restrictions are not met.

⚠ **Caution:**

- After traffic shaping is enabled on an FR main interface, all policies containing LR behaviors are to be removed from its subinterfaces.
- After you change the available bandwidth of a main interface with the **qos max-bandwidth** command, all policies containing LR behaviors are to be removed from its subinterfaces if the new available bandwidth is smaller than the sum of the LRs configured for the subinterfaces.

III. Applying a QoS policy to an ATM interface

- In the inbound direction, only DSCP remark and IP precedence remark are allowed. In the outbound direction, DSCP remark, IP precedence remark, ATM CLP bit remark, EF, AF, WFQ, CBQ, and GTS are allowed. Although ATM PVCs can support policies with GTS included, you cannot directly configure GTS on ATM PVCs.
- On an ATM PVC interface, DSCP remark, IP precedence remark, or CBQ is valid only when IPoA applies. They are invalid when IPoEoA, PPPoA, or PPPoEoA applies.
- For IPoEoA, PPPoA, and PPPoEoA packets, DSCP remark and IP precedence remark are valid only on virtual template or virtual Ethernet interfaces. On ATM physical interfaces, they are invalid.

3.6.6 Displaying and Debugging CBQ

After the above configuration, execute **display** commands in any view to display the running of the CBQ configuration, and to verify the effect of the configuration.

Table 3-55 Display and debug CBQ

Operation	Command
Configure the QoS policy traffic statistical interval and rate updating interval	**flow-interval qos** *flow-interval* [**update-interval** *seconds*]

Operation	Command
Display class information configured on the router	**display traffic classifier** { **system-defined** | **user-defined** } [*tcl-name*]
Display configuration information of specified traffic behavior	**display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*]
Display configuration information of specified class of specified policy and behavior associated with these classes.	**display qos policy** { **system-defined** | **user-defined** } [*policy-name* [**classifier** *tcl-name*]]
Display policy configuration information and operating condition of specified or all interface or ATM PVC.	**display qos policy interface** [*interface-type interface-number* [**inbound** | **outbound**] [**pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }]]
Display CBQ configuration information and operating condition of specified interface, specified PVC on specified or all interface or ATM PVC.	**display qos cbq interface** [*interface-type interface-number* [**pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }]]
Display debugging information of queue	**debugging qos cbq** { **ef** | **af** | **be** }

3.7 RTP Priority Queuing Configuration

RTP priority queue configuration includes:

- Apply RTP priority queuing on the interface
- Configure bandwidth limitation
- Display and debug RTP priority queuing configuration

3.7.1 Applying RTP priority queuing on the interface

The following command is used to apply RTP priority queue on the interface. It has no default configuration.

Perform the following configurations in interface view.

Table 3-56 Apply RTP priority queuing on the interface

Operation	Command
Apply RTP priority queuing on the interface	**qos rtpq start-port** *first-rtp-port-number* **end-port** *last-rtp-port-number* **bandwidth** *bandwidth* [**cbs** *committed-burst-size*]
Disable RTP priority queuing from the interface	**undo qos rtpq**

⚠ **Caution:**

Except for interfaces encapsulated with X.25 or LAPB, all physical interfaces can use RTPQ.

You can apply RTPQ to a dialer interface. Before that, make sure that the queuing configuration on its physical interfaces is the default and their bandwidth is adequate.

3.7.2 Configuring Maximum Reserved Bandwidth

This command can set the max reserved bandwidth percentage of the available bandwidth.

Perform the following configurations in interface view.

Table 3-57 Configure bandwidth limitation

Operation	Command
Configure bandwidth limitation	**qos reserved-bandwidth pct** *percentage*
Restore the default value	**undo qos reserved-bandwidth**

The *percentage* argument is the percentage of the reserved bandwidth. It is in the range of 1 to 100 and the default value is 80.

3.7.3 Displaying and Debugging RTP Priority Queuing Configuration

The following command can display the queue information of the current IP RTP Priority, including the current RTP queue length and number of RTP packet dropping. It can display the RTP priority queue configuration and statistics on an interface or on all interfaces.

Perform the following configuration in any view.

Table 3-58 Display RTP priority queue configuration and statistics on an interface

Operation	Command
Display configuration and statistics of RTP priority queue on an interface	**display qos rtpq interface** [*interface-type interface-number*]

3.7.4 Token Function of QoS

When FTP is used to transfer data, the upper layer protocol such as TCP provides the flow control function. This can however cause the configuration of CQ and WFQ, if they are configured, to lose effect. To resolve this problem, the token function of QoS was introduced into V 2.41. This function provides a flow control mechanism at the underlying layer queuing level. It can control the number of packets sent to the underlying interface queues based on the number of tokens.

If FTP applies, you are recommended to set the number of tokens sent by an interface to 1.

If the upper layer protocol, UDP for example, does not provide flow control, you are not recommended to use the token function of QoS in order to improve efficiency of data transfer.

Perform the following configuration in interface view.

Table 3-59 Configure the token function of QoS

Operation	Command
Configure the token function of QoS.	**qmtoken** *token-number*
Disable the token function of QoS.	**undo qmtoken**

By default, the token function of QoS is disabled.

Note:

After you configure this command on an interface, you must perform **shutdown** and **undo shutdown** on the interface to have the function take effect.
So far, this command is supported only by Ethernet, serial, and BRI interfaces.

3.8 Typical Configuration Example

3.8.1 PQ Configuration Example

I. Network requirements

As shown in the diagram, both Server and PC1 send data to PC2 through router 3Com1. Suppose Server sends key service data and PC1 sends common service data. Congestion may occur on interface serial2/0/0 resulting in packet loss because the rate of the incoming interface ethernet0/0/0 is larger than that of the outgoing interface serial2/0/0 on 3Com1. The mission-critical service data has priority when network congestion occurs.

II. Network diagram

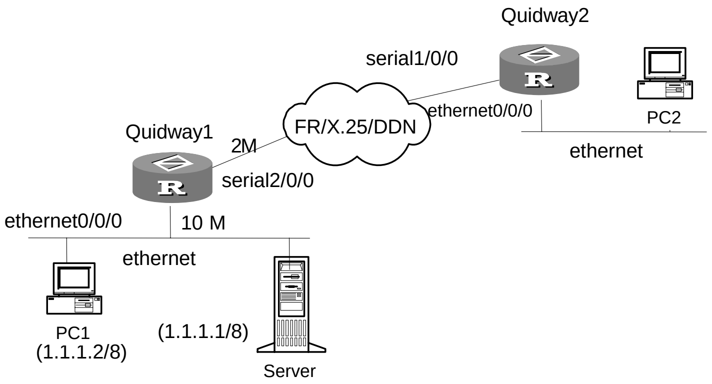


Figure 3-6 Network diagram for PQ configuration

III. Configuration procedure

Configure the router 3Com1:

# Configure ACL to match the packets from Server and PC1 respectively.

```
[3Com1] acl number 2001
[3Com1-acl-basic-2001] rule permit source 1.1.1.1 0.0.0.0
[3Com1-acl-basic-2001] quit
[3Com1] acl number 2002
[3Com1-acl-basic-2002] rule permit source 1.1.1.2 0.0.0.0
[3Com1-acl-basic-2002] quit
```

# Configure the priority-group so that the packets from Server can enter the high queue for cache and those from PC1 can enter the low queue for cache when the network congestion happens. The maximum queue length of the high queue should be set to 50 while that of the low queue set to 100.

```
[3Com1] qos pql 1 protocol ip acl 2001 queue top
[3Com1] qos pql 1 protocol ip acl 2002 queue bottom
[3Com1] qos pql 1 queue top queue-length 50
[3Com1] qos pql 1 queue bottom queue-length 100
```

# Apply the priority-group 1 on the interface serial 2/0/0

```
[3Com1] interface serial2/0/0
[3Com1-Serial2/0/0] qos pq pql 1
```

3.8.2 CBQ Configuration Example

I. Network requirements

As shown in the diagram, Router C sends data streams, which, in terms of DSCP domain of IP packet, can be grouped into four categories, across Router A and Router

B and finally to Router D. QoS policy is required in configuration. For the data streams with DSCP domain being AF11 and AF21, AF (assured forwarding) and minimum bandwidth 5% is defined, while for those with DSCP domain being EF, EF and minimum bandwidth 30% is specified.

For EF streams, their requirements for bandwidth, delay and jitter can be guaranteed, while LLQ technology is used to achieve their priority. Only bandwidth can be warranted in AF streams, while no bandwidth and delay guarantee is available for **Default** streams (the streams that do not match any class).

Check the following items before initiating configuration:

- Router C can send packets successful across Router A and Router B to Router D.
- DSCP domain has been configured for the packets before they enter Router A.

II. Network diagram

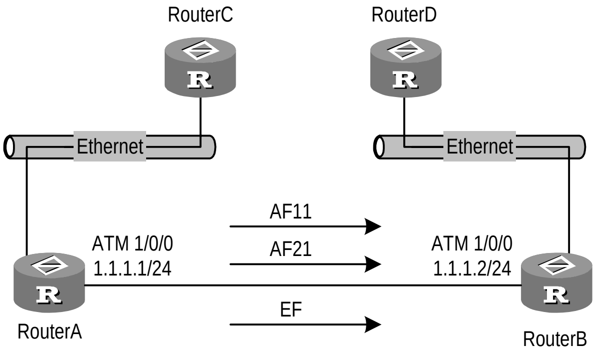


Figure 3-7 Network diagram for class-specific queuing configuration

III. Configuration procedure

Configure Router A

# Define three classes, match them respectively with the IP packets with their DSCP domain respectively being AF11, AF21 and EF.

```
[3Com] traffic classifier af11_class
[3Com-classifier-af11_class] if-match dscp af11
[3Com-classifier-af11_class] traffic classifier af21
[3Com-classifier-af21] if-match dscp af21
[3Com-classifier-af21] traffic classifier ef_class
[3Com-classifier-ef_class] if-match dscp ef
[3Com-classifier-ef_class] quit
```

# Define traffic behavior, configure AF and minimum bandwidth.

```
[3Com] traffic behavior af11_behav
[3Com-behavior-af11_behav] queue af bandwidth pct 5
[3Com-behavior-af11_behav] traffic behavior af21_behav
```

```
[3Com-behavior-af21_behav] queue af bandwidth pct 5
[3Com-behavior-af21_behav] quit
```

# Define traffic behavior, configure EF and minimum bandwidth (bandwidth and delay guarantee also available).

```
[3Com] traffic behavior ef_behav
[3Com-behavior-ef_behav] queue ef bandwidth pct 30
[3Com-behavior-ef_behav] quit
```

# Specify QoS policy and allocate traffic behaviors to different classes.

```
[3Com] qos policy dscp
[3Com-qospolicy-dscp] classifier af11_class behavior af11_behav
[3Com-qospolicy-dscp] classifier af21_class behavior af21_behav
[3Com-qospolicy-dscp] classifier ef_class behavior ef_behav
[3Com-qospolicy-dscp] quit
```

# Apply the QoS policy to the ATM PVC outbound direction of Router A.

```
[3Com] interface atm 1/0/0
[3Com-atm1/0/0] ip address 1.1.1.1 255.255.255.0
[3Com-atm1/0/0] pvc qostest 0/40
[3Com-atm-pvc-atm1/0/0-0/40-qostest] qos apply policy dscp outbound
```

When network congestion occurs, EF streams are forwarded with high priority.

3.8.3 CQ Configuration Example

I. Network requirements

In the following diagram, Router A and Router B are connected back-to-back using a PPP link. Use the PC attached to Router A as FTP and HTTP Server and the PC attached to Router B as FTP and HTTP Client. Configure the routers to have traffic forwarded from Router A to Router B.

Before configuring the routers, make sure to:

- Set up a PPP connection between Router A and Router B, and an FTP connection between the two PCs.
- On the client PC, FTP and HTTP large files from the FTP and HTTP server attached to Router A at the same time.

Customize the FTP and HTTP traffic to share link bandwidth in the ratio of 1 to 2.

II. Network diagram

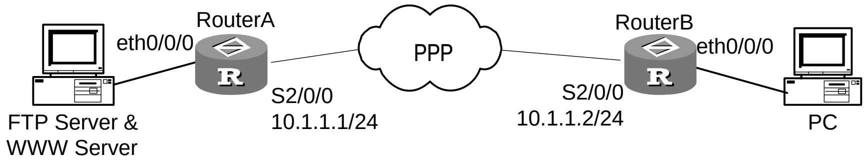


Figure 3-8 Network diagram for CQ configuration

III. Configuration procedure

Configure Router A as follows:

# Configure ACL rules for FTP and HTTP packets

```
[3Com] acl number 3001
[3Com-acl-adv-3001] rule 0 permit tcp source-port eq ftp
[3Com-acl-adv-3001] rule 1 permit tcp source-port eq ftp-data
[3Com-acl-adv-3001] rule 2 deny ip
[3Com] quit
[3Com] acl number 3002
[3Com-acl-adv-3001] rule 0 permit tcp source-port eq www
[3Com-acl-adv-3001] rule 1 deny ip
[3Com-acl-adv-3001] quit
```

# Configure CQ rules, customizing the FTP and HTTP traffic to share link bandwidth in the ratio of 1 to 2.

```
[3Com] qos cql 1 queue 11 serving 1000
[3Com] qos cql 1 queue 12 serving 2000
[3Com] qos cql 1 protocol ip acl 3001 queue 11
[3Com] qos cql 1 protocol ip acl 3002 queue 12
```

# Apply the CQ rule in outbound direction of interface Serial 2/0/0.

```
[3Com] interface Serial2/0/0
[3Com1-Serial2/0/0] link-protocol ppp
[3Com1-Serial2/0/0] ip address 10.1.1.1 255.255.255.0
[3Com1-Serial2/0/0] qos cq cql 1
[3Com1-Serial2/0/0] quit
```

3.8.4 CBQ Configuration Example

I. Network requirements

As shown in the network diagram, Router A and Router B are installed with FXS cards and connected to phones. The connection of the two routers is back-to-back and encapsulated with PPP.

Configure VoIP on the routers to have voice packets forwarded from interface Serial 2/0/0 on Router A to Router B. Use the PC attached to Router B as FTP and WWW Client and the PC attached to Router A as FTP and WWW Server. Do the following:

- On the client PC, FTP and HTTP large files from the server attached to Router A at the same time.
- On Router A, place a call to Router B.

The following are expected:

- The quality of voice is not affected by other traffic when the link is congested.
- The ratio of HTTP speed to FTP speed is the same as the ratio of the minimum bandwidth values assigned to them, in the example, 1:2.
- The FTP speed is not less than 64 kbps while the HTTP speed is not less than 32 kbps.

II. Network diagram

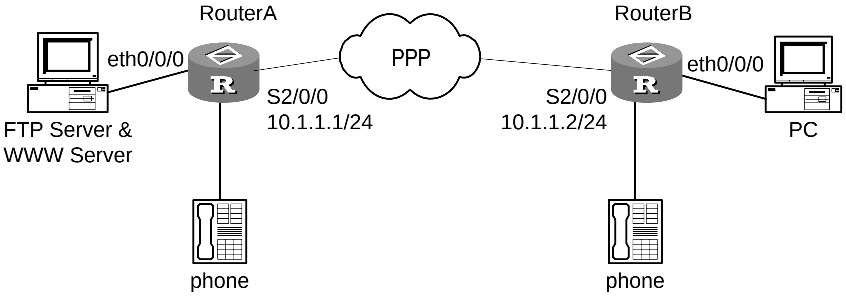


Figure 3-9 Network diagram for CBQ based on class

III. Configuration procedure

1) Configure Router A

# Configure VoIP

```
[3Com] voice-setup
[3Com-voice] dial-program
[3Com-voice-dial] entity 2631 pots
[3Com-voice-dial-entity2631] match-template 2631
[3Com-voice-dial-entity2631] line 1/0/0
[3Com-voice-dial-entity2631] quit
[3Com-voice-dial] entity 3680 voip
[3Com-voice-dial-entity3680] address ip 10.1.1.2
[3Com-voice-dial-entity3680] match-template 3680
[3Com-voice-dial-entity3680] quit
[3Com-voice-dial] quit
[3Com-voice] quit
```

# Configure ACL rules for FTP, HTTP and voice packets.

```
[3Com] acl number 3001 match-order auto
[3Com-acl-adv-3001] rule 0 permit tcp source any source-port eq ftp destination
any
[3Com-acl-adv-3001] rule 1 permit tcp source any source-port eq ftp-data
destination any
[3Com-acl-adv-3001] rule 2 deny ip source any destination any
[3Com-acl-adv-3001] quit
[3Com] acl number 3002 match-order auto
[3Com-acl-adv-3002] rule 0 permit tcp source any source-port eq www destination
any
[3Com-acl-adv-3002] rule 1 deny ip source any destination any
[3Com-acl-adv-3002] quit
[3Com] acl number 3011 match-order auto
[3Com-acl-adv-3011] rule 0 permit udp source any source-port range 16384 32768
destination any destination-port range 16384 32768
[3Com-acl-adv-3011] quit
```

# Configure the ACL rules for classifier matching.

```
[3Com] traffic classifier ftp operator and
[3Com-classifier-ftp] if-match acl 3001
[3Com-classifier-ftp] quit
[3Com] traffic classifier http operator and
[3Com-classifier-http] if-match acl 3002
[3Com-classifier-http] quit
[3Com] traffic classifier voice operator and
[3Com-classifier-voice] if-match acl 3011
[3Com-classifier-voice] quit
```

# Configure behaviors.

```
[3Com] traffic behavior ftp
[3Com-behavior-ftp] queue af bandwidth 64
[3Com-behavior-ftp] quit
[3Com] traffic behavior http
[3Com-behavior-http] queue af bandwidth 32
[3Com-behavior-http] quit
[3Com] traffic behavior voice
[3Com-behavior-voice] queue ef bandwidth 32 cbs 1500
[3Com-behavior-voice] quit
```

# Configure policies, associating classifiers with their respective behaviors: put voice packets in EF queues and FTP and HTTP packets in AF queues. The EF queues have priority over AF queues.

```
[3Com] qos policy CBQ
[3Com-qospolicy-CBQ] classifier ftp behavior ftp
```

```
[3Com-qospolicy-CBQ] classifier http behavior http
[3Com-qospolicy-CBQ] classifier voice behavior voice
[3Com-qospolicy-CBQ] quit
```

In an AF queue, the FTP packets are ensured the minimum bandwidth of 64 kbps and the HTTP packets are ensured the minimum bandwidth of 32 kbps. Voice packets in EF queues have sending priority. They are ensured the maximum bandwidth of 32 kbps.

# Apply the policy in outbound direction of interface serial2/0/0.

```
[3Com] interface Serial2/0/0
[3Com-Serial2/0/0] link-protocol ppp
[3Com-Serial2/0/0] ip address 10.1.1.1 255.255.255.0
[3Com-Serial2/0/0] qos max-bandwidth 2048
[3Com-Serial2/0/0] qos apply policy CBQ outbound
```

3.8.5 Integrated QoS Policy Embedding and LR Configuration Example

I. Network requirements

Figure 3-10 presents a scenario, where:

- Hosts on Network A, PC1 and PC2, need to send data to hosts on Network B. PC1 needs to send network performance monitoring data to UDP port 3000 on Server on Network B in addition.
- On 3Com 1, the rate of incoming interface Ethernet 1/0/0 is 10 Mbps, and the rate of outgoing interface Serial 3/0/0 is 2 Mbps. As the result of this rate discrepancy, congestion may occur on interface Serial 3/0/0.

It is required that:

- When congestion occurs, 256 kbps bandwidth is assured for data transmitted from Network A to Network B.
- The size of network performance monitoring data is limited under CIR rate, 80 kbps. Packets beyond the limit are not dropped directly. Instead, they are sent marked with the lowest preference to the downstream device.
- To ensure smooth transmission, LR does not apply to all data sent from Network A to Network B but network performance monitoring data.

II. Network diagram

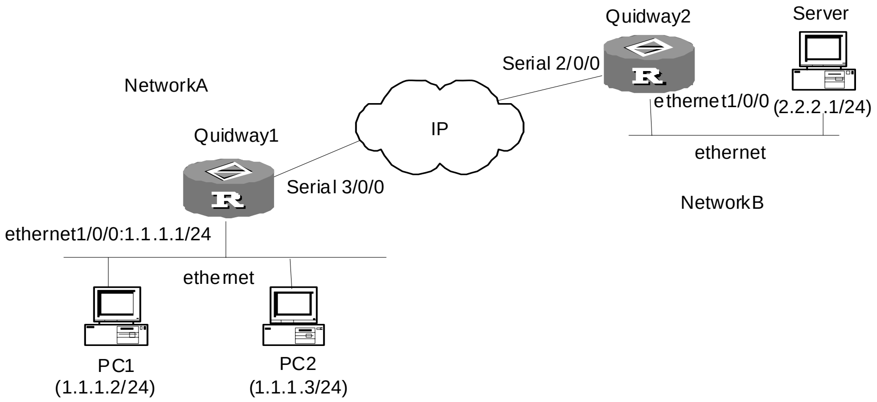


Figure 3-10 Network diagram for QoS policy embedding

III. Configuration procedure

Configure router 3Com 1:

# Configure an ACL for matching data packets sent from Network A to Network B.

```
[3Com1] acl number 3001
[3Com1-acl-adv-3001] rule permit ip source 1.1.1.0 0.0.0.255 destination 2.2.2.0 0.0.0.255
[3Com1-acl-adv-3001] quit
```

# Configure an ACL for matching network performance monitoring data packets sent from Network A to Network B.

```
[3Com1] acl number 3002
[3Com1-acl-adv-3002] rule permit udp source 1.1.1.2 0 destination 2.2.2.1 0 destination-port eq 3000
[3Com1-acl-adv-3002] quit
```

# Configure a traffic class named childclass for network performance monitoring data from PC 1 to Server.

```
[3Com1] traffic classifier childclass
[3Com1-classifier-childclass] if-match acl 3002
[3Com1-classifier-childclass] quit
```

# Configure an LR behavior.

```
[3Com1] traffic behavior childbehav
[3Com1-behavior-childbehav] car cir 80000 cbs 20000 ebs 0 green pass red remark-prec-pass 0
```

```
[3Com1-behavior-childbehav] quit
```

# Configure a child policy, applying the LR behavior to the network performance monitoring class.

```
[3Com1] qos policy childpolicy
[3Com1-qospolicy-childpolicy] classifier childclass behavior childbehav
```

# Configure a traffic class for data from Network A to Network B.

```
[3Com1] traffic classifier parentclass
[3Com1-classifier-parentclass] if-match acl 3001
[3Com1-classifier-parentclass] quit
```

# Configure an AF queuing behavior for data sent from Network A to Network B and embed the child policy in the behavior.

```
[3Com1] traffic behavior parentbehav
[3Com1-behavior-parentbehav] queue af bandwidth 256
[3Com1-behavior-parentbehav] traffic-policy childpolicy
[3Com1-behavior-parentbehav] quit
```

# Configure a parent policy, applying the AF queuing behavior to data sent from Network A to Network B.

```
[3Com1] qos policy parentpolicy
[3Com1-qospolicy-parentpolicy] classifier parentclass behavior parentbehav
[3Com1-qospolicy-parentpolicy] quit
```

# Apply the parent policy to the interface.

```
[3Com1] interface Serial3/0/0
[3Com1-Serial3/0/0] qos apply policy parentpolicy outbound
```

3.8.6 ATM PVC Remark Policy Configuration Example

I. Network requirements

As shown in the following figure, Routers A, B, and C are connected to an ATM network for communication. In this scenario:

- The ATM interfaces of the three routers are assigned IP addresses 202.38.160.1, 202.38.160.2, and 202.38.160.3 respectively.
- In the ATM network, Router A connects to Router B and Router C using the VPI/VCI pairs 0/40 and 0/41 respectively; Router B connects to Router A and Router C using the VPI/VCI pairs 0/50 and 0/51 respectively; Router C connects to Router A and Router B using the VPI/VCI pairs 0/60 and 0/61 respectively.
- IPoA is enabled on the PVCs on the involved ATM interfaces.
- Configure DSCP remark on PVC 0/40 of the outgoing interfaces on Router A.

II. Network diagram

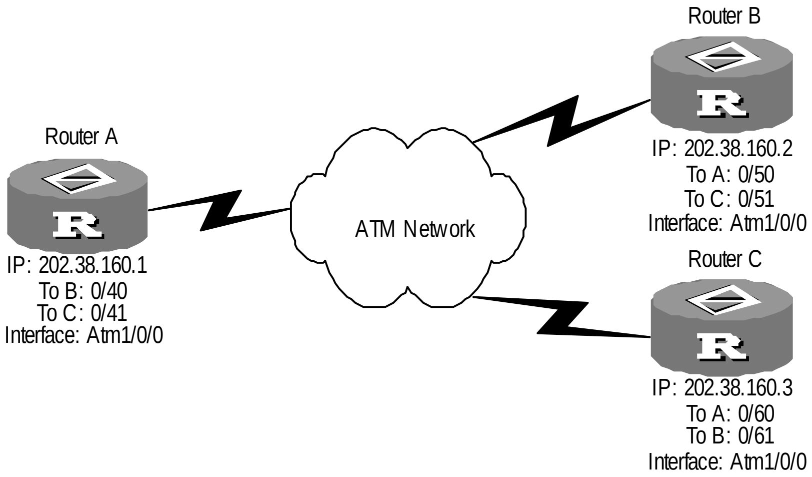


Figure 3-11 Network diagram for ATM PVC remark policy

III. Configuration procedure

1) Configure Router A:

# Enter the interface ATM 1/0/0 and assign an IP address to it.

```
<3Com> system-view
[3Com] interface atm 1/0/0
[3Com-atm1/0/0] ip address 202.38.160.1 255.255.255.0
```

# Create PVCs and run IP on them.

```
[3Com-atm1/0/0] pvc to_b 0/40
[3Com-atm-pvc-atm1/0/0-0/40-to_b] map ip 202.38.160.2
[3Com-atm-pvc-atm1/0/0-0/40-to_b] quit
[3Com-atm1/0/0] pvc to_c 0/41
[3Com-atm-pvc-atm1/0/0-0/41-to_c] map ip 202.38.160.3
[3Com-atm-pvc-atm1/0/0-0/41-to_c] quit
[3Com-atm1/0/0] quit
```

# Configure a matching rule for class 1.

```
[3Com] traffic classifier 1
[3Com-classifier-1] if-match ip-precedence 3
```

# Configure behavior 1.

```
[3Com-classifier-1] traffic behavior 1
[3Com-behavior-1] remark dscp af31
```

# Configure policy 1.

```
[3Com] qos policy 1
[3Com-qospolicy-1] classifier 1 behavior 1
[3Com-qospolicy-1] quit
```

# Apply policy 1 in the outbound direction of the ATM PVC to Router A.

```
[3Com] interface atm 1/0/0
[3Com-atm1/0/0] pvc to_b 0/40
[3Com-atm-pvc-atm1/0/0-0/60-to_a] qos apply policy 1 outbound
```

2) Configure Router B

# Enter the interface ATM 1/0/0 and assign an IP address to it.

```
<3Com> system-view
[3Com] interface atm 1/0/0
[3Com-atm1/0/0] ip address 202.38.160.2 255.255.255.0
```

# Create PVCs and run IP on them.

```
[3Com-atm1/0/0] pvc to_a 0/50
[3Com-atm-pvc-atm1/0/0-0/50-to_a] map ip 202.38.160.1
[3Com-atm-pvc-atm1/0/0-0/50-to_a] quit
[3Com-atm1/0/0] pvc to_c 0/51
[3Com-atm-pvc-atm1/0/0-0/51-to_c] map ip 202.38.160.3
```

3) Configure Router C

# Enter the interface ATM 1/0/0 and assign an IP address to it.

```
<3Com> system-view
[3Com] interface atm 1/0/0
[3Com-atm1/0/0] ip address 202.38.160.3 255.255.255.0
```

# Create PVCs and run IP on them.

```
[3Com-atm1/0/0] pvc to_a 0/60
[3Com-atm-pvc-atm1/0/0-0/60-to_a] map ip 202.38.160.1
[3Com-atm-pvc-atm1/0/0-0/60-to_a] quit
[3Com-atm1/0/0] pvc to_b 0/61
[3Com-atm-pvc-atm1/0/0-0/61-to_b] map ip 202.38.160.2
```

Router A remarks DSCP values of packets on its outbound interface, then the subsequent router performs functions like filtering, maximum bandwith restriction on those packets according to their DSCP values.

3.8.7 Congestion Management Using ATM CLP Bit Configuration Example

I. Network requirements

Router A and Router B are connected through an ATM network and running IPoA.

On Router A, do the following:

1) Configure a policy allowing the router to remark the ATM CLP bit to 1 for packets with IP precedence of 0.
2) Apply the policy to the outbound direction of interface atm 1/0/0.

On Router B, do the following:

1) Configure a policy allowing the router to remark IP precedence to 1 for packets with ATM CLP bit set to 1.
2) Apply the policy to the outbound direction of interface serial 0/0/0.

When congestion occurs on the ATM network, packets with CLP bit set to 1 are dropped first.

II. Network diagram

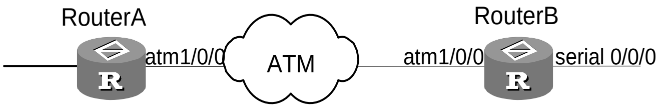


Figure 3-12 Network diagram for congestion management using ATM CLP bit

III. Configuration procedure

1) Configure Router A

# Configure QoS policy poll.

```
[RouterA] traffic classifier class1
[RouterA-classifier-class1] if-match ip-precedence 0
[RouterA-classifier-class1] traffic behavior database1
[RouterA-behavior-database] remark atm-clp 1
[RouterA-behavior-database] quit
[RouterA] qos policy pol1
[RouterA-qospolicy-poll] classifier class1 behavior database1
[RouterA-qospolicy-poll] quit
```

# Apply the policy to the outbound direction of interface atm 1/0/0.

```
[RouterA] interface atm1/0/0
[RouterA-Atm1/0/0] ip address 192.168.11.5 24
[RouterA-Atm1/0/0] pvc 2 0/40
[RouterA-atm-pvc-Atm1/0/0-0/40-2] map ip 192.168.11.6
[RouterA-atm-pvc-Atm1/0/0-0/40-2] qos apply policy pol1 outbound
[RouterA-atm-pvc-Atm1/0/0-0/40-2] quit
[RouterA-Atm1/0/0] quit
```

2) Configure Router B

# Configure interface atm 1/0/0.

```
[RouterB] interface atm1/0/0
[RouterB-Atm1/0/0] ip address 192.168.11.5 24
[RouterB-Atm1/0/0] pvc 2 0/40
[RouterB-atm-pvc-Atm1/0/0-0/40-2] map ip 192.168.11.6
[RouterB-atm-pvc-Atm1/0/0-0/40-2] quit
[RouterB-Atm1/0/0] quit
```

# Configure QoS policy poll.

```
[RouterB] traffic classifier class1
[RouterB-classifier-class1] if-match atmclp
[RouterB-classifier-class1] traffic behavior database1
[RouterB-behavior-database] remark ip-precedence 1
[RouterB-behavior-database] quit
[RouterB] qos policy pol1
[RouterB-qospolicy-poll] classifier class1 behavior database1
[RouterB-qospolicy-poll] quit
```

# Apply the policy to the outbound direction of interface serial 0/0/0.

```
[RouterB] interface serial0/0/0
[RouterB-atm-pvc-Atm1/0/0-0/40-2] qos apply policy pol1 outbound
```

3) Display the configuration

# When Router A has traffic destined for Router B, execute the following command on it to verify configuration information.

```
[RouterA] display qos policy interface outbound
Atm1/0/0, pvc 2 0/40
  Direction: Outbound
  Policy: poll
   Classifier: default-class
     Matched : 10/890 (Packets/Bytes)
     Rule(s) : if-match any
     Behavior:
      -none-

   Classifier: class1
     Matched : 20/1840 (Packets/Bytes)
     Operator: AND
     Rule(s) : if-match ip-precedence 0
     Behavior:
      Marking:
        Remark ATM CLP 1
        Remarked: 20 (Packets)
```

The output indicates that the CLP bit of 20 ATM packets was set. In case congestion occurs on the ATM network, these packets would be dropped first.

# On Router B, execute the following command to verify configuration information.

```
[RouterB] display qos policy interface outbound
Interface: Serial0/0/0


  Direction: Outbound
  Policy: pol1

   Classifier: default-class
     Matched : 10/890 (Packets/Bytes)
     Rule(s) : if-match any
     Behavior: be
      -none-

   Classifier: class1
     Matched : 20/1840 (Packets/Bytes)
     Operator: AND
     Rule(s) : if-match inbound interface Ethernet0/0
               if-match dscp 1 6 9
               if-match atmclp
     Behavior: database1
      Marking:
        Remark IP Precedence 1
        Remarked: 20 (Packets)
```

The ATM network had no congestion, the IP precedence of above-mentioned 20 ATM packets was set to 1.

Chapter 4 Congestion Avoidance

4.1 Introduction to Congestion Avoidance

Excessive congestion can endanger network resources greatly, so some avoidance measures must be taken. The Congestion Avoidance refers to a traffic control mechanism that can monitor the occupancy status of network resources (such as the queues or buffer). As congestion becomes worse, the system actively drops packets and tries to avoid the network overload through adjusting the network traffics.

Comparing with the end-to-end traffic control, this traffic control has broader significance, which affects more loads of application streams through router. Of course, while dropping packets, the router may cooperate with traffic control action on the source end, such as TCP traffic control to adjust the network's traffic to a reasonable load level. A good combination of packet-dropping policy with traffic control mechanism at the source end will always try to maximize the throughput and utilization of network and minimize the packet dropping and delay.

I. Traditional packet-dropping policy

Traditional policy of dropping packets adopts the Tail-Drop method. When the amount of packets in a queue reaches a certain maximum value, all new arrived packets will be dropped.

This kind of dropping policy will lead to phenomenon of TCP synchronization - when queues drop packets of several TCP connections at the same time, it will lead these TCP connections to enter congestion avoidance and slow start status to adjust traffics simultaneously, then reach a high peak of traffics simultaneously. In this way, Network traffic keeps saw-teeth pattern. This causes frequent sudden rises and decreases of bandwidth utilization ratio, lowering the bandwidth utilization efficiency.

II. RED and WRED

To avoid the phenomenon of TCP synchronization, RED (Random Early Detection) or WRED (Weighted Random Early Detection) can be used.

In RED algorithm, it sets minimum and maximum thresholds for each queue.

- When the length of queue is less than the minimum limitation, no packet will be dropped.
- When the length of queue exceeds the maximum limitation, all the incoming packets will be dropped.
- When the length of queue between low and high limitations, the packet will be dropped randomly. The method is to give a random number to every new packet, and then compare it with packet dropping probability of the current queue. If the

random number is larger than the latter, the packet will be dropped. The longer the length of queue, the higher the dropping probability is, but a maximum dropping probability will remain.

Unlike RED, the random number of WRED generated is based on priority. It uses IP precedence to determine the dropping policy thus the dropping probability of packets with high priority will relatively decrease.

RED and WRED employ the random packet dropping policy to avoid TCP synchronization - when packet of one TCP connection is dropped with a decreased sending rate, other TCP connections will still keep higher sending rate. So there are always some TCP connections, which have a higher sending rate to realize more efficient network bandwidth utilization.

To drop the packets through comparing the length of the queue with the high/low limitations (set the absolute length of queue threshold) will treat the bursting data stream unfairly and influence the transmission of data stream. So here we can use the average queue length (Set the relative comparison value with queue threshold and average length).

The equation used by WRED to calculate the avarage queue length is as follows:

Average queue length = (Average queue length in the past x $(1 – 1/2^n)$) + (Current queue length x $(1/2^n)$), where n is the weight factor, a configurable parameter.

The average length of queue reflects the changing of queue and is insensitive to bursting change of queue length, preventing the unfair treatment for the bursting data stream.

When WFQ is adopted, you can set weight factor, minimum threshold, maximum threshold and packet-dropping possibility for different queues that has different priority/DSCP packet. So packet with different priority will have different packet dropping characters.

The relation between WRED and Queue mechanism is shown as in the following figure.

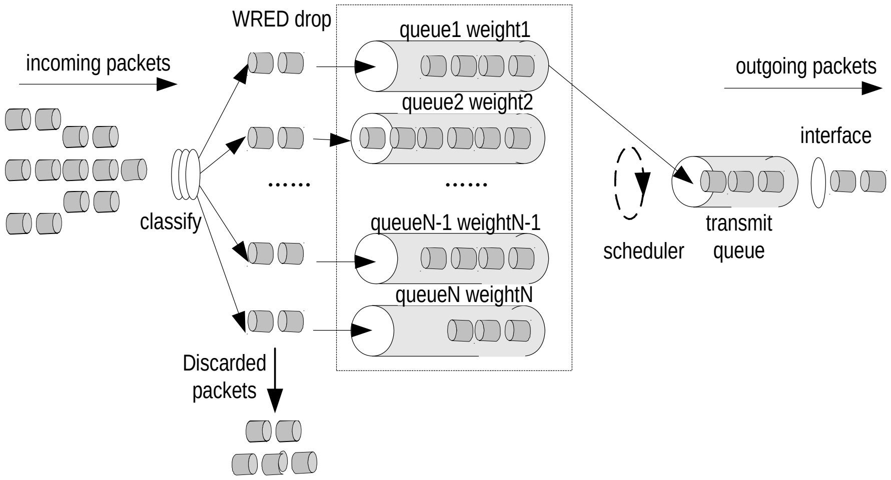


Figure 4-1 Relation between WRED and Queue mechanism

Associating WRED with WFQ, the flow-based WRED can be realized. Because different flow has its own queue during packet classification, the flow with small traffic always has a short queue length, so the packet dropping probability will be small. The flow with high traffic will have the longer queue length and will drop more packets, so we can protect the benefits of the flow with small traffic.

4.2 WRED Configuration

WRED configuration includes:

- Enable WRED
- Set WRED exponent for mean queue length calculation
- Set WRED parameters for each precedence

4.2.1 Enabling WRED

Perform the following configuration in interface view.

Table 4-1 Enable WRED

Operation	Command
Enable WRED	**qos wred**
Restore default	**undo qos wred**

WRED cannot be used independently or with the queuing methods but WFQ.

By default, WRED is not used and the dropping method is tail drop.

Note:

Make sure WFQ has already been applied on the interface before enabling WRED.

4.2.2 Setting WRED to Calculate the Coefficient of Average Queue Length

Set WRED to calculate the filter coefficient of the average queue length.

Perform the following configuration in interface view

Table 4-2 Set WRED exponent for mean queue depth calculation

Operation	Command
Set WRED exponent for mean queue depth calculation	**qos wred weighting-constant** *exponent*
Recover the default value of exponent	**undo qos wred weighting-constant**

The *exponent* is the filter coefficient to calculate the average queue length, ranging from 1 to 16, with the default set as 9.

You must use **qos wred** command first on the interface before applying WRED, and then set the parameter of WRED.

4.2.3 Setting WRED Priorities

When WFQ (Weighted Fair Queuing) is configured on an inerface, you can set minimum/maximum threshold and drop probability denominator of the each precedence of WRED.

Perform the following configuration in interface view.

Table 4-3 Set WRED parameters for each precedence

Operation	Command
Set WRED parameters for each precedence	**qos wred ip-precedence** *ip-precedence* **low-limit** *low-limit* **high-limit** *high-limit* **discard-probability** *discard-prob*
To restore the default value of precedence	**undo qos wred ip-precedence** *ip-precedence*

You must use **qos wred** command first on the interface before applying WRED, and then set the WRED parameter.

4.2.4 Setting the Parameters of a WRED DSCP

When an interface is configured with WRED, you can set the lower limit, upper limit, and drop probability denominator of a WRED DSCP.

Perform the following configuration in interface view.

Table 4-4 Set the parameters of a WRED DSCP

Operation	Command
Set the parameters of a WRED DSCP	**qos wred dscp** *dscp-value* **low-limit** *low-limit* **high-limit** *high-limit* **discard-probability** *discard-prob*
Restore the default settings of a WRED DSCP	**undo qos wred dscp** *dscp-value*

Before configuring the WRED parameters, you must use the **qos wred** command to apply the WRED to an interface.

4.3 WRED Display and Debug

After the above configuration, execute **display** command in any view to display the running of the WRED configuration, and to verify the effect of the configuration.

Table 4-5 Display WRED configuration and statistics information on the interface

Operation	Command
Display WRED configuration and statistics information on the interface	**display qos wred interface** [*interface-type interface-number*]

This command can show WRED configuration and statistics information on one or all interfaces

Chapter 5 Protocol Packet Priority Configuration

5.1 Introduction to IP Packet Priority

Protocol packets carry their priorities themselves. You can however assign them new priorities. By associating these priorities with QoS actions, you can provide protocol packets different QoS services.

Two types of priorities are available with IP packets: IP precedence and DSCP.

I. IP precedence

IP precedence is the first three bits in the ToS field of the IP header. These three bits can specify eight service classes, as shown in the following table.

Table 5-1 IP precedence levels

IP precedence level	IP precedence bits	Description
0	000	Routine
1	001	Priority
2	010	Immediate
3	011	Flash
4	100	Flash-override
5	101	Critical
6	110	Internet
7	111	Network

The internet and network levels are only intended for use within a network only.

On an access network, traffic is usually classified by the combination of IP precedence and IP quintuple. Different traffic streams are offered appropriate QoS according to the traffic behaviors configured on each node.

II. DSCP

Differentiated Services (DiffServ) model defines the six most significant bits in the IP DS (also known as ToS) field as DSCP. The first three bits of DSCP are for class selector, the fourth and fifth bits are for drop priorities, and the sixth bit is set to 0 meaning the current device sets service classes based on DS model.

With DiffServ networks, traffic is sorted into the following four per-hop-behavior (PHB) groups:

- Expedited forwarding (EF) that does not consider whether the link is shared by other traffic streams. It is suitable for priority services requiring low latency, low loss ratio, small jitter, and assured bandwidth. One example is virtual leased lines.
- Assured forwarding (AF). It is subdivided into four classes, AFs 1 through 4, each having three drop precedence levels allowing for further AF service discrimination. The QoS level of AF is lower than EF.
- Class selector (CS) compatible with IP precedence. It evolved from the IP ToS field and has eight classes.
- Best effort (BE) is a special case of CS; it provides no guarantee. AF traffic could be assigned to BE once exceeding the specified limit. All IP traffic is assigned to the BE PHB group by default.

The following table gives the possible DSCP values.

Table 5-2 DSCP values

Keyword	DSCP value (binary)	DSCP value (decimal)
ef	101110	46
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22
af31	011010	26
af32	011100	28
af33	011110	30
af41	100010	34
af42	100100	36
af43	100110	38
cs1	001000	8
cs2	010000	16
cs3	011000	24
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56

Keyword	DSCP value (binary)	DSCP value (decimal)
default (be)	000000	0

The following table gives the drop precedence values for AF classes.

Table 5-3 Drop precedence values for AF classes

Drop precedence	AF1 class	AF2 class	AF3 class	AF4 class
Low	001010	010010	011010	100010
Medium	001100	010100	011100	100100
High	001110	010110	011110	100110

The following table gives the IP precedence-DSCP map.

Table 5-4 IP precedence-DSCP map

IP precedence	DSCP class
5	EF
4	AF4
3	AF3
2	AF2
1	AF1
0	BE

On a distribution network, traffic is usually classified by the combination of DSCP and IP quintuple. Different traffic streams are offered appropriate QoS according to the traffic behaviors configured on each node.

5.2 Configuring Priorities for Protocol Packets

You may change priorities of protocol packets generated by current host.

Perform the following configuration in system view.

Table 5-5 Configure a priority for a type of protocol packets

Operation	Command
Configure a priority for the packets of the specified protocol	**protocol-priority protocol-type** *protocol-type* { **ip-precedence** *ip-precedence* **|** **dscp** *dscp-value* }

Operation	Command
Restore the default	**undo protocol-priority protocol-type** *protocol-type*

Caution:

Currently, you can only change priorities of six types of protocol packets: OSPF, Telnet, SNMP, ICMP, BGP, and LDP. In addition, this command is only valid for protocol packets generated by this host.

5.3 Protocol Packet Priority Configuration Example

I. Network requirements

Change the IP precedence of OSPF packets to 3.

II. Configuration procedure

# Set the IP precedence of OSPF packets to 3.

```
<3Com> system-view
[3Com] protocol-priority protocol-type ospf ip-precedence 3
```

# Display priorities of protocol packets.

```
[3Com] display protocol-priority

Protocol: ospf

  IP-Precedence: flash(3)
```

Chapter 6 MPLS QoS

6.1 MPLS QoS Overview

The QoS solution for MPLS mainly completes the following functions:

Classify the service traffic on CE or PE according to specific needs, for example, into three types: voice, video and data.

When PE adds a Label to the packet, it will map the IP precedence flag carried by the IP packet to the CoS domain of the flag, and thus the class information carried by IP is carried by the flag now.

Among the PE routers, the differentiated dispatching (such as PQ, WFQ, and CBQ) is performed, that is, transmit the service traffic with flag on a LSP in the mode of differentiated QoS.

🕮 **Note:**

To understand the contents in this chapter, you should have some background knowledge related to MPLS. Refer to “MPLS Configuration” in this manual for the description of MPLS basic concepts and related configurations. This chapter only involves MPLS QoS configuration.

6.2 MPLS QoS Configuration

To configure MPLS QoS, you should first perform the related configuration of MPLS and specify to display the route forwarding mode. For detailed configurations of MPLS, refer to “MPLS Configuration” in this manual. This chapter only describes MPLS QoS configuration.

MPLS QoS configuration includes:

- MPLS PQ
- MPLS CQ
- MPLS CBQ
- MPLS CAR

The following describes the method of configuration for each of the above in detail.

6.2.1 Configuring MPLS PQ

Complete these two steps to configure MPLS PQ: First, configure priority list according to MPLS EXP. Second, apply the priority list on the interface. For more information, refer to PQ Configuration in Congestion Management.

I. Configuring Priority List according to MPLS EXP

Classify the packets according to MPLS EXP value and enable them to enter different queues.

Perform the following configurations in system view.

Table 6-1 Configure priority list according to network protocol

Operation	Command
Configure priority list according to network protocol	**qos pql** *pql-index* **protocol mpls exp** { *mpls-experimental-value* } **queue** { **top** | **middle** | **normal** | **bottom** }
Delete corresponding classification rule of a specified group	**undo qos pql** *pql-index* **protocol mpls exp** *mpls-experimental-value*

For PQ configurations, refer back to the subsection “PQ (Priority Queuing)” in the section “Congestion Management Policies”.

II. Applying PLQ on the Interface

Apply a group of priority-lists on the interface; to use this command repeatedly will set a new priority-list for the same interface.

Perform the following configuration under interface view.

Table 6-2 Apply priority-list group on the interface

Operation	Command
Apply priority-list group on the interface	**qos pq pql** *pql-index*
Cancel PQ setting on the interface	**undo qos pq**

Not PQ but FIFO is employed on the interface by default.

6.2.2 Configuring MPLS CQ

Complete these two steps to configure MPLS CQ: First, configure priority list according to MPLS EXP. Second, apply the priority list on the interface. For more information, refer to CQ Configuration in Congestion Management.

I. Configuring custom-list according to MPLS EXP

Configure custom-list according to MPLS EXP and enable packets to enter different queues.

Perform the following configurations in system view.

Table 6-3 Configure custom-list according to network protocol

Operation	Command
Configure custom-list according to MPLS EXP	**qos cql** *cql-index* **protocol mpls exp** *experimental-number* **queue** *queue-number*
Delete the corresponding classification rule	**undo qos cql** *cql-index* **protocol mpls exp** *experimental-number*

For PQ configurations, refer back to the subsection “CQ (Custom Queuing)” in the section “Congestion Management Policies”.

II. Applying custom-list on the Interface

Perform the following configuration in interface view.

Table 6-4 Apply custom-list on the interface

Operation	Command
Apply Custom-list on the interface	**qos cq cql** *cql-index*
Cancel CQ setting on the interface	**undo qos cq**

Not CQ but FIFO is employed on the interface by default.

6.2.3 Configuring MPLS CBQ

Complete these four steps to configure MPLS CBQ: First, define CBQ classes and configure matching rule according to the MPLS EXP. Second, define traffic behaviors and configure processing scheme of MPLS EXP domain. Third, define a QoS policy and specify specific traffic behavior for CBQ classes. Forth, apply QoS policy on the interface. For more information, refer to PQ Configuration in Congestion Management.

I. Defining/deleting exp domain rule of packets matching MPLS

MPLS QoS allows users to set MPLS EXP domain on PE to classify MPLS packets and make them enter different queues to implement QoS. In this case, IP packets can travel through MPLS network transparently without change.

Firstly you should define a CBQ class with a certain class name, and then enter this class view to configure the classification regulation by EXP value in MPLS label field.

Perform the following configurations in system view.

Table 6-5 Define a class and enter the class view

Operation	Command
Define a class and enter the class view	**traffic classifier** *tcl-name* [**operator** { **and | or** }]
Delete a class	**undo traffic classifier** *tcl-name* [**operator** { **and | or** }]

Perform the following configurations in class view.

Table 6-6 Define/delete EXP domain rule of packets matched MPLS

Operation	Command
Define exp domain rule matching MPLS	**if-match** [**not**] **mpls-exp** { *mpls-experimental-value* }
Delete exp domain rule matching MPLS	**undo if-match** [**not**] **mpls-exp**

II. Setting the value of MPLS EXP domain

Configure the value of MPLS EXP domain and associate the class with the behavior in the policy view. Then, the packets matching the class can be MPLS EXP domain-labeled.

To define a traffic behavior, you should first create a traffic behavior name and then configure attributes in the new traffic behavior name.

Perform the following configurations in system view.

Table 6-7 Define a traffic behavior and enter traffic behavior view.

Operation	Command
Define a traffic behavior and enter traffic behavior view.	**traffic behavior** *behavior-name*
Delete a traffic behavior	**undo traffic behavior** *behavior-name*

Perform the following configurations in traffic behavior view.

Table 6-8 Set the value of the MPLS EXP domain to identify a matched packet

Operation	Command
Set the value of the MPLS EXP domain to identify a matched packet	**remark mpls-exp** *mpls-experimental-value*
Delete the setting of the value of the MPLS EXP domain	**undo remark mpls-exp**

III. Configuring policy

Firstly you should define a policy with a certain policy name and then enter the policy view to specify the behavior for the class defined.

Perform the following configurations in the system view.

Table 6-9 Define the policy and enter the policy view

Operation	Command
Define the policy and enter the policy view	**qos policy** *policy-name*
Delete the specified policy	**undo qos policy** *policy-name*

Perform the following configurations in the policy view.

Table 6-10 Specify the traffic behavior for the class in the policy

Operation	Command
Specify the traffic behavior for the class in the policy	**classifier** *tcl-name* **behavior** *behavior-name*
Remove the application of the specified class in the policy	**undo classifier** *tcl-name*

IV. Applying policy

Perform the following configuration in interface or ATM PVC view.

Table 6-11 Apply a policy to the interface or ATM PVC

Operation	Command
Apply a policy to the interface or ATM PVC	**qos apply policy** *policy-name* { **inbound** | **outbound** }
Remove the application of the policy on the interface or ATM PVC	**undo qos apply policy** { **inbound** | **outbound** }

6.2.4 Configuring MPLS CAR

Complete these two steps to configure MPLS CAR: First, determine supervision targets (what kinds of packets). Second, define supervision policy. You can choose access control list (ACL) or TP list (carl-index) in the first step or just select the **any** keyword to supervise all packets. For more details, refer to Traffic Supervision Configuration.

I. Applying TP policy on the interface and labeling MPLS packets

Apply TP policy (CAR) on the interface and label MPLS packets.

Perform the following configurations in interface view.

Table 6-12 Apply TP policy on the interface and label MPLS packets

Operation	Command
Apply TP policy on the interface and label MPLS packets	**qos car inbound** { **any** | **acl** *acl-number* | **carl** *carl-index* } **cir** *committed--information-rate* **cbs** *committed-burst-size* **ebs** *excess-burst-size* **green** *action* **red** *action*
Remove the application of TP policy on the interface and disable labeling of MPLS packets	**undo qos car inbound** { **any** | **acl** *acl-number* | **carl** *carl-index* } **cir** *committed-information-rate* **cbs** *committed-burst-size* **ebs** *excess-burst-size*

action can be

- **remark-mpls-exp-continue** *new-mpls-exp*: Configures the new MPLS EXP value, *new-mpls-exp*, and continue to be processed by the next CAR policy, ranging from 0 to 7.
- **remark-mpls-exp-pass** *new-mpls-exp*: Configures the new MPLS EXP value, *new-mpls-exp,* and send the packet to the destination, ranging from 0 to 7.

EXP domain of the MPLS packet can only be set on the inbound interface of the PE. If in the input direction is IP packet, but is encapsulated as MPLS packet in the output direction, the configured TP policy has taken effect.

When setting the EXP domain of the MPLS packet, two layers of labels shall be set and ToS domain in the IP header shall not be modified.

6.3 MPLS QoS Configuration Example

6.3.1 QoS Configuration for Streams in the Same VPN

I. Network requirements

In the network diagram, CE1 and CE2 belong to VPN1; the bandwidth of the PE1-P link and P-PE2 link is 2M. Define different QoS guarantee levels for the streams with different priority levels in the VPN1.

The configuration in this example includes these two parts:

First, configure MPLS VPN on the CE1, PE1, P, PE2 and CE2.

- Run OSPF between PE1, P and PE2
- Create MP-EBGP neighbors between PE and CE
- Create MP-IBGP neighbors between PEs

Second, configure MPLS QoS on the PE1 and P.

- Configure QoS policy on the ingress interface Ethernet1/1/0 on the PE1 and set EXP domain value according to the DSCP attribute of MPLS packets.

- On the Router P, identify streams according to their EXP domain value and configure stream-specific CBQs: EXP1 streams with 10% bandwidth, EXP2 streams with 20% bandwidth, EXP3 streams with 30% bandwidth and EXP4 streams with 40% bandwidth; delay guarantee is available for EXP4 streams.

Note:

Only MPLS QoS configuration is mentioned here. For MPLS VPN configuration, see MPLS Configuration of this manual.

II. Network diagram

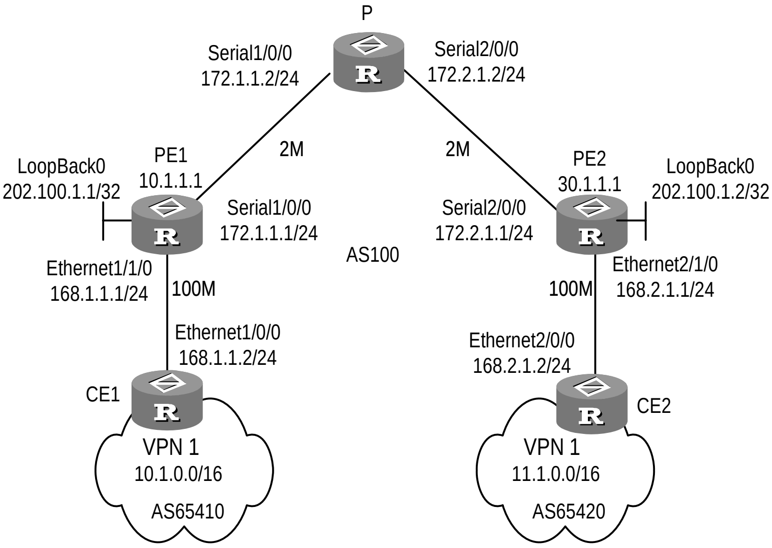


Figure 6-1 Network diagram for MPLS QoS configuration

III. Configuration procedure

- Configure PE1

# Define four classes, match them respectively with the MPLS packets with DSCP being AF11, AF21, AF31 and EF in the same VPN.

```
[PE1] traffic classifier af11
[PE1-classifier-af11] if-match dscp af11
[PE1-classifier-af11] traffic classifier af21
[PE1-classifier-af21] if-match dscp af21
[PE1-classifier-af21] traffic classifier af31
[PE1-classifier-af31] if-match dscp af31
[PE1-classifier-af31] traffic classifier efclass
[PE1-classifier-efclass] if-match dscp ef
```

```
[PE1-classifier-efclass] quit
```

# Define four traffic behaviors and configure EXP domain value for their MPLS packets.

```
[PE1] traffic behavior exp1
[PE1-behavior-exp1] remark mpls-exp 1
[PE1-behavior-exp1] traffic behavior exp2
[PE1-behavior-exp2] remark mpls-exp 2
[PE1-behavior-exp2] traffic behavior exp3
[PE1-behavior-exp3] remark mpls-exp 3
[PE1-behavior-exp3] traffic behavior exp4
[PE1-behavior-exp4] remark mpls-exp 4
[PE1-behavior-exp4] quit
```

# Define QoS policy to specify traffic behaviors to different packet types, that is to label different EXP values for different packet types.

```
[PE1] qos policy REMARK
[PE1-qospolicy-REMARK] classifier af11 behavior exp1
[PE1-qospolicy-REMARK] classifier af21 behavior exp2
[PE1-qospolicy-REMARK] classifier af31 behavior exp3
[PE1-qospolicy-REMARK] classifier efclass behavior exp4
[PE1-qospolicy-REMARK] quit
```

# Apply the QoS policy on the ingress interface of PE1.

```
[PE1] interface ethernet 1/1/0
[PE1-Ethernet1/1/0] qos apply policy REMARK inbound
[PE1-Ethernet1/1/0] quit
```

- Configure Router P

# Define four classes, match them respectively with the MPLS packets with EXP values being1, 2, 3 and 4.

```
[P] traffic classifier EXP1
[P-classifier-EXP1] if-match mpls-exp 1
[P-classifier-EXP1] traffic classifier EXP2
[P-classifier-EXP2] if-match mpls-exp 2
[P-classifier-EXP2] traffic classifier EXP3
[P-classifier-EXP3] if-match mpls-exp 3
[P-classifier-EXP3] traffic classifier EXP4
[P-classifier-EXP4] if-match mpls-exp 4
[P-classifier-EXP4] quit
```

# Define traffic behaviors and configure different bandwidth and delay levels for them.

```
[P] traffic behavior AF11
[P-behavior-AF11] queue af bandwidth pct 10
[P-behavior-AF11] traffic behavior AF21
[P-behavior-AF21] queue af bandwidth pct 20
```

```
[P-behavior-AF21] traffic behavior AF31
[P-behavior-AF31] queue af bandwidth pct 30
[P-behavior-AF31] traffic behavior EF
[P-behavior-EF] queue ef bandwidth pct 40
[P-behavior-EF] quit
```

# Define a QoS policy satisfying this requirement: EXP1 streams with 10% bandwidth, EXP2 streams with 20% bandwidth, EXP3 streams with 30% bandwidth and EXP4 streams with 40% bandwidth; delay guarantee is available for EXP4 streams.

```
[P] qos policy QUEUE
[P-qospolicy-QUEUE] classifier EXP1 behavior AF11
[P-qospolicy-QUEUE] classifier EXP2 behavior AF21
[P-qospolicy-QUEUE] classifier EXP3 behavior AF31
[P-qospolicy-QUEUE] classifier EXP4 behavior EF
[P-qospolicy-QUEUE] quit
```

# Apply the QoS policy on the outbound direction of the interface Serial2/0/0.

```
[P] interface serial 2/0/0
[P-Serial2/0/0] qos apply policy QUEUE outbound
```

Then when network congestion happens to VPN1, the streams of af11, af21, af31 and ef are received in a proportion of 1:2:3:4, while the delay for ef streams is less than the rest three types.

Reliability

Table of Contents

Chapter 1 Reliability Overview

1.1 Introduction to Reliability

During communication, any software or hardware error, network device or line fault for example, may disrupt the connection, causing transmission failure. To avoid these situations, V 2.41 provides backup center, virtual router redundancy protocol (VRRP) and hot backup technologies to ensure availability of a backup scheme when faults occur. This guarantees smooth communication, and makes the network more robust and reliable.

The backup center provides sound backup functions for the communication lines between routers. By assigning backup interfaces to an interface and tuning parameters such as priority and switchover delay of the backup interfaces, you can have the backup interfaces assume the work of the failed main interface before the ongoing service is affected. This significantly improves reliability of the lines. In V 2.41, a main interface can be a physical interface, subinterface or logical channel (such as an X.25 virtual circuit) on an interface; its backups can be dialer-route logical channels or physical interfaces.

VRRP improves reliability of connections to the outside networks and as such, is well suited to multicast or broadcast LANs such as Ethernet. Multiple routers can form a standby group or a virtual router, acting as the only egress gateway for the local network. These routers, however, are transparent to the local network. In the standby group, a router is engaged in packet forwarding, a backup router is ready for replacing the active router, and the other routers are listening. In case the active router fails, the backup router would take over and the other routers would elect among them a new backup router. This improves reliability, allowing the local hosts to continue their operation without any modification.

V 2.41 provides high-end devices with the hot backup mechanism. Usually, a high-end device achieves redundancy by using two main processing units (MPUs). When the active MPU fails, traffic automatically switches over to the slave MPU. In addition, hot backup allows in-service software upgrade, ensuring normal operation of the services.

Chapter 2 Backup Center Configurations

2.1 Introduction to Backup Center

To enhance network reliability, V 2.41 provides sound backup functions using the backup center.

- Interfaces that are backed up are main interfaces. They can be WAN interfaces, logical interfaces (including virtual template and dialer, but not MFR), or subinterfaces.
- Interfaces that provide backup to other interfaces are backup interfaces. They can be any physical interfaces, logical channels, or logical interfaces such as those created using the **dialer route logical-channel** *logic-channel-number* command, dialer interfaces, and virtual template interfaces on the router.
- For a main interface, you can configure multiple backup interfaces. In case the main interface fails, the order in which they are used depends on interface priority. If two backup interfaces with the same priority are available, the one configured first is selected.
- For interfaces that have multiple physical channels, ISDN BRI and ISDN PRI interfaces for example, you can use the logical interfaces created using the **dialer route logical-channel** *logic-channel-number* command to provide backup to multiple main interfaces.
- Backup center supports backup load sharing. When traffic on the main interface reaches the enable-threshold, the router brings up the backup interface with the highest priority among the available backup interfaces to share load together with the main interface. When traffic on the main interface is less than the disable-threshold, the router closes the backup interface with the lowest priority. This approach to load sharing is not preferred however, because it can result in loss of the packets sent to the backup interface that is shut down.
- The IMA-group interface cannot participate in interface backup.

2.2 Backup Center Configurations

The basic backup center configuration tasks are described in the following sections:

- Entering the View of a Main Interface
- Assigning Backup Interfaces with Priorities to the Main Interface
- Setting Failover and Fallback Delay
- Configuring Routes on the Main and Backup Interfaces

The advanced backup center configuration tasks are described in the following sections:

- Configuring the Warmup Timer
- Configuring Backup Load Sharing
- Setting Backup Bandwidth of the Main Interface
- Configuring Flow Check Interval

2.2.1 Entering the View of a Main Interface

On a device operating based on the V 2.41 platform, all physical interfaces or subinterfaces can be main interfaces. Before you can back up an interface, you must enter its view first.

Perform the following configuration in system view.

Table 2-1 Enter the view of a main interface

Operation	Command
Enter the view of a main interface.	**interface** *type number*

2.2.2 Assigning Backup Interfaces with Priorities to the Main Interface

Backup interfaces to the main interface can be physical interfaces or logical channels/interfaces such as those created using the **dialer route logical-channel** *logic-channel-number* command, dialer or virtual template interfaces.

Perform the following configuration in the view of the main interface.

Table 2-2 Assign a backup interface with a priority to the main interface

Operation	Command
Assign a backup interface with a priority to the main interface.	**standby interface** *type number* [*priority*]
Delete a backup interface of the main interface.	**undo standby interface** *type number*

The *priority* argument defaults to 0.

You can assign up to three backup interfaces to a main interface. The maximum number of main interfaces that the backup center can accommodate is 10. If two backup interfaces with the same priority are available, the one configured first would be selected in case the main interface goes down.

To use a logical channel created using the **dialer route logical-channel** command on a dial-up interface for backup, you must first create a logical channel interface, and then associate the logical channel interface with the logical channel by using the **dialer route logical-channel** command on the dial-up interface.

Perform the following configuration in the system view.

Table 2-3 Create a logical channel

Operation	Command
Create a logical channel (in system view)	**interface logic-channel** *logic-channel-numbe*r
Associate the created logical channel interface with the dialer-route logical channel (in physical dialer interface view)	**dialer route** *protocol next-hop-address* [**user** *hostname*] [**broadcast**] [*dial-number*] [**auto-dial**] **logical-channel** *logic-channel-number*

2.2.3 Setting Failover and Fallback Delays

You may set a failover delay on the main interface. After that, failover does not take place immediately after the main interface goes down. Instead, the backup interface takes over only if the main interface remains down upon expiry of the delay. If the main interface goes up before that, failover does not take place.

Before you can use this command, you must configure the **standby interface** command.

Perform the following configuration in the view of the main interface.

Table 2-4 Set failover and fallback delays

Operation	Command
Set failover and fallback delays.	**standby timer delay** *enable-delay disable-delay*
Restore the default failover delay.	**undo standby timer delay**

The *enable-delay* argument specifies the failover delay in the range 0 to 65535 seconds. It defaults to 0, meaning failover without delay.

The *disable-delay* argument specifies the fallback delay in the range 0 to 65535 seconds. It defaults to 0, meaning fallback without delay.

2.2.4 Configuring Routes on the Main and Backup Interfaces

You can use the **ip route-static** command in system view to configure the routes through the main interface and all its backup interfaces to the destination network segment. For detailed description on the **ip route-static** command, refer to the "Routing Protocol" part of this manual.

2.2.5 Configuring the Warmup Timer

Normally, when a router enabled with dial-up backup reboots, it may bring up the backup dial-up link if the negotiation of the main link is too slow; after the main link goes up, the traffic is switched to the main link.

After a warmup timer is set, the router tries to dial the backup link only when the main link fails to come up upon timeout of the warm-up timer.

Perform the following configuration in system view.

Table 2-5 Configure the warmup timer

Operation	Command
Configure the warmup timer	**dialer timer warmup** *seconds*
Restore the default	**undo dialer timer warmup**

By default, the warmup timer is set to 30 seconds.

2.2.6 Configuring Backup Load Sharing

Before you can use this command, you must configure the **standby interface** command.

Perform the following configuration in the view of the main interface.

Table 2-6 Configure load sharing on the main interface

Operation	Command
Configure backup load sharing on the main interface.	**standby threshold** *enable-threshold disable-threshold*
Disable backup load sharing on the main interface.	**undo standby threshold**

By default, backup load sharing is disabled on the interface.

2.2.7 Setting Backup Bandwidth of the Main Interface

When the main interface participates in backup load sharing, the backup center uses the backup bandwidth that you configured preferentially. If it is not configured, the backup center automatically obtains the backup bandwidth that the system assigns to the main interface, and if it is not available, requires you to assign backup bandwidth to the main interface.

Before you can use this command, you must configure the **standby interface** command.

Perform the following configuration in the view of the main interface.

Table 2-7 Set backup bandwidth of the main interface

Operation	Command
Set backup bandwidth of the main interface.	**standby bandwidth** *numbe*r
Restore the default backup bandwidth of the main interface.	**undo standby bandwidth**

The *number* argument defaults to 0.

2.2.8 Configuring Flow Check Interval

When the main interface participates in backup load sharing, the backup center checks its traffic size automatically at the interval configured using this command.

Before you can use this command, you must configure the **standby interface** command.

Perform the following configuration in the view of the main interface.

Table 2-8 Configure the flow check interval on the main interface

Operation	Command
Configure the interval for checking the traffic size on the main interface.	**standby timer flow-check** *interval-time*
Restore the default flow check interval.	**undo standby timer flow-check**

The flow check interval defaults to 30 seconds.

2.3 Displaying and Debugging the Backup Center

After completing the above configurations, you may execute the **display** command in any view to view the operating state about the backup center, and to verify the effect of the configurations.

Execute the **debugging** command in user view to enable debugging and to view state parameters for monitoring and maintenance purpose.

Table 2-9 Display and debug the backup center

Operation	Command
Enable backup debugging.	**debugging standby event**
Disable backup debugging.	**undo debugging standby event**
Display statistics about the traffic on the main interfaces participating in backup load balancing.	**display standby flow**

Operation	Command
Display the interface state and backup state of the main and backup interfaces, and the priority, backup state flag and backup load state of the backup interfaces.	**display standby state**

2.4 Backup Center Configuration Example

2.4.1 Configuring Backup between Physical Interfaces

I. Network requirements

Use interface Serial 2/0/0 to back up interface Serial 1/0/0.

II. Configuration procedure

# Enter the view of Serial 1/0/0.

```
[3Com] interface serial 1/0/0
```

# Specify Serial 2/0/0 to back up Serial 1/0/0.

```
[3Com-Serial1/0/0] standby interface serial2/0/0
```

# Set the failover and fallback delays to 10 seconds.

```
[3Com-Serial1/0/0] standby timer delay 10 10
```

2.4.2 Configuring Multiple Backup Interfaces

I. Network requirements

Use interfaces Serial 1/0/0 and Serial 2/0/0 to back up interface Serial 0/0/0, assigning interface Serial 1/0/0 a higher priority.

II. Configuration procedure

# Enter the view of Serial 0/0/0.

```
[3Com] interface serial0/0/0
[3Com-Serial0/0/0] interface serial0/0/0
```

# Specify interfaces Serial 1/0/0 and Serial 2/0/0 to back up Serial 0/0/0, and assign them the priorities 30 and 20 respectively.

```
[3Com-Serial0/0/0] standby interface serial1/0/0 30
[3Com-Serial0/0/0] standby interface serial2/0/0 20
```

2.4.3 Configuring Dial-up Backup to the ADSL

I. Network requirements

Connect Router A to the Internet through an ADSL link and back up the link with a common dial-up link, allowing the router to connect to the Internet through PSTN by placing PPP calls when the ADSL link fails.

II. Network diagram

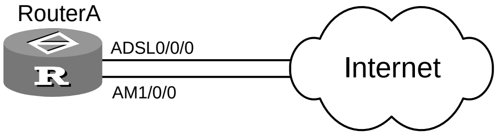


Figure 2-1 Network diagram for configuring dial-up backup to the ADSL

III. Configuration procedure

Configure Router A:

# Configure a dialer interface.

```
[3Com] dialer-rule 1 ip permit
[3Com] interface dialer 1
[3Com-Dialer1] dialer user 3Com
[3Com-Dialer1] dialer-group 1
[3Com-Dialer1] dialer bundle 1
[3Com-Dialer1] ip address ppp-negotiate
[3Com-Dialer1] standby interface analogmodem 1/0/0
```

# Configure a virtual Ethernet interface.

```
[3Com-Dialer1]interface virtual-ethernet 1
[3Com-Virtual-Ethernet1] mac 0001-0002-0003
[3Com-Virtual-Ethernet1] quit
[3Com] interface atm 0/0/0
[3Com-atm1/0/0] pvc to_adsl_a 0/60
[3Com-atm-pvc-atm0/0/0-0/60-to_adsl_a] map bridge virtual-ethernet 1
[3Com-atm-pvc-atm0/0/0-0/60-to_adsl_a] quit
```

# Configure a PPPoE session.

```
[3Com-atm1/0/0] virtual-ethernet 1
[3Com-virtual-Ethernet1] pppoe-client dial-bundle-number 1 idle-timeout 120
```

# Configure the AM interface.

```
[3Com-virtual-Ethernet1] interface analogmodem 1/0/0
[3Com-analogmodem 1/0/0] link-protocol ppp
[3Com-analogmodem 1/0/0] ip address ppp-negotiate
```

```
[3Com-analogmodem 1/0/0] dialer enable-circular
[3Com-analogmodem 1/0/0] dialer-group 1
[3Com-analogmodem 1/0/0] dialer number 163
[3Com-analogmodem 1/0/0] quit
```

# Configure static routing to the remote end.

```
[3Com] ip route 0.0.0.0 0 dialer 1 preference 70
```

Chapter 3 VRRP Configurations

3.1 Introduction to VRRP

Virtual router redundancy protocol (VRRP) is a fault-tolerant protocol. Normally, you can configure a default route for the hosts on a network, for example, 10.100.10.1 in the following figure. All packets destined to the external network are sent over this default route to Router A to gain access to the external networks. When Router A fails, all the hosts using Router A as the default next-hop router are isolated from the external network.

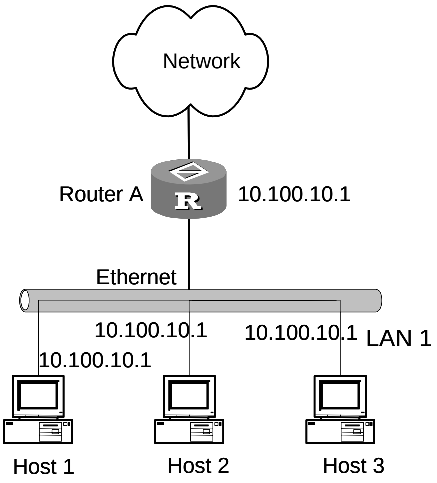


Figure 3-1 Network diagram for a LAN

VRRP was designed to address this problem on multicast and broadcast LANs such as Ethernet.

The following figure illustrates how VRRP is implemented.

VRRP combines a group of routers on a LAN (including a master and multiple backups) into a virtual router called standby group.

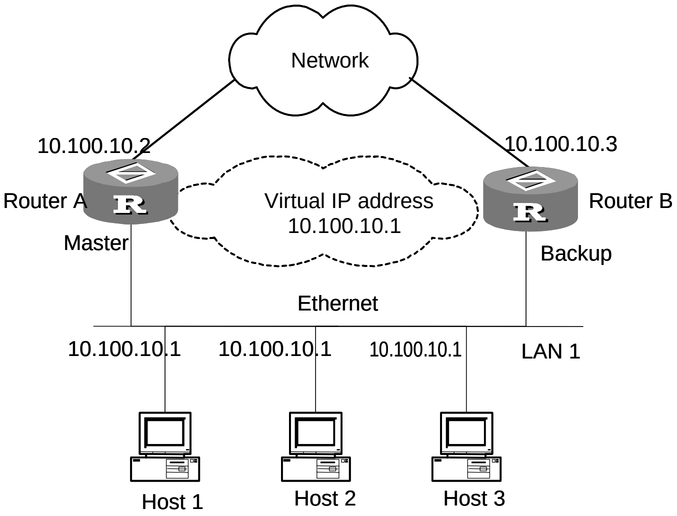


Figure 3-2 Virtual router

This virtual router has its own IP address: 10.100.10.1 (it can be the interface address on a router in the standby group). The routers in the standby group also have their own IP addresses: 10.100.10.2 for the master and 10.100.10.3 for a backup router for example.

The hosts on the LAN, however only know the IP address of this virtual router or 10.100.10.1 and as such, use this IP address as the address of the default next-hop router when communicating with the external network.

When the master in the standby group fails, the backup routers in the standby group elects a new master to take over, allowing the hosts on the network to communicate with the external network without interruption.

For more information about VRRP, refer to RFC 2338.

3.2 VRRP Configurations

The basic VRRP configuration tasks are described in the following sections:

- Enabling/Disabling Virtual IP Address Pinging
- Adding or Deleting a Virtual IP Address
- Configuring Router Priority in a Standby Group
- Configuring Preemption Mode and Preemption Delay

The advanced VRRP configuration tasks are described in the following sections:

- Configuring Authentication Mode and Authentication Key
- Configuring the Adver_Timer of VRRP
- Configuring Interface Tracking
- Configuring TTL Check on VRRP Packets

3.2.1 Enabling/Disabling Virtual IP Address Pinging

According to VRRP, users cannot ping the virtual IP addresses of standby groups and as such, cannot determine whether an IP address is assigned to a standby group. If a host on the network uses the same IP address of a standby group coincidently, all packets in this network will be forwarded to the host improperly.

You can however use this command to enable or disable users to ping the virtual IP addresses of standby groups.

Perform the following configuration in system view.

Table 3-1 Enable/disable virtual IP address pinging

Operation	Command
Enable virtual IP address pinging.	**vrrp ping-enable**
Disable virtual IP address pinging.	**undo vrrp ping-enable**

By default, virtual IP address pinging is disabled.

3.2.2 Adding or Deleting a Virtual IP Address

You may assign an IP address on this network segment to a virtual router or standby group or delete the specified or all virtual IP address from the virtual address list.

Perform the following configuration in interface view.

Table 3-2 Add/delete a virtual IP address

Operation	Command
Add a virtual IP address.	**vrrp vrid** *virtual-router-ID* **virtual-ip** *virtual-address*
Delete the specified or all virtual IP addresses.	**undo vrrp vrid** *virtual-router-ID* **virtual-ip** [*virtual-address*]

The standby group number *virtual-router-ID* is in the range 1 to 255. The virtual IP address can be an unassigned address on the network segment to which the standby group belongs, or the IP address of an interface in the standby group. In the latter case, the router owns the IP address is called IP address owner.

The system creates a standby group the first time that you assign an IP address to it. When you assign virtual IP addresses to the group after that, the system only adds the addresses to the virtual IP address list of this standby group.

Note that before you can configure a standby group, you must create it by assigning an IP address to it. Deleting the last virtual IP address from the standby group also deletes the standby group. After that, all its configurations become invalid.

Note:

- For the router, an interface can be assigned to 64 standby groups, each containing up to 16 virtual IP addresses. When more than 14 VRRP standby groups are present, you must enable promiscuous mode on interfaces to ensure connectivity of direct routes, preventing packet drop when VRRP backup and load sharing are used.
- When the state of the VRRP standby group on the current router is master, its virtual IP address in the standby group can be used as the source IP address for a GRE channel or the local IP address for an IKE peer.

3.2.3 Configuring Router Priority in a Standby Group

In VRRP, the role that a router plays in a standby group depends on its priority. The router with the highest priority becomes the master.

The priority is in the range 0 to 255, with a larger number indicating a higher priority. However, the configurable range is 1 to 254. The priority 0 is reserved for special use and 255 for the IP address owner.

Perform the following configuration in interface view.

Table 3-3 Configure the priority of the interface in the standby group

Operation	Command
Configure the priority of the interface in the standby group.	**vrrp vrid** *virtual-router-ID* **priority** *priority-value*
Restore the default value.	**undo vrrp vrid** *virtual-router-ID* **priority**

The priority defaults to 100. The higher the number, the higher the priority of the backup interface.

Note:

The IP address owner has two priorities: configurable and operating. The configurable priority is the one assigned using the **vrrp vrid** command and the operating priority is always 255 and not configurable.

3.2.4 Configuring Preemption Mode and Preemption Delay

In non-preemption mode, once a router in the standby group becomes the master and operates well, other routers, even assigned higher priority later, cannot preempt it. A backup router working in preemption mode however, can preempt a lower priority master. Accordingly, the existing master becomes a backup.

When enabling preemption in a standby group, you can configure a delay to have the backup routers wait for a while before preempting the existing master. This is to prevent frequent state transition on an unstable network where the backup routers cannot receive packets from the master regularly due to network congestion instead of master failure.

The delay is in the range 0 to 255 seconds.

Perform the following configuration in interface view.

Table 3-4 Configure the preemption mode and preemption delay for a standby group

Operation	Command
Enable preemption and configure preemption delay for a standby group.	**vrrp vrid** *virtual-router-ID* **preempt-mode** [**timer delay** *delay-value*]
Disable preemption in the standby group.	**undo vrrp vrid** *virtual-router-ID* **preempt-mode**

The default mode is preemption without delay.

🕮 **Note:**

After you disable preemption, the preemption delay automatically becomes to 0 seconds.

3.2.5 Configuring Authentication Mode and Authentication Key

VRRP provides two authentication modes: simple (simple text authentication) and MD5.

On a secure network, you can use the default where no authentication key is required. It allows the router to ignore authentication considerations when handling the VRRP packets to be sent and to consider those received as genuine and legitimate without authentication.

On a network where potential threats are present, you can set the authentication mode to simple, where the authentication key must not be greater than eight bytes. When the router sends a VRRP packet, it fills the authentication key into the VRRP packet. When the router receives a VRRP packet, it compares the authentication key in the packet with the one that it retains. If they are the same, the packet is considered genuine and legitimate. If otherwise, the packet is considered illegitimate and is discarded.

On an unsafe network, you can set the authentication mode to MD5. This allows the router to authenticate VRRP packets using the authentication method provided by authentication header (AH) and the MD5 algorithm. When input in simple text, an authentication key must be 1 to 8 characters long, for example, 1234567. When input in cipher text, an authentication key must be 24 characters long, for example, (TT8F]Y\5SQ=^Q`MAF4<1!!.

The router discards the packets that fail authentication and sends traps.

Perform the following configuration in interface view.

Table 3-5 Configure the authentication mode and authentication key

Operation	Command
Configure the authentication mode and authentication key.	**vrrp authentication-mode** { **md5** *key* | **simple** *key* }
Restore the default.	**undo vrrp authentication-mode**

By default, the router does not authenticate VRRP packets.

Note:

For the standby groups on the same interface, you must set the same authentication mode and authentication key.

3.2.6 Configuring the Adver_Timer of VRRP

In a VRRP standby group, the master tells other routers that it is alive by sending VRRP packets regularly. If no VRRP packets are received after a specified period, the backup assumes the master has failed and changes its state to master. The VRRP packet sending interval and the state transition of the backup are controlled by two timers: Adver_Timer and Master_Down_Timer.

The Master_Down_Timer is about three times that of the Adver_Timer. Either enormous traffic or difference of the timer settings on the routers can result in abnormal timeout of the Master_Down_Timer, causing state transition. One solution to this problem is to set Adver_Timer (in seconds) to a greater value and/or configure preemption delay.

Perform the following configuration in interface view.

Table 3-6 Configure the Adver_Timer of VRRP

Operation	Command
Configure the Adver_Timer of VRRP.	**vrrp vrid** *virtual-router-ID* **timer advertise** *adver-interval*
Restore the default.	**undo vrrp vrid** *virtual-router-ID* **timer advertise**

The *adver_interval* argument is in the range 1 to 255 seconds and defalults to 1 second.

3.2.7 Configuring Interface Tracking

The interface tracking function expands the backup functionality of VRRP. It provides backup not only when the interface to which a standby group is assigned fails but also when other interfaces on the router become unavailable. This is achieved by tracking interfaces. When a monitored interface goes down, the priority of the router owning this interface automatically decreased by the value specified by *value-reduced,* allowing a higher priority router in the standby group to take over as the master.

Perform the following configuration in interface view.

Table 3-7 Configure interface tracking

Operation	Command
Configure the interface to be tracked.	**vrrp vrid** *virtual-router-ID* **track** *interface-type interface-number* [**reduced** *priority-reduced*]
Disable to track the specified interface.	**undo vrrp vrid** *virtual-router-ID* **track** [*interface-type interface-number*]

The *priority-reduced* argument defaults to 10.

VRRP can track the state of both physical interfaces and logical interfaces such as VT and dialer interfaces.

The following describes when a VT or dialer interface is regarded up or down:

- In MP, a VT interface goes down when IPCP of all PPP links bound with the VT interface goes down, and goes up when IPCP of one PPP link goes up.
- In non-dial PPPoA, a VT interface goes down when IPCP of all PPP links goes down, and goes up when IPCP of one PPP link goes up.
- On a PPPoE or PPPoA server, a VT interface goes down when no session is present between the server and its client and goes up when PPPoE or PPPoA creates a session.

- On a PPPoE or PPPoA client, a dialer interface goes down when no session is present between the server and its client and goes up when PPPoE or PPPoA creates a session.

📖 **Note:**

You cannot configure interface tracking on the router that is IP address owner.

3.2.8 Configuring TTL Check on VRRP Packets

Perform the following configuration in Ethernet interface view.

Table 3-8 Configure TTL check on VRRP packets

Operation	Command
Disable TTL check on VRRP packets	**vrrp un-check ttl**
Enable TTL check on VRRP packets	**undo vrrp un-check ttl**

By default, TTL check on VRRP packets is enabled.

3.3 Displaying and Debugging VRRP

After completing the above configurations, you may execute the **display** command in any view to view the operating state about VRRP, and to verify the effect of the configurations.

Execute the **debugging** command in user view.

Table 3-9 Display and debug VRRP

Operation	Command
Display state information about VRRP.	**display vrrp** [**interface** *type number* [*virtual-router-ID*]]
Enable VRRP packet debugging.	**debugging vrrp packet**
Disable VRRP packet debugging.	**undo debugging vrrp packet**
Enable VRRP state debugging.	**debugging vrrp state**
Disable VRRP state debugging.	**undo debugging vrrp state**

By default, the debugging function is disabled.

3.4 VRRP Configuration Example

3.4.1 Configuring a Single VRRP Standby Group

I. Network requirements

Host A uses the VRRP standby group formed by Router A and Router B as its default gateway for accessing Host B on the Internet.

The VRRP standby group is defined by VRID 1 and virtual IP address 202.38.160.111. In the group, Router A is the master and Router B is the backup; preemption is allowed.

II. Network diagram

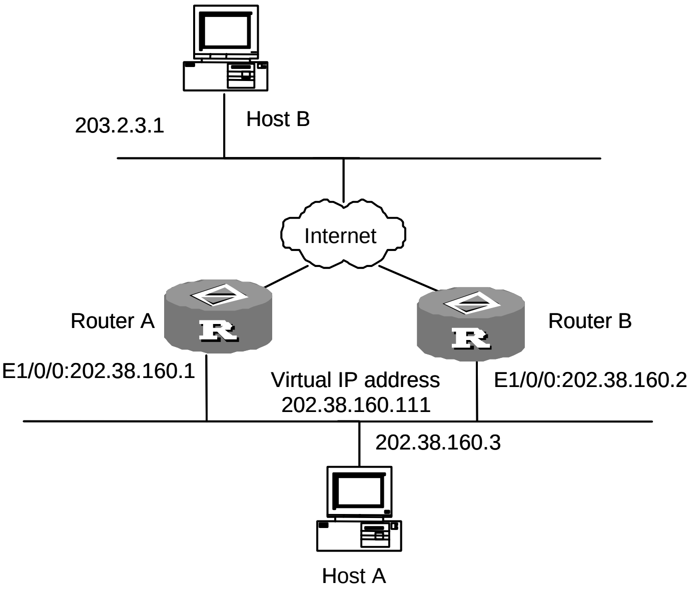


Figure 3-3 Network diagram for single VRRP standby group configuration

III. Configuration procedure

Configure Router A:

```
[3Com-Ethernet1/0/0] vrrp vrid 1 virtual-ip 202.38.160.111
[3Com-Ethernet1/0/0] vrrp vrid 1 priority 120
[3Com-Ethernet1/0/0] vrrp vrid 1 preempt-mode timer delay 5
```

Configure Router B:

```
[3Com-Ethernet1/0/0] vrrp vrid 1 virtual-ip 202.38.160.111
```

The standby group can be used immediately after configuration. On Host A, set the address of the default gateway to 202.38.160.111.

In normal circumstances, Router A functions as the gateway. When it is shut down or fails, Router B takes over. The preemption mode however allows Router A to become the master again after it recovers.

3.4.2 Configuring Interface Tracking

I. Network requirements

Sometimes even when Router A is operating, you may prefer to use Router B as the gateway because the Internet connection of Router A is unavailable. To accommodate to this situation, you may configure interface tracking.

To facilitate explanation, set the VRID number to 1 and configure authorization key and VRRP timer (which are optional in this application).

II. Network diagram

See Figure 3-3.

III. Configuration procedure

Configure Router A:

# Create a standby group.

```
[3Com-Ethernet1/0/0] vrrp vrid 1 virtual-ip 202.38.160.111
```

# Set the priority of the standby group.

```
[3Com-Ethernet1/0/0] vrrp vrid 1 priority 120
```

# Configure the authentication key of the standby group.

```
[3Com-Ethernet1/0/0] vrrp authentication-mode md5 3COM
```

# Configure the master to send VRRP packets at intervals of five seconds.

```
[3Com-Ethernet1/0/0] vrrp vrid 1 timer advertise 5
```

# Set the interface to be tracked.

```
[3Com-Ethernet1/0/0] vrrp vrid 1 track serial2/0/0 reduced 30
```

Configure Router B:

# Create a standby group.

```
[3Com-Ethernet1/0/0] vrrp vrid 1 virtual-ip 202.38.160.111
```

# Configure the authentication key of the standby group.

```
[3Com-Ethernet1/0/0] vrrp authentication-mode md5 3COM
```

# Configure the master to send VRRP packets at intervals of five seconds.

```
[3Com-Ethernet1/0/0] vrrp vrid 1 timer advertise 5
[3Com-Ethernet1/0/0] vrrp vrid 1 preempt-mode timer delay 5
```

In normal circumstances, Router A functions as the gateway. When interface Serial 2/0/0 on Router A becomes unavailable, the priority of Router A is reduced by 30, lower than that of Router B. Router B then preempts Router A to provide the gateway service.

When interface Serial 2/0/0 on Router A recovers, the router resumes its gateway function as the master.

3.4.3 Configuring Multiple Standby Groups

I. Network requirements

V 2.41 allows one router to join multiple standby groups.

You can implement load sharing by configuring multiple standby groups. For example, Router A may join standby group 1 as the master and standby group 2 as the backup, while Router B joins standby group 1 as the backup and standby group 2 as the master. By using them to provide the gateway service to different hosts, you can achieve load sharing while having the routers back up each other.

II. Network diagram

See Figure 3-3.

III. Configuration procedure

Configure Router A:

# Create standby group 1.

```
[3Com-Ethernet1/0/0] vrrp vrid 1 virtual-ip 202.38.160.111
```

# Set the priority of the standby group.

```
[3Com-Ethernet1/0/0] vrrp vrid 1 priority 120
```

# Create standby group 2.

```
[3Com-Ethernet1/0/0] vrrp vrid 2 virtual-ip 202.38.160.112
```

Configure Router B:

# Create standby group 1.

```
[3Com-Ethernet1/0/0] vrrp vrid 1 virtual-ip 202.38.160.111
```

# Create standby group 2.

```
[3Com-Ethernet1/0/0] vrrp vrid 2 virtual-ip 202.38.160.112
```

# Set the priority of standby group 2.

```
[3Com-Ethernet1/0/0] vrrp vrid 2 priority 120
```

3.5 VRRP Troubleshooting

The configuration of VRRP is simple. You can locate most of the problems by checking the output of the **display** command and the **debugging** command. The following present some troubleshooting cases.

Symptom 1:

The console screen displays error prompts frequently.

Solution:

Check that the received VRRP packets are correct.

The router may receive an incorrect VRRP packet for two reasons: its configuration is inconsistent with that on another router in the standby group; a device is attempting to send illegitimate VRRP packets. In the first case, modify the configuration. In the second case, you must resort to non-technical measures.

Symptom 2:

Multiple masters are present in the same standby group.

Solution:

If presence of multiple masters lasts a short period, this is normal and requires no manual intervention. If it lasts long, you must check that these masters can receive VRRP packets and the received packets are legitimate.

Do the following:

Have these routers ping each other.

If they can be pinged, check that their configurations are consistent, making sure that the same number of virtual IP addresses, the configured virtual IP addresses, timer setting and authentication mode are configured for the same VRRP standby group.

If they cannot be pinged, check for other reasons.

Symptom 3:

Frequent VRRP state transition is present.

Solution:

Set the Adver_Timer of the standby group to a larger value or configure a preemption delay.

Dial-Up

Table of Contents

Chapter 1 DCC Configuration

1.1 Overview

1.1.1 Introduction to DCC

I. DCC

Dial control center (DCC) is a routing technology for routers interconnected through a public switched network: public switched telephone network (PSTN) or integrated services digital network (ISDN). It can provide the dial-on-demand service whereby a router dials to set up a connection only when there is data to be transferred. When a link becomes idle, DCC automatically disconnects it.

Under certain circumstances, connections between routers are instantly established whenever there is data to be transferred, so the data transfer is characterized by no-time-correlation, outburst and small data amount. DCC provides a flexible, economical and efficient solution for such applications. In practice, DCC guarantees the priority of communications through designated backup lines. In the case that a primary line for normal communications becomes unavailable for any reasons, DCC uses the designated backup channels to carry out the communications to assure that the required services are timely completed.

At present, Frame Relay network is widely applied. Usually, the user accesses Frame Relay network through the leased line. To reduce the cost, the user can adopt Frame Relay over ISDN technology to access the Frame Relay network through ISDN line. Meanwhile, ISDN network can act as the backup of Frame Relay access.

II. Terms in DCC configuration

- Physical interface: Physical interface that actually exists, like the serial, BRI, asynchronous interfaces.
- Dialer interface: Logical interface for configuring DCC parameters. A physical interface can inherit the DCC configuration after it is bound to the dialer interface.
- Dial interface: A general term describing an interface for dialup connection. It can be a dialer interface, a physical interface bound to the dialer interface, or a physical interface directly configured with DCC parameters.

1.1.2 DCC Configuration Methods

V 2.41 provides two DCC configuration methods: circular DCC (C-DCC), and resource-shared DCC (RS-DCC). With distinguishing features, these two methods are applicable to different applications. In applications, the participating ends of a call can flexibly select either method as needed. In other words, one end can adopt C-DCC while the other end adopts RS-DCC to originate a call.

I. C-DCC

1) C-DCC is powerful and popular while relatively lacks flexibility and scalability. The features of C-DCC are:

- A logical dial (dialer) interface can use the services provided by multiple physical interfaces (such as Serial0/0/0). However, a physical interface can only belong to one dialer interface. That is, a physical interface can only provide one type of dial service.
- The user can either bind a physical interface to a dialer interface for inheriting the DCC parameters through assigning it to a dialer circular group, or directly configure DCC parameters on the physical interface.
- All the physical interfaces served for the same dialer circular group inherit the attributes of the same dialer interface.
- Through configuring the **dialer route** command, a dialer interface can be associated with multiple dialing destination addresses. Through configuring the **dialer number** command, however, a dialer interface can only be associated with one dialing destination address.

In addition, all the B channels on an ISDN BRI interface will inherit the configuration of this physical interface, and the dial route will become more complicated as the network grows and more protocols are supported. Therefore, the application of C-DCC is restricted due to the static binding between the dialing destination addresses and the physical interface configuration.

2) Association between the physical interfaces and dialer interfaces in C-DCC

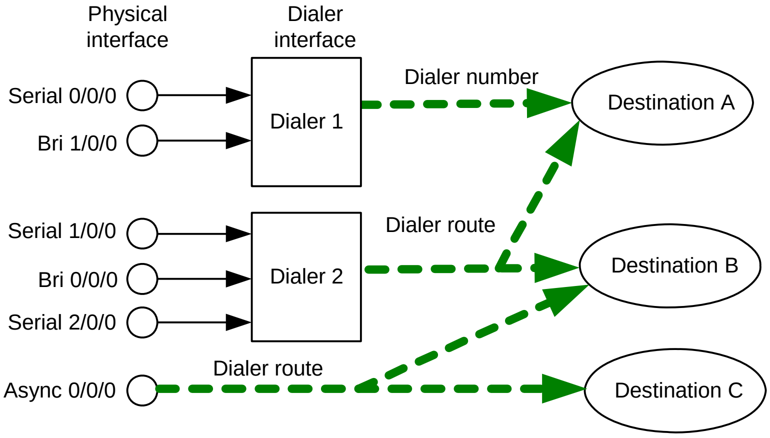


Figure 1-1 Association between the physical interfaces and dialer interfaces in C-DCC

As shown in Figure 1-1, in the case that dialer interfaces are used, a physical interface can only belong to one dialer interface, but each dialer interface can associate with multiple destination addresses. Each dialer interface can contain multiple physical interfaces. In addition, a physical interface does not necessarily belong to any dialer interface, and can directly route to one or multiple destination addresses.

As shown above, physical interfaces Serial1/0/0, Bri0/0/0 and Serial2/0/0 belong to Dialer2, and there are different dial-numbers (a kind of address) directing to different destination addresses for Dialer2. That means Dialer2 has multiple addresses.

II. RS-DCC

Comparing with C-DCC, RS-DCC is concise, and is available with good flexibility due to the separation of logical and physical configurations. Specifically, RS-DCC has the following features:

- Separate the configuration of physical interfaces from the logical configuration required for calls and then dynamically binds them. Thus, a physical interface can provide services for various dial applications.
- A dialer interface only associates with a dialing destination address, which is specified in the **dialer number** command.
- Each logical dialer interface can use the services provided by multiple physical interfaces, and each physical interface can serve multiple dialer interfaces at the same time.
- Dial attributes are described by RS-attribute set. All the calls originated to the same destination network use the same RS-attribute set (including the parameters like dialer interface, dialer bundle, physical interface, etc).
- RS-DCC parameters cannot be directly configured on a physical interface. The physical interface can have RS-DCC service only after it is bound to a dialer interface.
- The figure below shows the association of the physical interfaces, dialer bundles and dialer interfaces in RS-DCC

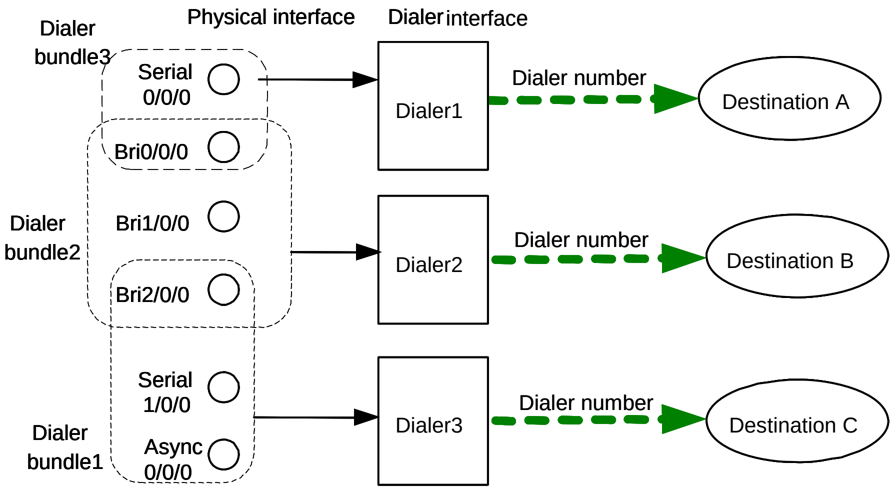


Figure 1-2 Association of physical interfaces, dialer bundles and dialer interfaces in RS-DCC

As shown in Figure 1-2, a physical interface can belong to multiple dialer bundles and serves for them, but each dialer interface can only associate with one destination address. Only one dialer bundle can be used by each dialer interface, and each dialer bundle contains multiple physical interfaces with different priorities.

In the above figure, Dialer2 uses Dialer bundle2, and physical interfaces Bri0/0/0, Bri1/0/0 and Bri2/0/0 are members of Dialer bundle2. These physical interfaces have different priorities. Suppose that Bri0/0/0 in Dialer bundle2 is assigned with the priority 100, Bri1/0/0 with 50, and Bri2/0/0 with 75. Since the priority of Bri0/0/0 is higher than that of Bri1/0/0 and Bri2/0/0, Bri0/0/0 will be selected first when Dialer2 selects a physical interface from Dialer bundle2.

1.1.3 DCC Features Available with V 2.41

I. Basic DCC features

V 2.41 provides users with flexible and practical dial interface solution, featuring:

- Support various dial interfaces, such as synchronous/asynchronous serial interface, AUX port, ISDN BRI or PRI interface, and AM interface. The user can flexibly combine them, depending on the actual networking and network topology.
- Support the link layer protocols, such as PPP and Frame Relay, on dial interfaces (physical or dialer interfaces).
- Support the network layer protocols, such as IP, IPX on dial interfaces.
- Support dynamic routing protocols, such as RIP and OSPF, on dial interfaces.
- Provide flexible dial interface standby modes.
- Provide administer modem devices with the command in user-interface view.

II. Implementing callback through DCC

In callback, the “called party” originates a return call to the “calling party”. In which, the calling party is the client, and the called party is the server. The callback client originates a call first, and the callback server determines whether to originate a return call. If a callback is needed, the server will immediately disconnect and originate a return call.

DCC callback can:

- Enhance security: When placing a return call, the server will dial the calling number configured at the local end. Hence, the insecurity resulted from the distribution of user name and password can be avoided.
- Change the charge bearer. This is useful for saving cost in the case that the call rates in two directions are different.
- Consolidate the call charge bills, which will facilitate the settlement.

At present, V 2.41 system provides the PPP callback and ISDN caller identification callback features. The PPP callback conforms to RFC1570 system and supports that the client and server own fixed network addresses, or that the client accepts the dynamic network address.

1.1.4 Preparation for DCC Configuration

I. Determining the topology of DCC application

- Determine which routers will provide DCC and the relevant communication parameters between the routers.
- Determine the interfaces on the routers that provide DCC, and the functions carried out by each interface.
- Determine the data transfer medium, e.g. PSTN or ISDN.

II. Preparing the data for DCC configuration

- Identify the interface type (synchronous/asynchronous serial interface, ISDN BRI or PRI interface, AM interface, AUX interface) and configures the basic physical parameters on the interface.
- Configure the link layer protocol (PPP, HDLC, Frame Relay, X.25 or other protocols) to be used on the dial interface.
- Configure the network protocol (IP or other protocols) to be used on the dial interface.
- Configure the routing protocol (RIP, OSPF, or other protocols) to be supported on the dial interface.
- Selects a DCC configuration method (C-DCC or RS-DCC).

III. Configuring the parameters of DCC

Follow the procedure to configure the basic DCC parameters according to the selected DCC configuration method, e.g., a C-DCC or RS-DCC, to enable the initial DCC implementation. Configure MP binding, PPP callback, ISDN caller identification callback, ISDN leased line, or/and auto-dial in addition to the basic DCC configuration if special applications are required. Alternatively, depending on the actual dialing link state, the user can make an appropriate adjustment to the attribute parameters of the DCC dial interface.

1.2 DCC Configuration

DCC configuration includes to:

- Configure the basic parameters of DCC
- Configure C-DCC
- Configure RS-DCC
- Configure MP binding for DCC
- Configure PPP callback
- Configure ISDN caller identification callback

- Configure special DCC functions
- Configure attributes of DCC dial interface
- Configure traffic statistic interval
- Clear a dial-up link
- Configure dialer-route logical interfaces for backup
- Specify a physical interface for placing/receiving calls

1.2.1 Configuring the Basic Parameters of DCC

Regardless of which method is used, C-DCC or RS-DCC, you must perform the tasks described in this section.

I. Configuring the mode of the physical interface

For a synchronous/asynchronous serial interface, you must set its operating mode depending on the connected modem. If the connected modem is asynchronous, set the interface to operate in asynchronous mode and then enable modem dial on the corresponding user interface. If the connected modem is synchronous, set the interface to operate in synchronous mode.

For an ISDN BRI or PRI interface, skip this step.

Perform the following configuration in dial interface (synchronous/asynchronous serial interface) view.

Table 1-1 Configure physical interface mode

Operation	Command
Configure the synchronous/asynchronous serial port to operate in asynchronous or synchronous mode	**physical-mode** { **async | sync** }
Configure the asynchronous serial port to operate in protocol mode	**async mode** { **flow | protocol** }
Enable modem dial on user-interface	**modem** [**both | call-in**]

By default, the synchronous/asynchronous serial port operates in **synchronous** mode and the asynchronous interface operates in **flow** mode.

📖 **Note:**

For the synchronous serial port connected to the synchronous modem, there is no need to configure the **physical-mode** command.

II. Configuring link layer and network and routing protocols on the interface

Execute the **link-protocol** command and **ip address** command in the dial interface view and perform other configurations in system view.

Table 1-2 Configure link layer and network and routing protocols on the interface

Operation	Command
Set a link layer protocol on the dial interface	**link-protocol** *linklayer-protocol-type*
Configure an IP address for the dial interface	**ip address** *ipaddress mask*
Configure RIP	**rip**
Configure OSPF	**ospf** [*process-id*]
Configure BGP	**bgp** *as-number*

Where, *linklayer-protocol-type* is interface type dependent. For more information about how to configure it, refer to the “Link Layer Protocol”, “Network Protocol”, and “Routing Protocol” parts of this manual.

📖 **Note:**

For an ISDN B channel enabled with RS-DCC, its initial encapsulation is PPP. After this B channel is selected for communication, its encapsulation protocol changes dynamically to accommodate to the dialer interfaces with different encapsulations. This allows for great flexibility. After the B channel is released, its link protocol becomes PPP automatically.

III. Associating a DCC dialer ACL with the interface

A properly configured dialer ACL can filter various packets that traverse the dial interface. The packets fall into two categories, depending on whether the packets are in compliance with the “permit” or “deny” statements in the dialer ACL.

- The packet complies with the “permit” statements. If the corresponding link has been set up, DCC will send the packet via this link and clear all the data in the idle-timeout timer. If not, it will originate a new call.
- The packet does not comply with the “permit” statements in the list. If the corresponding link has been set up, DCC will send the packet via this link without clearing the idle-timeout timer to zero. If not, it will discard the packet without originating a call.

To enable DCC to originate a call normally, the user must configure a DCC dialer ACL and associate the corresponding interface (physical or dialer interface) to the dialer ACL through the **dialer-group** command. Otherwise, DCC cannot normally originate a call. The user can either directly configure the conditions for filtering packets in the DCC dialer ACL, or reference the filtering rules in an ACL.

Perform the configuration of the **dialer-group** command in dial interface (physical or dialer interface) and other configurations in system view.

Table 1-3 Configure physical interface mode

Operation	Command
Configure DCC dial-up ACL	**dialer-rule** *dialer-number* { *protocol-name* { **permit** | **deny** } | **acl** *acl-number* }
Delete DCC dial-up ACL	**undo dialer-rule** *dialer-number* { **acl** | *protocol-name* }
Configure the dialer group on a dialer interface	**dialer-group** *group-number*
Remove a dialer interface from a specified dialer group.	**undo dialer-group**
Create and enter an ACL view	**acl number** *access-list-number*
Configure the standard ACL rule	**rule** [*rule-id*] { **permit** | **deny** } [**source** *sour-addr sour-wildcard* | **any**] [**time-range** *time-name*] [**logging**] [**fragment**]
Configure the extended ACL rule	**rule** [*rule-id*] { **permit** | **deny** } *protocol* [**source** *sour-addr sour-wildcard* | **any**] [**destination** *dest-addr dest-mask* | **any**] [**source-port** *operator port1* [*port2*]] [**destination-port** *operator port1* [*port2*]] [**icmp-type** *icmp-type icmp-code*] [**precedence** *precedence*] [**tos** *tos*] [**time-range** *time-name*] [**logging**] [**fragment**]
Configure the interface-based ACL rule	**rule** [*rule-id*] { **permit** | **deny** } { **interface** *type number* } [**time-range** *time-name*] [**logging**]

By default, neither DCC dialer ACL, nor the access control group assigned with a dial interface is configured.

Note:

Make sure that the arguments in the commands **dialer rule** *dialer-number* and **dialer-group** *dialer-group* are consistent.

1.2.2 Configuring C-DCC

If C-DCC is used, each physical interface can either be directly configured with the DCC parameters, or bound to a dialer interface to inherit the DCC parameters through a dialer circular group. Between these two options, configuring the DCC parameters directly on a physical interface is only applicable for a single interface to originate calls to one or more remote ends. However, dialer circular group is also applicable for multiple interfaces to originate calls to one or more remote ends in addition to that.

Dialer circular group associates a dialer interface with a group of physical interfaces. The DCC configurations of this dialer interface are automatically inherited by all the physical interfaces in the dialer circular group. After configuring the parameters for the dialer circular group, any physical interface in the group can call any predefined destination if the dialer interface is associated with multiple destinations.

Depending on the network topology and DCC dialing demands, such as one interface or multiple interfaces can both originate and receive calls, the user can flexibly use one configuration or the combination of several configurations in the C-DCC configurations introduced below.

🕮 **Note:**

In the C-DCC implementation of DCC, the two dial parties can configure password authentication protocol (PAP) or challenge-handshake authentication protocol (CHAP) authentication. However, the other party must configure authentication if one party has done that. For security of dialing ID, the user is recommended to configure authentication in actual networking applications. For configuration methods, refer to the section in *Operation Manual - Link Layer Protocol* and note the following items accordingly:

- At the sending side, if DCC is directly enabled on the physical interface, directly configure PAP or CHAP authentication on the physical interface. If DCC is enabled through a dialer circular group, configure PAP or CHAP authentication on the dialer interface.
- When configuring PAP or CHAP authentication at the receiving end, the user is recommended to make the configuration on both physical and dialer interfaces. That is because the physical interface will first implement PPP negotiation and authenticate the validity of the dialing user when receiving a DCC call request, and then deliver the call to the upper layer DCC module for processing.

I. Configuring an interface to originate calls to a remote end

Perform the following configuration steps after the basic DCC configuration is completed. As shown in the following figure, a local interface originates a call to a single remote end (the picture components of inverse color represent the routers irrelevant with the networking):

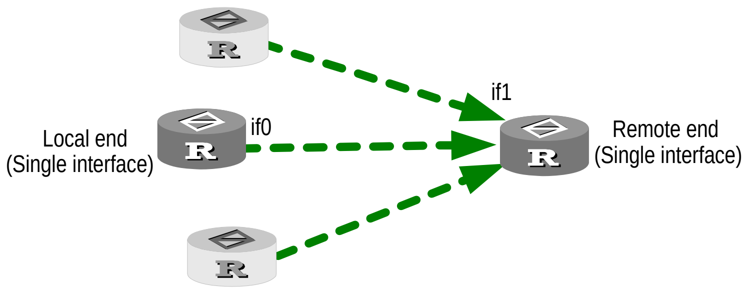


Figure 1-3 An interface placing a call to a remote end

As shown in the above figure, the single local interface interface0 (if0) originates a DCC call to the single remote interface if1. Since the call is originated to a single remote end, the dialer string can be configured using the **dialer number** or **dialer route** command. When the call is originated from the single interface at the local end, the dialer circular group can be used to configure the DCC. The user can select to configure either PAP or CHAP authentication on the interface.

Perform the following configuration in dial interface (physical or dialer interface) view.

Table 1-4 Configure a local interface to originate calls to a remote end

Operation	Command
Enable C-DCC	**dialer enable-circular**
Configure a dialer number for calling a remote end	**dialer number** *dial-number*
Delete the dialer number for calling the remote end	**undo dialer number**

By default, C-DCC is enabled on ISDN BRI and PRI interfaces, but disabled on other interfaces (serial, asynchronous, AUX, etc.) and the user should manually configure the **dialer enable-circular** command. No dialer number for calling the remote end is configured by default.

II. Configuring an interface to receive calls from a remote end

Perform the following configuration steps after the basic DCC configuration is implemented. As shown in the following figure, a local interface receives a call from a single remote end (the picture components of inverse color represent the routers irrelevant with the networking):

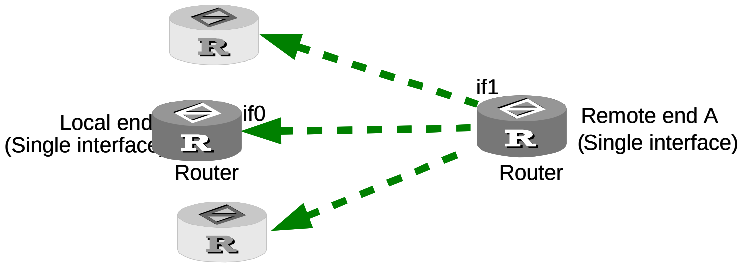


Figure 1-4 An interface receiving a call from a remote end

As shown in the above figure, the single local interface interface0 (if0) receives a DCC call from a single remote interface if1. Since the call is received by a single local interface, the dialer circular group can be used to configure DCC. The user can select to configure either PAP or CHAP authentication.

Perform the following configuration in dial interface (physical or dialer interface) view.

Table 1-5 Configure a local interface to receive calls from a remote interface

Operation	Command
Enable C-DCC	**dialer enable-circular**

By default, C-DCC is enabled on ISDN BRI and PRI interfaces, but disabled on other interfaces (serial, asynchronous, AUX, etc.) and the user should manually configure the **dialer enable-circular** command.

III. Configuring originating calls from an interface to multiple remote ends

Perform the following configuration steps after the basic DCC configuration is implemented. As shown in the following figure, a local interface originates calls to multiple remote ends (the picture components of inverse color represent the routers irrelevant with the specific networking):

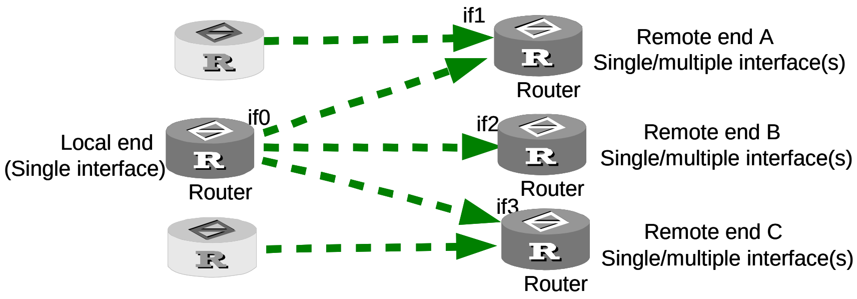


Figure 1-5 An interface placing calls to multiple remote ends

As shown in the above figure, a single local interface interface0 (if0) originates DCC calls to the remote interfaces if1 and if2. Since calls are originated to multiple remote ends, the user must use the **dialer route** command to configure the dialer numbers and destination addresses. Since the calls are originated from a single local interface, the dialer circular group can be used to configure DCC. The user can select to configure either PAP or CHAP authentication.

Perform the following configuration in dial interface (physical or dialer interface) view.

Table 1-6 Configure a local interface to originate calls to multiple remote ends

Operation	Command
Enable C-DCC	**dialer enable-circular**
Configure destination address(es) and dialer number(s) for calling one or more remote ends	**dialer route** *protocol next-hop-address* [**mask** *network-mask-length*] *dial-number* [**autodial**]
Delete the destination address(es) and dialer number(s) for calling one or more remote ends	**undo dialer route** *protocol next-hop-address*

By default, C-DCC is enabled on ISDN BRI and PRI interfaces, but disabled on other interfaces (serial, asynchronous, AUX, etc.) and the user should manually configure the **dialer enable-circular** command. No dialer numbers for calling the remote ends are configured by default.

IV. Configuring an interface to receive calls from multiple remote ends

Perform the following configuration steps after the basic DCC configuration is implemented. As shown in the following figure, a local interface receives calls from multiple remote ends (the picture components of inverse color represent the routers irrelevant with the networking):

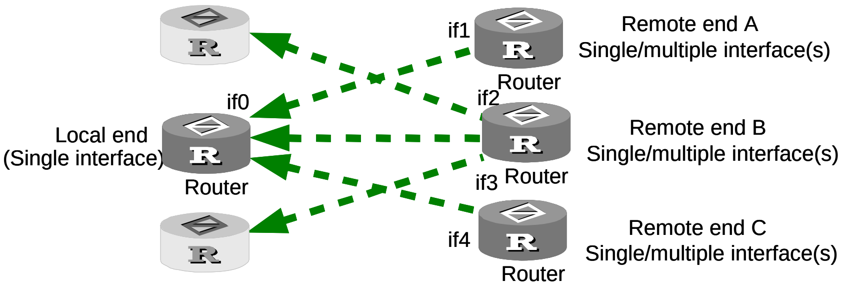


Figure 1-6 An interface receiving calls from multiple remote ends

As shown in the above figure, the single local interface interface0 (if0) receives DCC calls from the remote interfaces if1 and if4. Since the local end is a single interface, the dialer circular group can be used to configure DCC. The user can select to configure either PAP or CHAP authentication.

Use **local-user** in system view and **password** in local user view to configure the username and password of a user that is allowed to dial in, and then perform other configuration tasks in dial interface (physical or dialer interface) view.

Table 1-7 Configure a local interface to receive calls from multiple remote ends

Operation	Command
Enable C-DCC	**dialer enable-circular**

By default, C-DCC is enabled on ISDN BRI and PRI interfaces, but disabled on other interfaces (serial, asynchronous, AUX, etc.) and the user should manually configure the **dialer enable-circular** command. No authentication parameters or dial-in user information are configured by default.

V. Configuring multiple interfaces to originate calls to multiple remote ends

Perform the following configuration steps after the basic DCC configuration is implemented. As shown in the following figure, multiple local interfaces originate calls to multiple remote ends (the picture components of inverse color represent the routers irrelevant with the networking):

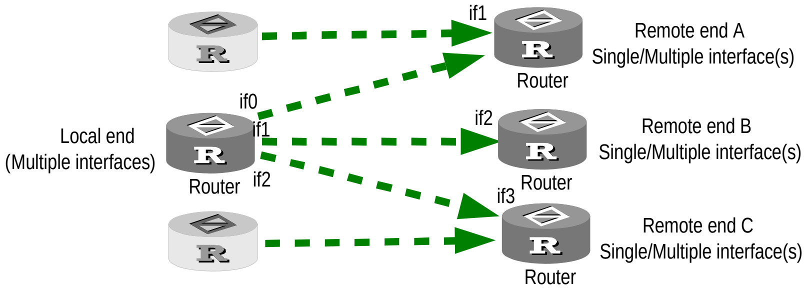


Figure 1-7 Multiple interfaces placing calls to multiple remote ends

As shown in the above figure, the local interfaces interface0 (if0), if1, and if2 originate DCC calls to the remote interfaces if1, if2 and if3. For allowing calls to multiple remote ends, the user must use the **dialer route** command to configure the dialer strings and destination addresses. For the calls to originate from multiple interfaces, the dialer circular group must be used to configure DCC. The user can select to configure either PAP or CHAP authentication.

Instead of using their own IP addresses, the physical interfaces in the dialer circular group use the IP address of the dialer interface to make calls. The *number* argument in the **dialer circular-group** *number* command configured in the view of a physical interface must be the same as the one used in the **interface dialer** *number* command corresponding to this physical interface. ISDN BRI or PRI interface is regarded as the dialer circular group for its own B channels. At the same time, they can be the physical interfaces in other dialer circular groups.

Use the **interface dialer** command to create a dialer interface in system view, add a physical interface to the specified dialer circular group through the **dialer circular-group** command in interface view, and perform other configuration processes in dialer interface view.

Table 1-8 Configure multiple local interfaces to originate calls to multiple remote ends

Operation	Command
Enable C-DCC	**dialer enable-circular**
Configure the destination address(es) and the dialer number(s) for calling one (or more) remote end(s)	**dialer route** *protocol next-hop-address* [**mask** *network-mask-length*] *dial-number* [**autodial**]
Delete the destination address(es) and dialer number(s) for calling one (or more) remote ends	**undo dialer route** *protocol next-hop-address*
Create a dialer interface and enter the dialer interface view	**interface dialer** *number*
Delete the existing configurations of the dialer interface	**undo interface dialer** *number*
Bundle a physical interface with the specified dialer circular group	**dialer circular-group** *number*
Delete the physical interface from the specified dialer circular group	**undo dialer circular-group**
Configure the priority of the physical interface in the dialer circular group	**dialer priority** *priority*
Restore the default priority of the physical interface in the dialer circular group	**undo dialer priority**

By default, C-DCC is enabled on ISDN BRI and PRI interfaces, but disabled on other interfaces (serial, asynchronous, AUX, etc.) and the user should manually configure the **dialer enable-circular** command. In addition when no dialer interface is created, the physical interface does not belong to any dialer circular group, and the default priority is 1 if the physical interface is added to the dialer circular group.

VI. Configuring multiple interfaces to receive calls from multiple remote ends

Perform the following configuration steps after the basic DCC configuration is implemented. As shown in the following figure, multiple local interfaces receive calls from multiple remote ends (the picture components of inverse color represent the routers irrelevant with the networking):

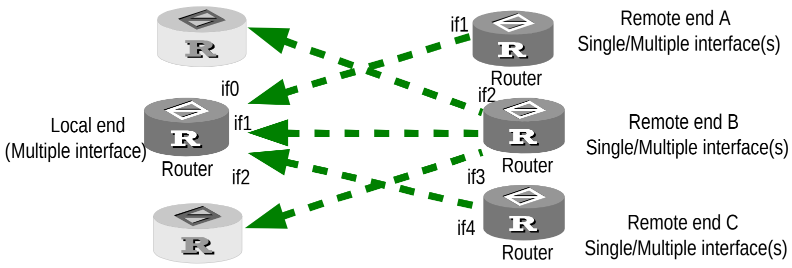


Figure 1-8 Multiple interfaces receiving calls from multiple remote ends

As shown in the above figure, the local interfaces interface1 (if0), if1, and if2 receive DCC calls from the remote interfaces if1, if2 and if3. Since the local end is multiple interfaces, the dialer circular group must be used to configure DCC. The user can select to configure either PAP or CHAP authentication.

Use **local-user** in system view and **password** in local user view to configure the username and password of a user that is allowed to dial in, and perform other configuration tasks in dial interface (physical or dialer interface) view.

Table 1-9 Configure multiple local interfaces to receive calls from multiple remote ends

Operation	Command
Enable C-DCC	**dialer enable-circular**
Create a dialer interface and enter the dialer interface view	**interface dialer** *number*
Delete the existing configuration of the dialer interface	**undo interface dialer** *number*
Add a physical interface to the specified dialer circular group	**dialer circular-group** *number*
Delete the physical interface from the specified dialer circular group	**undo dialer circular-group**

By default, C-DCC is enabled on ISDN BRI and PRI interfaces, but disabled on other interfaces (Serial, Asynchronous, AUX, etc.) and the user should manually configure the **dialer enable-circular** command. If no dialer interface is created then by default, the physical interfaces do not belong to any dialer circular group.

1.2.3 Configuring RS-DCC

Each RS-attribute set consists of a dialer interface, the attributes of the interface, and a dialer bundle. Specifically,

- Only one dialing number can be defined for a dialer interface. Since this dialing number has its own dial attributes set, all the calls originated by dialing this number can use the same DCC attribute parameters (such as dialing rate).

- Each dialer interface can use only one dialer bundle, which contains multiple physical interfaces of different priorities. However, each physical interface can be used by different dialer bundles. For an ISDN BRI or PRI interface, the number of B channels used can be configured by using the **dialer bundle** command.
- All the calls aimed to the same destination segment use the same RS-attribute set.

Due to the differences between the configurations of logical and physical interface, RS-DCC are applicable for more network topologies and DCC dialing requirements, especially for the situation in which multiple interface groups originate calls to multiple remote interfaces.

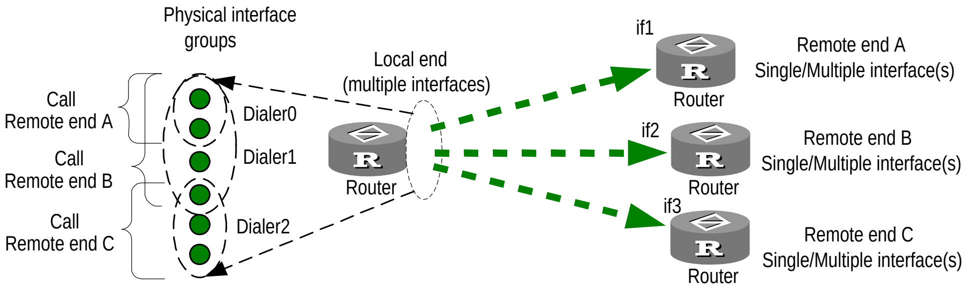

Physical interface groups
Call Remote end A
Call Remote end B
Call Remote end C
Dialer0
Dialer1
Dialer2
Local end (multiple interfaces)
Router
if1
if2
if3
Router
Router
Router
Remote end A Single/Multiple interface(s)
Remote end B Single/Multiple interface(s)
Remote end C Single/Multiple interface(s)

Figure 1-9 Multiple interfaces placing calls to multiple remote ends in the RS-DCC implementation

As shown in the above figure, different dialer interfaces are used for establishing calls to different remote ends. (That is, one dialer interface only corresponds to one remote end.) A physical interface can generate calls to different destinations by joining the interface into bundles, each of which corresponds to a certain dialer interface.

When you configure RS-DCC based on RS-attribute set, a physical interface only needs to be configured with the link layer protocol and the number of the dialer bundle to which the physical interface belongs.

Note:

When you configure RS-DCC based on RS-attribute set, a RS-attribute set is unable to apply its attributes to the physical interfaces in a dialer bundle. (For example, it is unable to apply PPP authentication to the physical interfaces.) In other words, the physical interfaces do not inherit the authentication attribute of the RS-attribute set. Therefore, authentication of the related information must be configured on the physical interfaces at the receiving end.

When RS-DCC applies, you must configure authentication (including the dialer user and PPP authentication configuration tasks) on both dialer interfaces and their physical interface. That is because RS-DCC needs to conduct PPP negotiation first on the physical interface and sends the agreed-upon peer username to DCC. Based on this peer username, DCC decides which dialer interface is used and then sends its configuration to PPP. PPP then starts IP control protocol (IPCP) negotiation with the configuration of the dialer interface.

RS-DCC configuration includes to:

- Enable RS-DCC
- Configure the dialer interface and dialer number
- Create dialer bundle and assigning physical interfaces to it
- Configure dialing authentication for RS-DCC

I. Enabling RS-DCC

Before enabling the RS-DCC, please use the command **undo dialer enable-circular** to disable C-DCC first, then enable the RS-DCC by using the **dialer bundle** command.

Perform the following configuration in dialer interface view.

Table 1-10 Enable RS-DCC

Operation	Command
Disable C-DCC	**undo dialer enable-circular**
Enable RS-DCC and specify the user name	**dialer user** *username*
configure the dialer bundle used by Dialer interface	**dialer bundle** *number*
Disable RS-DCC and delete the dialer bundle	**undo dialer bundle**

By default, RS-DCC is disabled and no dialer bundle is created.

II. Configuring the dialer interface and dialer number

Since the attributes of the physical interface may be changed by the dialer number, the DCC parameters should be configured on the dialer interface. Furthermore, only the **dialer number** command can be used to configure the dialer numbers for calling the remote ends.

Use the **interface dialer** command to create a dialer interface in system view, and then perform other configurations in dialer interface view.

Table 1-11 Configure a dialer interface and dialer number

Operation	Command
Create a dialer interface, and enter the dialer interface view	**interface dialer** *number*
Delete the existing configuration of the dialer interface	**undo interface dialer** *number*
Configure a dialer number for calling a remote end	**dialer number** *dial-number*
Delete the dialer number for calling a remote end	**undo dialer number**

By default, no dialer interface is created.

III. Creating dialer bundle and assigning physical interfaces to it

To implement the RS-DCC, the system selects a physical interface based on the dialing priority from a dialer bundle. The command **dialer bundle** is used for creating the dialer bundle for a Dialer interface and the **dialer user** command is used to enable the RS-DCC function simultaneously, which is mentioned above.

Perform the following configuration steps in physical interface view.

Table 1-12 Creating a dialer bundle and assigning the physical interfaces to it

Operation	Command
Add a physical interface to the specified dialer bundle	**dialer bundle-member** *number* [**priority** *priority*]
Delete the physical interface from the dialer bundle	**undo dialer bundle-member** *number*

By default, no dialer bundle is created, and the physical interfaces do not belong to any dialer bundle. If a physical interface is assigned to a dialer bundle, a default priority of 1 is assigned.

IV. Configuring dialing authentication for RS-DCC

To implement the RS-DCC, it is required for the called party to identify the calling parties through authentication because of the complicated map relations between the physical interfaces and the dialer interfaces. Therefore, PAP or CHAP authentication must be configured.

Use **dialer user** in dialer interface view, **local-user** in system view, **password** in local user view, and other configuration tasks in dial interface (physical or dialer interface) view.

Table 1-13 Configure multiple interfaces to receive calls from multiple remote ends

Operation	Command
Configure the remote user name	**dialer user** *username*
Delete the remote user name	**undo dialer user**
Configure the link layer protocol to PPP	**link-protocol ppp**
Configure an authentication mode	**ppp authentication-mode** { **pap** | **chap** }
Configure the interface to send the local user name and password for PAP authentication	**ppp pap local-user** *username* **password** { **cipher** | **simple** } *password*
Configure the user name that the local end will send to the remote end for CHAP authentication	**ppp chap user** *username*
Configure the password that the local end will send to the remote end for CHAP authentication	**ppp chap password** { **cipher** | **simple** } *password*
Configure the username of the remote end that is allowed to dial in	**local-user** *username*
Configure a password for the remote end that is allowed to dial in	**password** { **cipher** | **simple** } *password*

Note:

- The users are recommended to configure either PAP or CHAP authentication on both the physical and dialer interfaces of both sender and receiver.
- When PPP is encapsulated on a Dialer interface, the remote user name gained through PPP authentication procedure will determine the Dialer interface for receiving calls, then the command **dialer user** is a must and the command **dialer number** is optional.

1.2.4 Configuring MP Binding for DCC

I. Implementing MP by setting link load thresholds

In DCC applications, you can configure load thresholds for links.

When you set the link load threshold in the range 1 to 99, MP tunes allocated bandwidth according to actual traffic percentage as follows:

- When the percentage of traffic on a link to bandwidth exceeds the defined traffic threshold, the system automatically brings up the second link, and assigns them to one MP bundle. When the percentage of traffic on these two links to bandwidth exceeds the defined traffic threshold, the system brings up the third link, and assigns it to the MP bundle, so on and so forth. This ensures appropriate traffic distribution for DCC links.

- On the contrary, when the percentage of the traffic of N (which is an integer greater than 2) links to the bandwidth of N-1 links is smaller than the defined traffic threshold, the system will automatically shutdown a link, so on and so forth. Thus, the utility rate of DCC links can be kept within an appropriate range.

To implement MP binding with DCC, you must use dialer interfaces. The following is how MP operates after you configure the **ppp mp** and **dialer threshold** commands on a dialer interface:

1) When the ratio of traffic to bandwidth on a physical interface (or B channel) assigned to the dialer interface exceeds the load threshold, DCC brings up another physical interface assigned to the dialer interface, and assigns these links to an MP bundle. If the physical interfaces are ISDN BRI or PRI interfaces, DCC uses idle B channels on them to form an MP bundle.
2) When the number of bundled links reaches the upper threshold specified by the *max-bind-num* argument, DCC stops to bring up new links.

Note that when MP is used with DCC, the commands **dialer threshold**, **ppp mp max-bind**, and **ppp mp min-bind** must be configured in dialer interface view. When configuring other PPP commands, observe the following:

- In the C-DCC approach, configure in dialer interface view.
- In the RS-DCC approach, configure in dialer interface view at the calling end and in physical dial interface view at the called end. At the calling end, however, you are recommended to configure the same PPP parameters on both dialer and physical dial interfaces, to ensure reliable PPP link negotiation.

Table 1-14 Configure MP by setting link load thresholds

Operation	Command
Enable MP	**ppp mp**
Configure upper limit of links in an MP bundle	**ppp mp max-bind** *max-bind-num*
Set link load thresholds	**dialer threshold** *traffic-percentage* [**in-out** | **in** | **out**]

By default, the upper limit of links in an MP bundle is 16, MP is disabled, and link load threshold is not configured.

Note:

- The **dialer threshold** command takes effect only on dial MP links. It does not take effect on non-dial MP links and dial links with MP disabled.
- You need to configure the **dialer threshold** command only at the calling end.
- If the **dialer threshold 0** command is configured, DCC may bring up all available links and the **dialer timer idle** command becomes invalid.

II. Implementing MP by setting the lower limit of links in an MP bundle

Some dial applications may require multiple links to carry service. To this end, you may configure the **ppp mp min-bind** command, allowing the router to bring up multiple when triggered to ensure minimum bandwidth. The following is how MP operates in this case:

1) The router brings up the first link.
2) When the first link comes up, the router checks whether the number of links in the MP bundle reaches the lower limit specified by the *min-bind-num* argument. If not, the router brings up the second link.

This process continues until the number of links in the MP bundle reaches the lower limit.

Perform the following configuration in dialer interface view.

Table 1-15 Configure MP by setting lower limit of links in an MP bundle

Operation	Command
Enable MP	**PPP mp**
Configure the lower limit of links in an MP bundle	**ppp mp min-bind** *min-bind-num*

By default, no lower limit of links is set for MP bundling.

Note:

- Configure PPP commands on both dialer and physical interfaces to ensure reliable PPP link negotiation.
- Similar to the **dialer threshold 0** command, the **ppp mp min-bind** command voids the **dialer timer idle** command. When it is configured, the router does not look at traffic size to bring up links for MP bundling or tear down links that have been brought up.

When the three commands, **ppp mp min-bind**, **dialer threshold**, and **ppp mp max-bind**, are configured, the router performs MP bundling as follows:

1) Bring up a minimum number of links depending on the setting of the **ppp mp min-bind** command.
2) If traffic size exceeds the link load threshold set by the **dialer threshold** command still, bring up the next idle link. This process continues until the number of links reaches the upper limit set by the **ppp mp max-bind** command or traffic size decreases below the specified link load threshold.

1.2.5 Configuring PPP Callback

When configuring PPP callback, one endpoint of a connection should be configured as client, and the other endpoint as server. The calling party is the callback client and the called party is the callback server. The client first originates a call, and the server determines whether to originate a return call. If it determines to do that, the callback server disconnects and then originates a return call according to the information such as user name or callback number.

🕮 **Note:**

- Configure PPP callback after completing the basic configuration of C-DCC or RS-DCC.
- PPP callback implementation requires authentication. The users are recommended to configure PAP or CHAP authentication on both the physical and dialer interfaces on both the callback client and server.

I. Configuring PPP callback in the C-DCC implementation

1) Configure PPP callback client in the C-DCC implementation

As a callback client, a router can originate calls to the remote end (which can be a router or Windows NT server having the PPP callback server function), and receive the return calls from the remote end.

Use **local-user** in system view and **password** in local user view to configure a username and password, and perform other configurations in dial interface (physical or dialer interface) view.

Table 1-16 Implement PPP callback (client configuration) in C-DCC

Operation	Command
Set the link layer protocol of the interface to PPP	**link-protocol ppp**

Operation	Command
Configure the local end to send the username and password for PAP authentication	**ppp pap local-user** *username* **password** { **cipher** | **simple** } *password*
Configure the local user name sent to the remote end for CHAP authentication	**ppp chap user** *username*
Configure the password that the local end will send to the remote end for CHAP authentication	**ppp chap password** { **cipher** | **simple** } *password*
Configure the username of the remote end that is allowed to dial in	**local-user** *username*
Configure a password for the remote end that is allowed to dial in	**password** { **cipher** | **simple** } *password*
Configure the local end to be the PPP callback client	**ppp callback client**
Disable the local end to be the PPP callback client	**undo ppp callback client**
Configure the destination addresses and dial number(s) for calling one (or more) remote ends	**dialer route** *protocol next-hop-address* [**mask** *network-mask-length*] *dial-number* [**autodial**]
Configure the dial number for a Windows NT server to originate return calls to the router	**ppp callback ntstring** *dial-number*
Delete the dial number that a Windows NT server needs for placing return calls to the router	**undo ppp callback ntstring**

By default, callback is disabled and no Windows NT server callback dial number is configured.

2) Configure the PPP callback server in the C-DCC implementation

The callback server can originate a return call according to either the network address configured in the **dialer route** command (PPP authentication must be configured in this case), or the dial number configured in the **service-type ppp** command. Therefore, the user must configure either method in the **dialer callback-center** command for placing the return call.

The user should configure the callback client user name in the **dialer route** command, so that the callback server can authenticate whether a calling party is a legal callback user when receiving its call requesting callback.

Use the **service-type ppp** command to configure the callback user and callback dial number in local user view, and perform other configurations in dial interface (physical or dialer interface) view.

Table 1-17 Implement PPP callback (server configuration) in C-DCC

Operation	Command
Set the link layer protocol of the interface to PPP	**link-protocol ppp**
Configure an authentication mode	**ppp authentication-mode** { **pap** | **chap** }
Configure the user name that the local end will send to the remote end for CHAP authentication	**ppp chap user** *username*
Configure the password that the local end will send to the remote end for CHAP authentication	**ppp chap password** { **cipher** | **simple** } *password*
Configure the callback user and callback number	**service-type ppp** [**callback-nocheck | callback-number** *callback-number* | **call-number** *call-number* [*subcall-number*]]
Configure the local end to be the PPP callback server	**ppp callback server**
Disable the local end to be the PPP callback server	**undo ppp callback server**
Configure the PPP callback reference	**dialer callback-center** [**user**] [**dial-number**]
Disable the callback server function of the router	**undo dialer callback-center**
Configure the destination address(es) and dial number(s) for calling one (or more) remote ends	**dialer route** *protocol next-hop-address* [**mask** *network-mask-length*] *dial-number* **autodial**

By default, the system does not enable the callback function. Once it is enabled, the server will originate return calls according to the user name configured in the **dialer route** command.

Note:

If the callback client adopts the dynamically assigned network address, the server will be unable to use the **dialer route** command to configure a callback dial number to associate with the network address. In this case, the callback client can only use the **service-type ppp** command to configure a callback dial number to associate with the callback user name, and hence determine the callback reference.

II. Configuring PPP callback in the RS-DCC implementation

1) Configure the PPP callback client in the RS-DCC implementation

As a callback client, a router can originate calls to the remote end (which can be a router or Windows NT server having the PPP callback server function), and receive the return calls from the remote end.

When RS-DCC are used to implement PPP callback, the PPP authentication configuration at client end is the same as that of C-DCC, except that the client in RS-DCC implementation must use the **dialer number** command to configure a dial number. Refer to section 1.2.5 I. 1) “Configure PPP callback client in the C-DCC implementation”.

Perform the following configuration in dialer interface view.

Table 1-18 Implement PPP callback (client configuration) in RS-DCC

Operation	Command
Configure the local end to be the PPP callback client	**ppp callback client**
Disable the local end to be the PPP callback client	**undo ppp callback client**
Configure the dialer number for calling a remote end	**dialer number** *dial-number*
Configure the dial number for a Windows NT server to originate return calls to the router	**ppp callback ntstring** *dial-number*
Delete the dial number that a Windows NT server needs for placing return calls to the router	**undo ppp callback ntstring**

By default, callback is disabled and no Windows NT server callback dial number is configured.

2) Configure the PPP callback server in the RS-DCC implementation

When RS-DCC are adopted to implement PPP callback, the PPP authentication configuration at server end is the same as that of C-DCC, except that the server in the RS-DCC implementation can only originate a return call according to the dial number configured in the **service-type ppp** command. Refer to the section “Configure the PPP callback server in the C-DCC implementation” in *Operation Manual – Dial-up*.

Use **local-user** in system view and **service-type ppp** in local user view to configure the callback user and callback dial number, and perform other configurations in dialer interface view.

Table 1-19 Implement PPP callback (server configuration) in RS-DCC

Operation	Command
Configure a callback PPP user	**local-user** *username*
Configure the callback number of the PPP user	**service-type ppp callback-number** *callback-number*
Configure the local end to be the PPP callback server	**ppp callback server**
Disable the local end to be the PPP callback server	**undo ppp callback server**
Configure the PPP callback reference	**dialer callback-center dial-number**
Disable the callback server function of the router	**undo dialer callback-center**

By default, the system does not enable the callback function.

III. Configuring local authentication of PPP callback

Callback users can be authenticated not only by username/password but also by callback number.

Table 1-20 Configure local user authentication for PPP callback

Operation	Command
Configure a username	**local-user** *username*
Remove a user	**undo local-user** *username*
Configure the password	**password** { **simple** | **cipher** } *password*
Cancel the password	**undo password**
Configure user callback authentication	**service-type ppp callback-nocheck**
Cancel user callback authentication	**undo service-type ppp callback-nocheck**
Configure the callback attribute	**service-type ppp call-number** *call-number* [*subcall-number*]
Delete the callback attribute	**undo service-type ppp call-number** *call-number* [*subcall-number*]

By default, neither callback number nor authentication is set.

1.2.6 Configuring ISDN Caller Identification Callback

In an ISDN environment, implementing DCC callback through the ISDN caller identification function requires no authentication, nor are there other configurations requirements.

I. Features of ISDN caller Identification callback

1) In the applications of ISDN caller Identification callback, the callback server can process an incoming call in three ways, depending on the matching result of the calling number and the dialer call-in command at the local end:

- Denies the incoming call: The **dialer call-in** command has been configured, but no match is found for the dial-in number and the configured dialer callers.
- Accepts the incoming call: The **dialer call-in** command is not configured, or a match is found for the dial-in number and a **dialer call-in** command configured without the keyword "**callback**".
- Calls back: The **dialer call-in** command has been configured, and a match is found for the dial-in number and a **dialer call-in callback** command.

2) The match for the incoming number and the dialer call-in commands is determined on the basis of right-most matching. The character "*" in the number represents any characters. If multiple dialer call-in commands match the incoming number, the following rules will apply for determining the best match:

- Primary rule: The best match is the number with the fewest "*".
- Secondary rule: The best match is the one that is found first.

3) Confirm the dialer call-in at server end is associated with the incoming call

- In C-DCC, upon receiving an incoming call, the server searches for the **dialer call-in** matching the incoming number in the **dialer call-in** commands configured on the physical interface or the dialer interface to which the physical interfaces belongs.
- In RS-DCC, upon receiving an incoming call, the server searches for the **dialer call-in** matching the incoming number in the dialer interfaces to which the physical interface belongs.

II. Implementing ISDN caller identification callback in the C-DCC

1) Implement ISDN caller identification callback client in the C-DCC

Perform the following configuration in dial interface (physical or dialer interface) view.

Table 1-21 Implement ISDN caller identification callback (client configuration)

Operation	Command
Configure the destination addresses and dial number(s) for calling one (or more) remote ends	**dialer route** *protocol next-hop-address* [**mask** *network-mask-length*] *dial-number* [**autodial**]

2) Implement the ISDN caller identification callback server in the C-DCC

Perform the following configuration in dial interface (physical or dialer interface) view.

Table 1-22 Implement ISDN caller identification callback (server configuration)

Operation	Command
Configure the local end to implement ISDN callback according to the ISDN caller identification	**dialer call-in** *remote-number* [**callback**]
Disable the local end to implement ISDN callback according to the ISDN caller identification	**undo dialer call-in** *remote-number* [**callback**]
Configure the destination address(es) and dial number(s) for calling one (or more) remote ends	**dialer route** *protocol next-hop-address* [**mask** *network-mask-length*] *dial-number* [**autodial**]

By default, callback according to ISDN caller identification is not configured.

Note:

The **dialer route** command configured on the dial interface (physical or dialer) at the server should be exactly the same **dialer route** in the dial-in dialer number.

III. Implementing ISDN caller identification callback in the RS-DCC

1) Implement ISDN caller identification callback client in the RS-DCC

Perform the following configuration in dialer interface view.

Table 1-23 Implement ISDN caller identification callback (client configuration) in RS-DCC

Operation	Command
Configure the dial number for calling a remote end	**dialer number** [*dial-number*]

2) Implement the ISDN caller identification callback server in the RS-DCC

Perform the following configuration in dialer interface view.

Table 1-24 Implement ISDN caller identification callback (server configuration) in RS-DCC

Operation	Command
Configure the local end to implement ISDN callback according to the ISDN caller identification	**dialer call-in** *remote-number* [**callback**]
Disable the local end to implement ISDN callback according to the ISDN caller identification	**undo dialer call-in** *remote-number* [**callback**]
Configure the dialer number for calling a remote end	**dialer number** [*dial-number*]

By default, callback according to ISDN caller identification is not configured.

Note:

A dialer number should be configured on the dialer interface at server end through the **dialer number** command, but it is not required to be exactly the same as the dial-in dialer number.

1.2.7 Configuring Dialer Route (Advanced)

I. Configuring dialer-route logical interfaces for backup

After finishing basic dial-up configurations, you can configure dialer-route logical interfaces for backup. To this end, you must first create a logical channel interface, and then associate it with the dialer-route logical channel by using the **dialer route logical-channel** command on the dial-up interface.

Perform the following configuration beginning in system view.

Table 1-25 Associate a logical channel interface with a dialer-route logical channel

Operation	Command
Create a logical channel interface in system view	**interface logic-channel** *logic-channel-number*
Associate the dialer-route logical channel with the created logical channel interface (in physical dial-up interface)	**dialer route** *protocol next-hop-address* [**user** *hostname*] [**broadcast**] [*dial-number*] [**auto-dial**] **logical-channel** *logic-channel-number*

For more information, refer to the “Reliability” part of this manual.

II. Specifying a physical interface for placing/receiving calls

When multiple physical interfaces are assigned to a dialer interface and their dial-up links are connected to different ISDN switches, you need to associate dial-up numbers with physical interfaces. This configuration is intended for dialer interfaces only and is not available with RS-DCC.

Table 1-26 Specify the physical interface for placing/receiving calls

Operation	Command
Specify the physical interface for placing/receiving calls	**dialer route** *protocol next-hop-address* [**mask** *network-mask-length*] [**user** *hostname*] [**broadcast**] [*dial-number*] [**auto-dial**] **interface** *interface-type interface-number*
Remove a dialer route	**undo dialer route** *protocol next-hop-address* [**mask** *network-mask-length*]

1.2.8 Configuring Special DCC Functions

I. Configuring ISDN leased line

This function can only be used with C-DCC and must be implemented after C-DCC has been configured. ISDN leased line application is fulfilled through establishing semi permanent ISDN MP connections. Such application requires that a leased line has been established on the PBX of the telecommunication service provider and has been connected to the remote device.

Perform the following configuration in dial interface (ISDN BRI or PRI interface) view.

Table 1-27 Configure ISDN leased line for C-DCC

Operation	Command
Configure a B channel for ISDN leased line connection	**dialer isdn-leased** *number*
Delete the B channel for ISDN leased line connection	**undo dialer isdn-leased** *number*

By default, no B channel is configured for ISDN leased line connection.

ISDN BRI interfaces support both 64 kbps leased lines and 128 kbps leased lines. For more information, refer to the chapter discussing ISDN configuration in the “Line Layer Protocol” part of this manual.

II. Configuring auto-dial

This function can only be used with C-DCC. With a C-DCC, after the router is started, the DCC will automatically attempt to dial the remote end of the connection without requiring a triggering packet. If a normal connection cannot be established with the remote end, DCC will automatically retry at a certain interval. Compared with the auto-dial DCC triggered by packets, such connections do not automatically disconnect due to timeout. In other words, the **dialer timer idle** command does not take effect on auto-dial.

Perform the following configuration in dial interface (physical or dialer interface) view.

Table 1-28 Configure auto-dial

Operation	Command
Configure one (or more) remote destination address(es) and dialer number(s) that the router will auto-dial	**dialer route** *protocol next-hop-address* [**mask** *network-mask-length*] *dialer-number* **autodial**
Configure an auto-dial interval	**dialer timer autodial** *seconds*
Restore the default auto-dial interval	**undo dialer timer autodial**

By default, auto-dial is not configured. If auto-dial function is enabled, the interval for auto-dial defaults to 300 seconds.

III. Configuring dialer number circular standby

This function can only be used with C-DCC. When setting the same destination addresses using C-DCC, multiple **dialer route** commands can be configured, these commands corresponding to different dialer numbers. These **dialer route** commands form a kind of circular standby, i.e., which means that if the calling dial number can not connect to peer end, then the number configured in next **dialer route** command will be selected automatically for re-calling.

Perform the following configuration in dial interface (physical or dialer interface) view.

Table 1-29 Configure dialer number circular standby

Operation	Command
Configure one remote destination address(es) and dialer number(s)	**dialer route** *protocol next-hop-address* [**mask** *network-mask-length*] *dial-number* **autodial**

1.2.9 Configuring Attributes of DCC Dial Interface

C-DCC and RS-DCC also have some optional parameters. Flexibly configuring these parameters can improve DCC efficiency, and hence satisfies various requirements.

DCC dial interface attributes configuration overs the process to:

- Configure the link idle time
- Configure the link disconnection time before initiating the next call
- Configure the link idle time when interface completion
- Configure the timeout of call setting up
- Configure the buffer queue length of the dial interface

I. Configuring the link idle time

In the case that a dial interface originates a call, if the line is idle for an amount of time, DCC will disconnect the line. The idle time means that in the duration of it no packet in the ACL conforms to the "permit" rule and needs to be transferred.

Perform the following configuration in dial interface (physical or dialer interface) view.

Table 1-30 Configure the link idle time

Operation	Command
Configure the link idle time	**dialer timer idle** *seconds*
Restore the link idle time to the default value	**undo dialer timer idle**

By default, the link idle time is 120 seconds.

🕮 **Note:**

Modified idle timer value does not take effect if the link has been set up. It takes effect only when the link is set up again for the next call.

II. Configuring the link disconnection time before initiation of the next call

After a line for DCC calls enters the down status due to faults or disconnection, a specified period of time must be elapsed (the interval before it can originate the next call) before a new dialup connection can be established again. Thereby, the possibility of overloading the remote PBX can be prevented.

Perform the following configuration in dial interface (physical or dialer interface) view.

Table 1-31 Configure the link disconnection time before initiating the next call

Operation	Command
Configure the link disconnection time before initiating the next call	**dialer timer enable** *seconds*
Restore the link disconnection time before initiating the next call to the default value	**undo dialer timer enable**

By default, the link disconnection time is 5 seconds.

III. Configuring the link idle time upon interface competition

If all the channels are unavailable when DCC originates a new call, a condition of contention occurs. This suggests that the network is very busy. Normally, after a line is set up, idle-timeout timer will take effect. However, if a call to a different destination address is originated at this time, competition will occur. In this case, DCC replaces the idle timeout timer with the compete-idle timer. In other words, the line will be automatically disconnected after the line-idle time exceeds the time specified by the compete-idle timer.

Perform the following configuration in dial interface (physical or dialer interface) view.

Table 1-32 Configure the link idle time upon interface competition

Operation	Command
Configure the link idle time upon interface competition	**dialer timer compete** *seconds*
Restore the link idle time upon interface competition to the default value	**undo dialer timer compete**

By default, the link idle time is 20 seconds when interface competition occurs.

IV. Configuring the timeout of call setting up

When placing DCC calls to some remote ends, the intervals between originating the calls and establishing the connections are not the same. To effectively control the time that should wait for the connection after a call is originated, the user can configure the wait-carrier timer to specify duration, after which DCC will terminate the call if the connection cannot be established.

Perform the following configuration in dial interface (physical or dialer interface) view.

Table 1-33 Configure the timeout of call setting up

Operation	Command
Configure the timeout of call setting up	**dialer timer wait-carrier** *seconds*
Restore the timeout of call setting up to the default value	**undo dialer wait-carrier**

By default, the timeout of call setting up is 60 seconds.

V. Configuring the buffer queue length of the dialer

Before a dialer buffer queue is established, a packet received from the dial interface will be discarded if the connection is not established yet. However, if a buffer queue is established on the dial interface, the packet will be stored until a connection is established rather than discarded.

Perform the following configuration in dial interface (physical or dialer interface) view.

Table 1-34 Configure the buffer queue length of the dial interface

Operation	Command
Configure the buffer queue length of the dial interface	**dialer queue-length** *packets*
Remove the buffer queue length of the dial interface	**undo dialer queue-length**

By default, no buffer queues are configured on dial interfaces.

VI. Setting the warmup timer of the dial-up backup function

Perform the following configuration in system view.

Table 1-35 Set the warmup timer of the dial-up backup function

Operation	Command
Set the length of the warmup timer on the router configured with the dial-up backup function	**dialer timer warmup** *seconds*
Restore the default	**undo dialer timer warmup**

By default, the length of the timer is 30 seconds.

1.2.10 Configuring Traffic Statistic Interval

Perform the following configuration in system view.

Table 1-36 Configure flow-control

Operation	Command
Configure traffic statistic interval	**flow-interval** *interval*
Restore the default traffic statistic interval	**undo flow-interval**

Traffic statistic interval defaults to 20 seconds.

1.2.11 Clearing Dial-Up Links

Execute the following command in any view.

Table 1-37 Clear a dial-up link

Operation	Command
Clear a dial-up link or the session link on the specified interface at the PPPoE/PPPoA client	**dialer disconnect interface** [*interface-type interface-number*]

1.3 DCC Display and Debug

After completing the above configuration steps, execute the **display** command in all views to display the running of the DCC configuration, and to verify the effect of the configuration.

Execute the **debugging** command in user view for the debugging.

Table 1-38 Display and debug DCC

Operation	Command
Display the dial interface information	**display dialer** [**interface** *interface-type interface-number*]
Enable DCC debugging	**debugging dialer** { **all** | **event** | **packet** }

1.4 DCC Configuration Example

1.4.1 DCC Applications in Common Use

I. Network requirements

RouterA can call RouterB and RouterC via multiple interfaces. Likewise, RouterB and RouterC can respectively call RouterA. However, RouterB and RouterC cannot call each other.

As shown in the following figure, when C-DCC is used, the addresses of RouterA, RouterB and RouterC are on the same segment. In this case, 100.1.1.1, 100.1.1.2, and 100.1.1.3 are the addresses respectively for RouterA, RouterB and RouterC. When RS-DCC is used, the addresses of RouterA and RouterB are on the same segment, so are the addresses of RouterA and RouterC. The addresses of the interfaces Dialer0 and Dialer1 on RouterA are respectively 100.1.1.1 and 122.1.1.1. The address of the Dialer0 on RouterB is 100.1.1.2, and that of the Dialer0 on RouterC is 122.1.1.2.

II. Network diagram

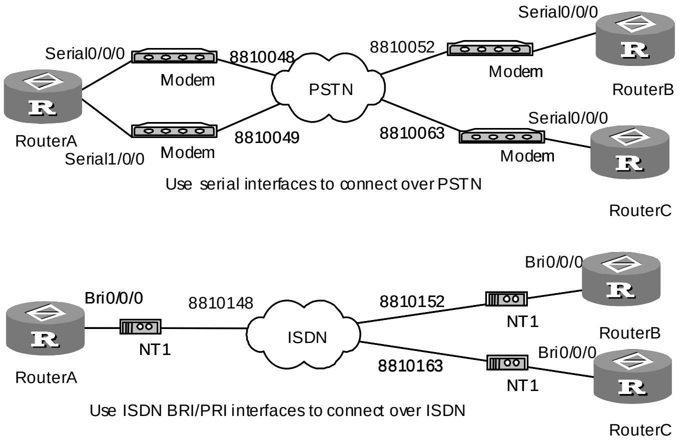


Figure 1-10 Network diagram for a common DCC application

III. Configuration procedure

Solution 1: Establish a connection via the serial interface by using C-DCC, configure the DCC parameters on the dialer interface for RouterA with the help of a dialer circular group, and directly configure the DCC parameters on the physical interfaces on RouterB and RouterC.

1) Configure RouterA

# Configure dial-up ACL.

```
[3Com] dialer-rule 1 ip permit
```

# Configure Dialer0 interface address, enable C-DCC and the DCC to the peer.

```
[3Com] interface dialer 0
[3Com-Dialer0] dialer enable-circular
[3Com-Dialer0] ip address 100.1.1.1 255.255.255.0
[3Com-Dialer0] dialer-group 1
[3Com-Dialer0] dialer route ip 100.1.1.2 8810052
[3Com-Dialer0] dialer route ip 100.1.1.3 8810063
```

# Configure the asynchronous protocol mode of Serial0/0/0 interface, using Dialer Circular group.

```
[3Com-Dialer0] interface serial 0/0/0
[3Com-Serial0/0/0] physical-mode async
[3Com-Serial0/0/0] async mode protocol
[3Com-Serial0/0/0] dialer circular-group 0
```

# Configure the asynchronous protocol mode of Serial1/0/0 interface, using Dialer Circular group.

```
[3Com-Serial0/0/0] interface serial 1/0/0
[3Com-Serial1/0/0] physical-mode async
```

```
[3Com-Serial1/0/0] async mode protocol
[3Com-Serial1/0/0] dialer circular-group 0
```

# Configure user-interface to enable dial-up mode.

```
[3Com-Serial1/0/0] user-interface tty1
[3Com-ui-tty1] modem
[3Com-ui-tty1] user-interface tty2
[3Com-ui-tty2] modem
```

2) Configure RouterB

# Configure dial-up ACL.

```
[3Com] dialer-rule 1 ip permit
```

# Configure the asynchronous dial-up mode of Serial0/0/0.

```
[3Com] interface serial 0/0/0
[3Com-Serial0/0/0] physical-mode async
[3Com-Serial0/0/0] async mode protocol
```

# Configure Dialer0 interface address, enable C-DCC and the DCC to the peer.

```
[3Com-Serial0/0/0] ip address 100.1.1.2 255.255.255.0
[3Com-Serial0/0/0] dialer enable-circular
[3Com-Serial0/0/0] dialer-group 1
[3Com-Serial0/0/0] dialer route ip 100.1.1.1 8810048
[3Com-Serial0/0/0] dialer route ip 100.1.1.1 8810049
```

# Configure user-interface to enable dial-up mode.

```
[3Com-Serial0/0/0] user-interface tty1
[3Com-ui-tty1] modem
```

3) Configure RouterC

# Configure dial-up ACL.

```
[3Com] dialer-rule 1 ip permit
```

# Configure the asynchronous dial-up mode of Serial0/0/0.

```
[3Com] interface serial 0/0/0
[3Com-Serial0/0/0] physical-mode async
[3Com-Serial0/0/0] async mode protocol
```

# Configure Dialer0 interface address, enable C-DCC and the DCC to the peer.

```
[3Com-Serial0/0/0] ip address 100.1.1.3 255.255.255.0
[3Com-Serial0/0/0] dialer enable-circular
[3Com-Serial0/0/0] dialer-group 1
[3Com-Serial0/0/0] dialer route ip 100.1.1.1 8810048
[3Com-Serial0/0/0] dialer route ip 100.1.1.1 8810049
```

# Configure user-interface to enable dial-up mode.

```
[3Com-Serial0/0/0] user-interface tty1
```

```
[3Com-ui-tty1] modem
```

Solution 2: Resource-Share DCC to setup a connection via the serial interface and configure DCC parameters on Dialer interface.

1) Configure RouterA

# Configure dial-up ACL, the local userb and userc.

```
[3Com] dialer-rule 1 ip permit
[3Com] local-user userb
[3Com-luser-userb] password simple userb
[3Com-luser-userb] service-type ppp
[3Com-luser-userb] quit
[3Com] local-user userc
[3Com-luser-userc] password simple userc
[3Com-luser-userc] service-type ppp
[3Com-luser-userc] quit
```

# Configure Dialer0 interface address and enable RS-DCC.

```
[3Com] interface dialer 0
[3Com-Dialer0] ip address 100.1.1.1 255.255.255.0
[3Com-Dialer0] undo dialer enable-circular
[3Com-Dialer0] dialer user userb
[3Com-Dialer0] dialer bundle 1
```

# Configure the users that are allowed to dial-up Dialer0 interface, PPP authentication information and the DCC to the remote end.

```
[3Com-Dialer0] dialer-group 1
[3Com-Dialer0] ppp authentication-mode pap
[3Com-Dialer0] ppp pap local-user usera password simple usera
[3Com-Dialer0] dialer number 8810052
```

# Configure Dialer1 interface address and enable RS-DCC.

```
[3Com-Dialer0] interface dialer 1
[3Com-Dialer1] ip address 122.1.1.1 255.255.255.0
[3Com-Dialer1] undo dialer enable-circular
[3Com-Dialer1] dialer user userc
[3Com-Dialer1] dialer bundle 2
```

# Configure the users that are allowed to dial-up Dialer1 interface, PPP authentication information and the DCC to the remote end.

```
[3Com-Dialer1] dialer-group 1
[3Com-Dialer1] ppp authentication-mode pap
[3Com-Dialer1] ppp pap local-user usera password simple usera
[3Com-Dialer1] dialer number 8810063
```

# Configure the asynchronous protocol mode of Serial0/0/0, PPP authentication information and the Dialer bundle to which the interface belongs.

```
[3Com-Dialer1] interface serial 0/0/0
[3Com-Serial0/0/0] physical-mode async
[3Com-Serial0/0/0] async mode protocol
[3Com-Serial0/0/0] dialer bundle-member 1
[3Com-Serial0/0/0] dialer bundle-member 2
[3Com-Serial0/0/0] link-protocol ppp
[3Com-Serial0/0/0] ppp authentication-mode pap
[3Com-Serial0/0/0] ppp pap local-user usera password simple usera
```

# Configure the asynchronous protocol mode of Serial1/0/0, PPP authentication information and the Dialer bundle to which the interface belongs.

```
[3Com-Serial0/0/0] interface serial 1/0/0
[3Com-Serial1/0/0] physical-mode async
[3Com-Serial1/0/0] async mode protocol
[3Com-Serial1/0/0] dialer bundle-member 1
[3Com-Serial1/0/0] dialer bundle-member 2
[3Com-Serial1/0/0] link-protocol ppp
[3Com-Serial1/0/0] ppp authentication-mode pap
[3Com-Serial1/0/0] ppp pap local-user usera password simple usera
```

# Configure the user-interface to enable dial-up mode.

```
[3Com-Serial1/0/0] user-interface tty1
[3Com-ui-tty1] modem
[3Com-ui-tty1] user-interface tty2
[3Com-ui-tty2] modem
```

2) Configure RouterB

# Configure dial-up ACL and the local usera.

```
[3Com] dialer-rule 2 ip permit
[3Com] local-user usera
[3Com-luser-usera] password simple usera
[3Com-luser-usera] service-type ppp
[3Com-luser-usera] quit
```

# Configure Dialer0 interface address and enable RS-DCC.

```
[3Com] interface dialer 0
[3Com-Dialer0] ip address 100.1.1.2 255.255.255.0
[3Com-Dialer0] undo dialer enable-circular
[3Com-Dialer0] dialer user usera
[3Com-Dialer0] dialer bundle 1
[3Com-Dialer0] dialer number 8810052
```

# Configure the users that are allowed to dial-up Dialer0 interface, PPP authentication information and the DCC to the remote end.

```
[3Com-Dialer0] dialer-group 2
[3Com-Dialer0] ppp authentication-mode pap
[3Com-Dialer0] ppp pap local-user userb password simple userb
```

# Configure the asynchronous protocol mode of Serial0/0/0, PPP authentication information and the Dialer bundle to which the interface belongs.

```
[3Com-Dialer0] interface serial 0/0/0
[3Com-Serial0/0/0] physical-mode async
[3Com-Serial0/0/0] async mode protocol
[3Com-Serial0/0/0] dialer bundle-member 1
[3Com-Serial0/0/0] link-protocol ppp
[3Com-Serial0/0/0] ppp authentication-mode pap
[3Com-Serial0/0/0] ppp pap local-user userb password simple usera
```

# Configure the user-interface to enable dial-up mode.

```
[3Com-Serial0/0/0] user-interface tty1
[3Com-ui-tty1] modem
```

3) Configure RouterC

# Configure dial-up ACL and the local usera.

```
[3Com] dialer-rule 1 ip permit
[3Com] local-user usera
[3Com-luser-usera] password simple usera
[3Com-luser-usera] service-type ppp
[3Com-luser-usera] quit
```

# Configure Dialer0 interface address and enable RS-DCC.

```
[3Com] interface dialer 0
[3Com-Dialer0] ip address 122.1.1.2 255.255.255.0
[3Com-Dialer0] undo dialer enable-circular
[3Com-Dialer0] dialer user usera
[3Com-Dialer0] dialer bundle 1
[3Com-Dialer0] dialer number 8810049
```

# Configure the users that are allowed to dial-up Dialer0 interface, PPP authentication information and the DCC to the remote end.

```
[3Com-Dialer0] dialer-group 1
[3Com-Dialer0] ppp authentication-mode pap
[3Com-Dialer0] ppp pap local-user userc password simple userc
```

# Configure the asynchronous protocol mode of Serial0/0/0, PPP authentication information and the Dialer bundle to which the interface belongs.

```
[3Com-Dialer0] interface serial 0/0/0
```

```
[3Com-Serial0/0/0] physical-mode async
[3Com-Serial0/0/0] async mode protocol
[3Com-Serial0/0/0] dialer bundle-member 1
[3Com-Serial0/0/0] link-protocol ppp
[3Com-Serial0/0/0] ppp authentication-mode pap
[3Com-Serial0/0/0] ppp pap local-user userc password simple userc
```

# Configure the user-interface to enable dial-up mode.

```
[3Com-Serial0/0/0] user-interface tty1
[3Com-ui-tty1] modem
```

Solution 3: Use C-DCC to set up a connection vial ISDN BRI or PRI and configure DCC parameters on the physical interface.

1) Configure RouterA

# Configure dial-up ACL.

```
[3Com] dialer-rule 1 ip permit
```

# Configure Bri0/0/0 interface address, enable C-DCC and the DCC to the remote end.

```
[3Com] interface bri 0/0/0
[3Com-Bri0/0/0] ip address 100.1.1.1 255.255.255.0
[3Com-Bri0/0/0] dialer enable-circular
[3Com-Bri0/0/0] dialer-group 1
[3Com-Bri0/0/0] dialer route ip 100.1.1.2 8810052
[3Com-Bri0/0/0] dialer route ip 100.1.1.3 8810063
```

2) Configure RouterB

# Configure dial-up ACL.

```
[3Com] dialer-rule 2 ip permit
```

# Configure Bri0/0/0 interface address, enable C-DCC and the DCC to the remote end.

```
[3Com] interface bri 0/0/0
[3Com-Bri0/0/0] ip address 100.1.1.2 255.255.255.0
[3Com-Bri0/0/0] dialer enable-circular
[3Com-Bri0/0/0] dialer-group 2
[3Com-Bri0/0/0] dialer route ip 100.1.1.1 8810048
```

3) Configure RouterC

# Configure dial-up ACL.

```
[3Com] dialer-rule 1 ip permit
```

# Configure Bri0/0/0 interface address, enable C-DCC and the DCC to the remote end.

```
[3Com] interface bri 0/0/0
[3Com-Bri0/0/0] ip address 100.1.1.3 255.255.255.0
[3Com-Bri0/0/0] dialer enable-circular
[3Com-Bri0/0/0] dialer-group 1
```

```
[3Com-Bri0/0/0] dialer route ip 100.1.1.1 8810048
```

Solution 4: Resource-Share DCC to setup a connection via ISDN BRI or PRI, and configure DCC parameters on Dialer interface.

1) Configure RouterA

# Configure dial-up ACL, local userb and userc.

```
[3Com] dialer-rule 1 ip permit
[3Com] local-user userb
[3Com-luser-userb] password simple userb
[3Com-luser-userb] service-type ppp
[3Com-luser-userb] quit
[3Com] local-user userc
[3Com-luser-userc] password simple userc
[3Com-luser-userc] service-type ppp
[3Com-luser-userc] quit
```

# Configure Dialer0 interface address and enable RS-DCC.

```
[3Com] interface dialer 0
[3Com-Dialer0] ip address 100.1.1.1 255.255.255.0
[3Com-Dialer0] undo dialer enable-circular
[3Com-Dialer0] dialer user userb
[3Com-Dialer0] dialer bundle 1
```

# Configure the users that are allowed to dial-up Dialer0 interface, PPP authentication information and the DCC to the remote end.

```
[3Com-Dialer0] dialer-group 1
[3Com-Dialer0] ppp authentication-mode pap
[3Com-Dialer0] ppp pap local-user usera password simple usera
[3Com-Dialer0] dialer number 8810152
```

# Configure Dialer1 interface address and enable RS-DCC.

```
[3Com-Dialer0] interface dialer 1
[3Com-Dialer1] ip address 122.1.1.1 255.255.255.0
[3Com-Dialer1] undo dialer enable-circular
[3Com-Dialer1] dialer user userc
[3Com-Dialer1] dialer bundle 2
```

# Configure the users that are allowed to dial-up Dialer1 interface, PPP authentication information and the DCC to the remote end.

```
[3Com-Dialer1] dialer-group 1
[3Com-Dialer1] ppp authentication-mode pap
[3Com-Dialer1] ppp pap local-user usera password simple usera
[3Com-Dialer1] dialer number 8810163
```

# Configure Bri0/0/0 PPP authentication information and the Dialer bundle to which the interface belongs.

```
[3Com-Dialer1] interface bri 0/0/0
[3Com-Bri0/0/0] undo dialer enable-circular
[3Com-Bri0/0/0] dialer bundle-member 1
[3Com-Bri0/0/0] dialer bundle-member 2
[3Com-Bri0/0/0] link-protocol ppp
[3Com-Bri0/0/0] ppp authentication-mode pap
[3Com-Bri0/0/0] ppp pap local-user usera password simple usera
```

2) Configure RouterB:

# Configure dial-up ACL and local usera.

```
[3Com] dialer-rule 2 ip permit
[3Com] local-user usera
[3Com-luser-usera] password simple usera
[3Com-luser-usera] service-type ppp
[3Com-luser-usera] quit
```

# Configure Dialer0 interface address and enable RS-DCC.

```
[3Com] interface dialer 0
[3Com-Dialer0] ip address 100.1.1.2 255.255.255.0
[3Com-Dialer0] undo dialer enable-circular
[3Com-Dialer0] dialer user usera
[3Com-Dialer0] dialer bundle 1
[3Com-Dialer0] dialer number 8810148
```

# Configure the users that are allowed to dial-up Dialer0 interface, PPP authentication information and the DCC to the remote end.

```
[3Com-Dialer0] dialer-group 2
[3Com-Dialer0] ppp authentication-mode pap
[3Com-Dialer0] ppp pap local-user userb password simple userb
```

# Configure Bri0/0/0 PPP authentication information and the Dialer bundle to which the interface belongs.

```
[3Com-Dialer0] interface bri 0/0/0
[3Com-Bri0/0/0] undo dialer enable-circular
[3Com-Bri0/0/0] dialer bundle-member 1
[3Com-Bri0/0/0] link-protocol ppp
[3Com-Bri0/0/0] ppp authentication-mode pap
[3Com-Bri0/0/0] ppp pap local-user usera password simple usera
```

3) Configure RouterC

# Configure dial-up ACL and local usera.

```
[3Com] dialer-rule 1 ip permit
[3Com] local-user usera
```

```
[3Com-luser-usera] password simple usera
[3Com-luser-usera] service-type ppp
[3Com-luser-usera] quit
```

# Configure Dialer0 interface address and enable RS-DCC.

```
[3Com] interface dialer 0
[3Com-Dialer0] ip address 122.1.1.2 255.255.255.0
[3Com-Dialer0] undo dialer enable-circular
[3Com-Dialer0] dialer user usera
[3Com-Dialer0] dialer bundle 1
[3Com-Dialer0] dialer number 8810148
```

# Configure the users that are allowed to dial-up Dialer0 interface, PPP authentication information and the DCC to the remote end.

```
[3Com-Dialer0] dialer-group 1
[3Com-Dialer0] ppp authentication-mode pap
[3Com-Dialer0] ppp pap local-user userc password simple userc
```

# Configure Bri0/0/0 PPP authentication information and the Dialer bundle to which the interface belongs.

```
[3Com-Dialer0] interface bri 0/0/0
[3Com-Bri0/0/0] undo dialer enable-circular
[3Com-Bri0/0/0] dialer bundle-member 1
[3Com-Bri0/0/0] link-protocol ppp
[3Com-Bri0/0/0] ppp authentication-mode pap
[3Com-Bri0/0/0] ppp pap local-user usera password simple usera
```

1.4.2 DCC Application Providing MP Binding

I. Network requirements

The local router is connected to the remote end via two ISDN BRI interfaces. It is required to set the traffic threshold to distribute the traffic. Thus, the bandwidth resources can be allocated according to the actual traffic. The maximum available bandwidth is specified.

As shown in the following figure, the ISDN BRI interfaces on RouterA and the ISDN PRI interface on RouterB are connected through an ISDN network. RouterA is required to adopt RS-DCC to call RouterB, and RouterB adopts C-DCC to call RouterA. The addresses of RouterA and RouterB are respectively 100.1.1.1 and 100.1.1.2.

II. Network diagram

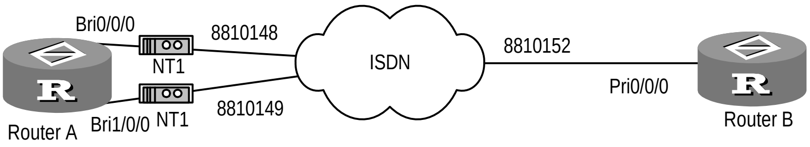


Figure 1-11 Network for the DCC application providing MP binding

III. Configuration procedure

1) Configure RouterA

# Configure the dial-up ACL, local user userb, and flow control interval.

```
[3Com] dialer-rule 1 ip permit
[3Com] local-user userb
[3Com-luser-userb] password simple userb
[3Com-luser-userb] service-type ppp
[3Com-luser-userb] quit
[3Com] flow-interval 3
```

# Configure the address of interface Dialer0, enable RS-DCC and MP bundling.

```
[3Com] interface dialer 0
[3Com-Dialer0] ip address 100.1.1.1 255.255.255.0
[3Com-Dialer0] undo dialer enable-circular
[3Com-Dialer0] dialer user userb
[3Com-Dialer0] dialer bundle 1
[3Com-Dialer0] ppp mp
[3Com-Dialer0] dialer threshold 50
```

# Configure the users that are allowed to dial-up Dialer0 interface, PPP authentication information and the DCC to the remote end.

```
[3Com-Dialer0] dialer-group 1
[3Com-Dialer0] ppp authentication-mode pap
[3Com-Dialer0] ppp pap local-user usera password simple usera
[3Com-Dialer0] dialer number 8810152
```

# Configure Bri0/0/0 PPP authentication information and the Dialer bundle to which the interface belongs.

```
[3Com-Dialer0] interface bri 0/0/0
[3Com-Bri0/0/0] undo dialer enable-circular
[3Com-Bri0/0/0] dialer bundle-member 1
[3Com-Bri0/0/0] ppp mp
[3Com-Bri0/0/0] link-protocol ppp
[3Com-Bri0/0/0] ppp authentication-mode pap
[3Com-Bri0/0/0] ppp pap local-user usera password simple usera
```

# Configure Bri1/0/0 PPP authentication information and the Dialer bundle to which the interface belongs.

```
[3Com-Bri0/0/0] interface bri 1/0/0
[3Com-Bri1/0/0] undo dialer enable-circular
[3Com-Bri1/0/0] dialer bundle-member 1
[3Com-Bri1/0/0] ppp mp
[3Com-Bri1/0/0] link-protocol ppp
[3Com-Bri1/0/0] ppp authentication-mode pap
[3Com-Bri1/0/0] ppp pap local-user usera password simple usera
```

2) Configure RouterB

# Configure the dial-up ACL, local user usera, and flow control interval.

```
[3Com] dialer-rule 2 ip permit
[3Com] local-user usera
[3Com-luser-usera] password simple usera
[3Com-luser-usera] service-type ppp
[3Com-luser-usera] quit
[3Com] flow-interval 3
```

# Configure the address of the interface Dialer 0, the dial string to the remote end, MP bundling, and PPP authentication.

```
[3Com] interface dialer 0
[3Com-Dialer0] ip address 100.1.1.2 255.255.255.0
[3Com-Dialer0] dialer enable-circular
[3Com-Dialer0] dialer route ip 100.1.1.1 8810148
[3Com-Dialer0] dialer route ip 100.1.1.1 8810149
[3Com-Dialer0] ppp mp
[3Com-Dialer0] ppp authentication-mode pap
[3Com-Dialer0] ppp pap local-user userb password simple userb
```

# Configure the interface Serial0/0/0:15.

```
[3Com] controller e1 0/0/0
[3Com-E1-0/0/0] pri-set
[3Com-E1-0/0/0] interface serial 0/0/0:15
```

# Enable C-DCC and associate with the interface Dialer 0.

```
[3Com-Serial0/0/0:15] dialer enable-circular
[3Com-Serial0/0/0:15] dialer circular-group 0
[3Com-Serial0/0/0:15] dialer-group 2
```

# Configure information on MP and PPP authentication on the interface Serial0/0/0:15.

```
[3Com-Serial0/0/0:15] link-protocol ppp
[3Com-Serial0/0/0:15] ppp mp
[3Com-Serial0/0/0:15] ip address 100.1.1.2 255.255.255.0
[3Com-Serial0/0/0:15] ppp authentication-mode pap
```

```
[3Com-Serial0/0/0:15] ppp pap local-user userb password simple userb
```

1.4.3 DCC Application Using ISDN BRI Interface to Dial and Providing Leased Line

I. Network requirements

To implement C-DCC, use a B channel on the ISDN BRI interface to provide a leased line, and another B channel to implement remote dialing connection.

As shown in the following figure, the B2 channel on the interface Bri0/0/0 of RouterA is connected to the B1 channel on the interface Bri0/0/0 of RouterC to provide a leased line, whereas the B1 channel is connected to RouterB through dialup.

In the ISDN network, configure on the switches connected to RouterA and RouterC a semipermanent connection from 8810148 to 8810152, ensuring that both RouterA and RouterC can set up virtual circuit connections to the ISDN network. RouterA adopts C-DCC to call RouterB and RouterC, so do RouterB and RouterC. The addresses of RouterA, RouterB and RouterC are respectively 100.1.1.1, 100.1.1.2, and 100.1.1.3.

II. Network diagram

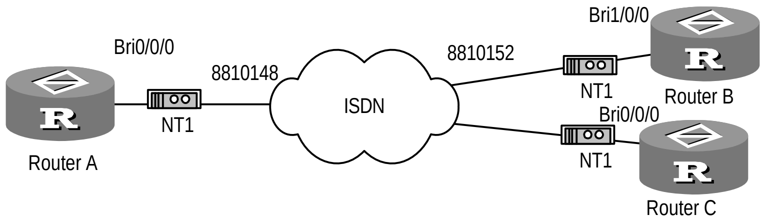


Figure 1-12 DCC using the ISDN BRI interface to provide dial and a leased line simultaneously

III. Configuration procedure

1) Configure RouterA

```
[3Com] dialer-rule 1 ip permit
[3Com] interface bri 0/0/0
[3Com-Bri0/0/0] ip address 100.1.1.1 255.255.255.0
[3Com-Bri0/0/0] dialer enable-circular
[3Com-Bri0/0/0] dialer isdn-leased 1
[3Com-Bri0/0/0] dialer-group 1
[3Com-Bri0/0/0] dialer route ip 100.1.1.2 8810152
```

2) Configure RouterB

```
[3Com] dialer-rule 2 ip permit
[3Com] interface bri 1/0/0
[3Com-Bri1/0/0] ip address 100.1.1.2 255.255.255.0
[3Com-Bri1/0/0] dialer enable-circular
```

```
[3Com-Bri1/0/0] dialer-group 2
[3Com-Bri1/0/0] dialer route ip 100.1.1.1 8810148
```

3) Configure RouterC

```
[3Com] dialer-rule 1 ip permit
[3Com] interface bri 0/0/0
[3Com-Bri0/0/0] ip address 100.1.1.3 255.255.255.0
[3Com-Bri0/0/0] dialer enable-circular
[3Com-Bri0/0/0] dialer isdn-leased 0
[3Com-Bri0/0/0] dialer-group 1
[3Com-Bri0/0/0] dialer route ip 100.1.1.1 8810148
```

1.4.4 Router-to-Router Callback for DCC

I. Network requirements

Two routers realize PPP callback via the serial interfaces across PSTN, and ISDN callback with the ISDN caller identification technique across ISDN.

As shown in the following figure, in the C-DCC implementation, RouterA and RouterB are interconnected via the serial interfaces across PSTN, RouterC and RouterD are interconnected via ISDN BRI/PRI interfaces across ISDN. RouterA and RouterC are specified to be the callback clients, while RouterB and RouterD are callback servers. RouterA and RouterC use the same address 100.1.1.1, whereas RouterB and RouterD use the same address 100.1.1.2.

II. Network diagram

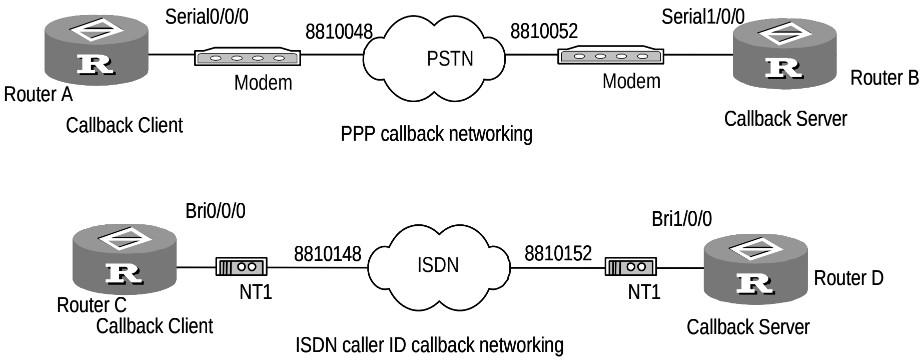


Figure 1-13 Network for the DCC application providing router-to-router callback

III. Configuration procedure

Solution 1: Use C-DCC to implement PPP callback. The server determines the callback client by the username configured by the command **dialer route**.

1) Configure RouterA

```
[3Com] dialer-rule 1 ip permit
```

```
[3Com] interface serial 0/0/0
[3Com-Serial0/0/0] ip address 100.1.1.1 255.255.255.0
[3Com-Serial0/0/0] physical-mode async
[3Com-Serial0/0/0] dialer enable-circular
[3Com-Serial0/0/0] dialer-group 1
[3Com-Serial0/0/0] dialer route ip 100.1.1.2 8810052
[3Com-Serial0/0/0] link-protocol ppp
[3Com-Serial0/0/0] ppp pap local-user usera password simple usera
[3Com-Serial0/0/0] ppp callback client
[3Com-Serial0/0/0] user-interface tty1
[3Com-ui-tty1] modem
```

2) Configure RouterB

```
[3Com] dialer-rule 2 ip permit
[3Com] local-user usera
[3Com-luser-usera] password simple usera
[3Com-luser-usera] service-type ppp
[3Com-luser-usera] quit
[3Com] interface serial 1/0/0
[3Com-Serial1/0/0] ip address 100.1.1.2 255.255.255.0
[3Com-Serial1/0/0] physical-mode async
[3Com-Serial1/0/0] async mode protocol
[3Com-Serial1/0/0] dialer enable-circular
[3Com-Serial1/0/0] dialer-group 2
[3Com-Serial1/0/0] dialer route ip 100.1.1.1 user usera 8810048
[3Com-Serial1/0/0] dialer callback-center user
[3Com-Serial1/0/0] link-protocol ppp
[3Com-Serial1/0/0] ppp authentication-mode pap
[3Com-Serial1/0/0] ppp callback server
[3Com-Serial1/0/0] user-interface tty2
[3Com-ui-tty2] modem
```

Solution 2: Use C-DCC to implement PPP callback. The server dynamically creates dialer routes and callbacks the clients according to the dialer numbers.

1) Configure RouterA

```
[3Com] dialer-rule 1 ip permit
[3Com] interface serial 0/0/0
[3Com-Serial0/0/0] ip address 100.1.1.1 255.255.255.0
[3Com-Serial0/0/0] physical-mode async
[3Com-Serial0/0/0] async mode protocol
[3Com-Serial0/0/0] dialer enable-circular
[3Com-Serial0/0/0] dialer-group 1
[3Com-Serial0/0/0] dialer route ip 100.1.1.2 8810052
[3Com-Serial0/0/0] link-protocol ppp
```

```
[3Com-Serial0/0/0] ppp pap local-user usera password simple usera
[3Com-Serial0/0/0] ppp callback client
[3Com-Serial0/0/0] user-interface tty1
[3Com-ui-tty1] modem
```

2) Configure RouterB

```
[3Com] dialer-rule 2 ip permit
[3Com] local-user usera
[3Com-luser-usera] password simple usera
[3Com-luser-usera] service-type ppp
[3Com-luser-usera] service-type ppp callback-number 8810048
[3Com-luser-usera] quit
[3Com] interface serial 1/0/0
[3Com-Serial1/0/0] ip address 100.1.1.2 255.255.255.0
[3Com-Serial1/0/0] physical-mode async
[3Com-Serial1/0/0] async mode protocol
[3Com-Serial1/0/0] dialer enable-circular
[3Com-Serial1/0/0] dialer-group 2
[3Com-Serial1/0/0] dialer route ip 100.1.1.1 user usera 8810048
[3Com-Serial1/0/0] dialer callback-center dial-number
[3Com-Serial1/0/0] link-protocol ppp
[3Com-Serial1/0/0] ppp authentication-mode pap
[3Com-Serial1/0/0] ppp callback server
[3Com-Serial1/0/0] user-interface tty2
[3Com-ui-tty2] modem
```

Solution 3: Use C-DCC to implement ISDN caller identification callback.

1) Configure RouterA

```
[3Com] dialer-rule 1 ip permit
[3Com] interface bri 0/0/0
[3Com-Bri0/0/0] ip address 100.1.1.1 255.255.255.0
[3Com-Bri0/0/0] dialer-group 1
[3Com-Bri0/0/0] dialer route ip 100.1.1.2 user usera 8810152
```

2) Configure RouterB

```
[3Com] dialer-rule 2 ip permit
[3Com] interface bri 1/0/0
[3Com-Bri1/0/0] ip address 100.1.1.2 255.255.255.0
[3Com-Bri1/0/0] dialer-group 2
[3Com-Bri1/0/0] dialer route ip 100.1.1.1 user usera 8810148
[3Com-Bri1/0/0] dialer call-in 8810148 callback
```

1.4.5 Router-to-PC Callback for DCC

I. Network requirements

A router and a PC realize PPP callback via the serial interfaces over PSTN. As shown in the following figure, the PC and RouterA are interconnected via the modems across PSTN. C-DCC is adopted in this case. The PC is specified to be the callback client whereas RouterA to be the callback server. They implement callback according to the configuration of the **dialer route** command. RouterA uses the address 100.1.1.1 and the PC accepts the address assigned by RouterA.

II. Network diagram

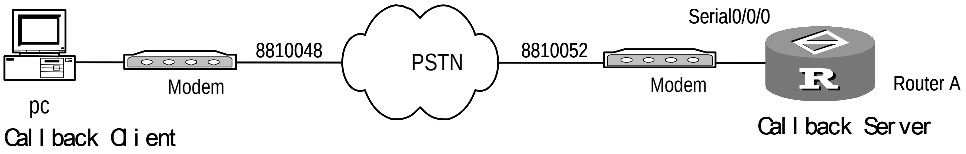


Figure 1-14 Network for the DCC application providing router-to-PC callback

III. Configuration procedure

1) Configure PC

First, configure the modem connected to the PC to be in “auto answer mode”, and then open [Start/Programs/Accessories/Communications/Dialup network]. Click [Set up new connection] in the [Dialup network] window, select the [Server type] page in the established new connection, and perform the following operations:

- Select the option [PPP]
- Set the [Logon network] option as unchecked
- Set the [Start software compression] as unchecked

Select [TCP/IP setting] in the [Server type] page, and perform the following operations:

- Check the option [Server allocated with IP address]
- Set the [Use IP head pointer compression] option as unchecked
- Set the [Use default gateway of the remote network] option as unchecked

2) Configure RouterA

```
[3Com] dialer-rule 1 ip permit
[3Com] local-user userpc
[3Com-luser-userc] password simple userpc
[3Com-luser-userc] service-type ppp
[3Com-luser-userc] quit
[3Com] interface serial 0/0/0
[3Com-Serial0/0/0] ip address 100.1.1.1 255.255.255.0
[3Com-Serial0/0/0] remote address 100.1.1.2
```

```
[3Com-Serial0/0/0] physical-mode async
[3Com-Serial0/0/0] modem
[3Com-Serial0/0/0] dialer enable-circular
[3Com-Serial0/0/0] dialer-group 1
[3Com-Serial0/0/0] dialer route ip 100.1.1.2 user userpc 8810052
[3Com-Serial0/0/0] dialer callback-center user
[3Com-Serial0/0/0] link-protocol ppp
[3Com-Serial0/0/0] ppp authentication-mode pap system
[3Com-Serial0/0/0] ppp pap local-user 3Com password simple 3Com
[3Com-Serial0/0/0] ppp callback server
```

1.4.6 NT Server-to-Router Callback for DCC

I. Network requirements

A router and an NT server implement PPP callback via the serial interfaces across PSTN.

As shown in the following figure, RouterA and the NT server are interconnected via the modems across PSTN. In this case, C-DCC is adopted. RouterA is specified as the callback client and the NT server as the callback server. Callback is implemented according to the configuration of the **dialer route** command. The NT server uses the address 100.1.1.254, and RouterA accepts the address assigned by the NT server.

II. Network diagram

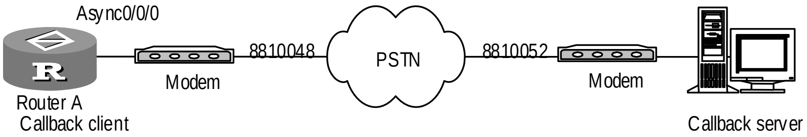


Figure 1-15 Network for the DCC application providing NT server-to-router callback

III. Configuration procedure

1) Configure RouterA

```
[3Com] dialer-rule 1 ip permit
[3Com] interface async 0/0/0
[3Com-Async0/0/0] async mode protocol
[3Com-Async0/0/0] link-protocol ppp
[3Com-Async0/0/0] ppp callback client
[3Com-Async0/0/0] ppp pap local-user 3Com password simple 3Com
[3Com-Async0/0/0] ip address ppp-negotiate
[3Com-Async0/0/0] dialer enable-circular
[3Com-Async0/0/0] dialer-group 1
[3Com-Async0/0/0] dialer route ip 100.1.1.254 8810052
```

2) Configure NT server

Configure the modem connected to the PC to be in “auto answer mode”, open [Start/Programs/Accessories/Communications/Dialup Network], click [Set up new connection] in the [Dialup Network] window, select the [Server type] page in the established new connection, and perform the following operations:

First, open the [Network attributes/Services] page, add “remote access server” in it and configure RAS attribute, click the <Add> button to install the modem, and set the modem attribute to “Dial-out and dial-in”. If the modem has been installed, click <Configure>. Click the <Network> button on the right to set the network attributes of RAS, including:

- Select “TCP/IP” in both [Dial-out protocol] and [Server setting].
- Click <Configure> on the right to configure an address assignment method for the dial-in client. It can be either “Use DHCP” or “Use static address set”.
- Select [Allow any authentication] to configure “Encryption setting”.

Then, select the menu bar [Management tools/Server management] to enable remote accessing service.

Finally, select the menu bar [Management tools/Remote access management] to enter the management interface, select [Users/Authorities] in it, and choose the user that can implement remote access. Three callback attributes are available, including:

- No callback
- Set by the dial-in party: The **ppp callback ntstring** *dial-number* command should be configured on the router if this method is selected.
- Preset to *number*: If this method is selected, the *dial-number* set on the router will be invalid and the NT system will dial the preset *number* when placing a return call.

1.4.7 Dial Number Backup and Internet Access by DCC

I. Network requirements

In PSTN, the dial number circular backup is fulfilled through configuring the **dialer route** command at the dialing side. The access side provides the accessing service for DCC via the asynchronous serial interface, and adopts the PAP authentication to authenticate the validity of the dialing party. In ISDN, single dialer number and CHAP authentication are adopted, and other configurations are similar to the PSTN side.

As shown in the following figure, RouterB and RouterD work as access server, RouterA and RouterC at the dialing side accept the negotiated addresses assigned by the remote ends. The address pool for allocation is in the range of 100.1.1.1 to 100.1.1.16. RouterB and RouterD use the address 100.1.1.254, and obtain the dialer numbers 8810048 to 8810055 from the telecommunications service provider. ISDN dial number is 8810148, which provides services for 16 network users.

II. Network diagram

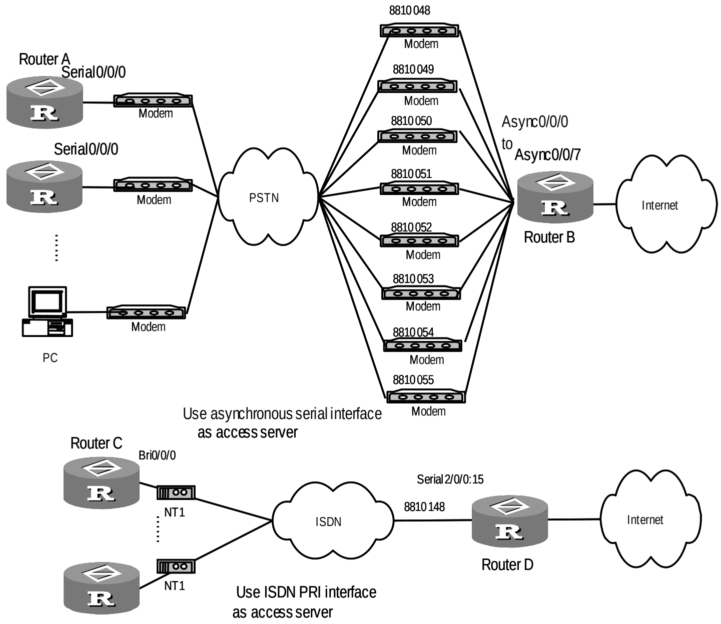


Figure 1-16 Network for the DCC application providing dial number circular standby and accessing service

III. Configuration procedure

Solution 1: Configure dial number circular standby on the dialing parties, adopt C-DCC to set up connections on the 8 asynchronous serial interfaces at the access side, and configure the DCC parameters on the dialer interfaces.

1) Configure RouterA

```
[3Com] dialer-rule 1 ip permit
[3Com] local-user userb
[3Com-luser-userb] password simple userb
[3Com-luser-userb] service-type ppp
[3Com-luser-userb] quit
[3Com] interface serial 0/0/0
[3Com-Serial0/0/0] physical-mode async
[3Com-Serial0/0/0] async mode protocol
[3Com-Serial0/0/0] ip address ppp-negotiate
[3Com-Serial0/0/0] dialer enable-circular
[3Com-Serial0/0/0] dialer-group 1
[3Com-Serial0/0/0] dialer route ip 100.1.1.254 8810048
[3Com-Serial0/0/0] dialer route ip 100.1.1.254 8810049
......
[3Com-Serial0/0/0] dialer route ip 100.1.1.254 8810055
[3Com-Serial0/0/0] link-protocol ppp
```

```
[3Com-Serial0/0/0] ppp pap local-user user1 password simple user1
[3Com-Serial0/0/0] user-interface tty1
[3Com-ui-tty1] modem
```

2) Configure RouterB

```
[3Com] dialer-rule 2 ip permit
[3Com] local-user user1
[3Com-luser-user1] password simple user1
[3Com-luser-user1] service-type ppp
[3Com-luser-user1] quit
[3Com] local-user user2
[3Com-luser-user2]password simple user2
[3Com-luser-user2] service-type ppp
[3Com-luser-user2] quit
……
[3Com] local-user user16
[3Com-luser-user16] password simple user16
[3Com-luser-user16] service-type ppp
[3Com-luser-user16] quit
[3Com] interface dialer 0
[3Com-Dialer0] ip address 100.1.1.254 255.255.255.0
[3Com-Dialer0] remote address pool 1
[3Com-Dialer0] dialer enable-circular
[3Com-Dialer0] dialer-group 2
[3Com-Dialer0] link-protocol ppp
[3Com-Dialer0] ppp authentication-mode pap domain system
[3Com-Dialer0] ppp pap local-user userc password simple userc
[3Com-Dialer0] interface async0/0/1
[3Com-Async0/0/1] async mode protocol
[3Com-Async0/0/1] dialer circular-group 0
[3Com-Async0/0/1] link-protocol ppp
[3Com-Async0/0/1] ppp authentication-mode pap domain system
[3Com-Async0/0/1] interface async0/0/2
[3Com-Async0/0/2] async mode protocol
[3Com-Async0/0/2] dialer circular-group 0
……
[3Com-Async0/0/7] interface async0/0/8
[3Com-Async0/0/8] async mode protocol
[3Com-Async0/0/8] dialer circular-group 0
[3Com-Async0/0/8] link-protocol ppp
[3Com-Async0/0/8] ppp authentication-mode pap domain system
[3Com-Async0/0/8] user-interface tty1
[3Com-ui-tty1] modem
[3Com-ui-tty1] user-interface tty2
```

```
[3Com-ui-tty2] modem
……
[3Com-ui-tty7] user-interface tty8
[3Com-ui-tty8] modem
[3Com-ui-tty8] quit
[3Com] domain system
[3Com-isp-system] ip pool 1 100.1.1.1 100.1.1.16
[3Com-isp-system] quit
```

3) Configure subscriber PC

Install a modem in a subscriber PC, configure it to be in “auto answer mode”, open [Start/Programs/Accessories/Communications/Dialup network], click [Set up new connection] in the [Dialup network] window, and select [Server type] in the established new connection, and perform the following operations:

- Select the option [PPP]
- Set the option [Login network] as unchecked
- Set the option [Start software compression] as unchecked

Select [TCP/IP setting] in the [Server type] page, and perform the following operations:

- Check the option [Server allocated with IP address]
- Set the [Use IP head pointer compression] option as unchecked
- Set the [Use default gateway of the remote network] option as unchecked

Start dialing, and input the user name user1 and the password pass1.

Solution 2: The dialing side uses a single number to dial, and the accessing side uses C-DCC to set up the connection via the ISDN PRI interface. Configure the DCC parameters on the dialer interface.

1) Configure RouterC

```
[3Com] dialer-rule 1 ip permit
[3Com] local-user userb
[3Com-luser-userb] password simple userb
[3Com-luser-userb] service-type ppp
[3Com-luser-userb] quit
[3Com] interface bri 0/0/0
[3Com-Bri0/0/0] ip address ppp-negotiate
[3Com-Bri0/0/0] dialer enable-circular
[3Com-Bri0/0/0] dialer-group 1
[3Com-Bri0/0/0] dialer route ip 100.1.1.254 8810148
[3Com-Bri0/0/0] link-protocol ppp
[3Com-Bri0/0/0] ppp chap user user1
[3Com-Bri0/0/0] ppp chap password simple pass1
```

2) Configure RouterD

```
[3Com] dialer-rule 2 ip permit
[3Com] local-user user1
```

```
[3Com-luser-user1] password simple user1
[3Com-luser-user1] service-type ppp
[3Com-luser-user1] quit
[3Com] local-user user2
[3Com-luser-user2] password simple user2
[3Com-luser-user2] service-type ppp
[3Com-luser-user2] quit
……
[3Com] local-user user16
[3Com-luser-user16] password simple user16
[3Com-luser-user16] service-type ppp
[3Com-luser-user16] quit
[3Com] controller e1 2/0/0
[3Com-E1 2/0/0] pri-set
[3Com-E1 2/0/0] interface serial 2/0/0:15
[3Com-Serial2/0/0:15] ip address 100.1.1.254 255.255.255.0
[3Com-Serial2/0/0:15] remote address pool 1
[3Com-Serial2/0/0:15] dialer enable-circular
[3Com-Serial2/0/0:15] dialer-group 2
[3Com-Serial2/0/0:15] link-protocol ppp
[3Com-Serial2/0/0:15] ppp authentication-mode chap system
[3Com-Serial2/0/0:15] ppp chap user userb
[3Com-Serial2/0/0:15] ppp chap password simple passb
[3Com-Serial2/0/0:15] quit
[3Com] domain system
[3Com-isp-system] ip pool 1 100.1.1.1 100.1.1.16
[3Com-isp-system] quit
```

1.4.8 Logical Interface Standby through Dialer Route for DCC

I. Network requirements

RouterA and RouterB are directly connected via the serial interfaces. At the same time, RouterA forms a dialup connection with RouterB via a modem through PSTN. RouterB cannot call RouterA via dialing.

As shown in the following figure, a logical interface is generated through configuring the **dialer route** command on RouterA. This interface can be used as either the standby interface for other interfaces or the main interface. The port Serial0/0/0 on RouterA is used as the dialer interface, and Serial1/0/0 is connected to RouterB through straightforward DDN. The address of Serial0/0/0 on RouterA is 100.1.1.1, and the address of the Serial1/0/0 connected to DDN is 200.1.1.1. The address of the dialer interface on RouterB is 100.1.1.2, and the address of the interface connected to DDN is 200.1.1.2.

II. Network diagram

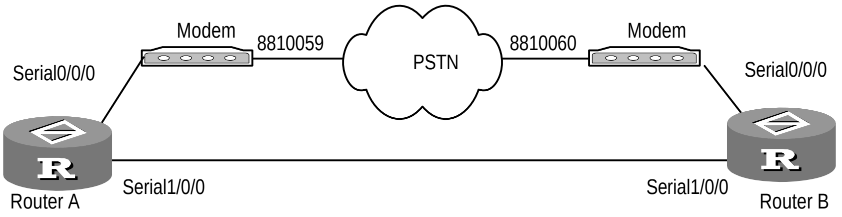


Figure 1-17 Network for the DCC application providing logic interface standby through dialer route

III. Configuration procedure

Solution 1: Adopt C-DCC and use the logic interface configured through the **dialer route** command as the standby interface.

1) Configure RouterA

```
[3Com] dialer-rule 1 ip permit
[3Com] interface serial 0/0/0
[3Com-Serial0/0/0] physical-mode async
[3Com-Serial0/0/0] modem
[3Com-Serial0/0/0] ip address 100.1.1.1 255.255.255.0
[3Com-Serial0/0/0] dialer enable-circular
[3Com-Serial0/0/0] dialer-group 1
[3Com-Serial0/0/0] dialer route ip 100.1.1.2 8810060 logic-channel 1
[3Com-Serial0/0/0] interface serial 1/0/0
[3Com-Serial1] ip address 200.1.1.1 255.255.255.0
[3Com-Serial1] link-protocol ppp
[3Com-Serial1] standby logic-channel 1
```

2) Configure RouterB

```
[3Com] dialer-rule 2 ip permit
[3Com] interface serial 0/0/0
[3Com-Serial0/0/0] physical-mode async
[3Com-Serial0/0/0] modem
[3Com-Serial0/0/0] ip address 100.1.1.2 255.255.255.0
[3Com-Serial0/0/0] dialer enable-circular
[3Com-Serial0/0/0] dialer-group 2
[3Com-Serial0/0/0] dialer route ip 100.1.1.1 8810059 logic-channel 1
[3Com-Serial0/0/0] interface serial 1/0/0
[3Com-Serial1/0/0] ip address 200.1.1.2 255.255.255.0
[3Com-Serial1/0/0] link-protocol ppp
[3Com-Serial1/0/0] standby logic-channel 1
[3Com-Serial1/0/0] user-interface tty1
[3Com-Serial1/0/0] modem
```

Solution 2: Adopt C-DCC and use the logical interface configured through the **dialer route** command as the main interface.

1) Configure RouterA

```
[3Com] dialer-rule 1 ip permit
[3Com] interface serial 0/0/0
[3Com-Serial0/0/0] physical-mode async
[3Com-Serial0/0/0] async mode protocol
[3Com-Serial0/0/0] ip address 100.1.1.1 255.255.255.0
[3Com-Serial0/0/0] dialer enable-circular
[3Com-Serial0/0/0] dialer-group 1
[3Com-Serial0/0/0] dialer route ip 100.1.1.2 8810060 logic-channel 1
[3Com-Serial0/0/0] interface serial 1/0/0
[3Com-Serial1/0/0] ip address 200.1.1.1 255.255.255.0
[3Com-Serial1/0/0] link-protocol ppp
[3Com-Serial1/0/0] standby interface logic-channel 1
[3Com-Serial1/0/0] user-interface tty1
[3Com-ui-tty1] modem
```

2) Configure RouterB

```
[3Com] dialer-rule 2 ip permit
[3Com] interface serial 0/0/0
[3Com-Serial0/0/0] physical-mode async
[3Com-Serial0/0/0] async mode protocol
[3Com-Serial0/0/0] ip address 100.1.1.2 255.255.255.0
[3Com-Serial0/0/0] dialer enable-circular
[3Com-Serial0/0/0] dialer-group 2
[3Com-Serial0/0/0] dialer route ip 100.1.1.1 8810059 logic-channel 1
[3Com-Serial0/0/0] interface serial 1/0/0
[3Com-Serial1/0/0] ip address 200.1.1.2 255.255.255.0
[3Com-Serial1/0/0] link-protocol ppp
[3Com-Serial1/0/0] standby interface logic-channel 1
[3Com-Serial1/0/0] user-interface tty1
[3Com-ui-tty1] modem
```

1.4.9 Placing/Receiving Calls from a Specified Physical Interface

I. Network requirements

As shown in the following network diagram, Router A uses IP address 22.0.0.1. Its interfaces BRI 0/0/0 and PRI 1/0/0 are connected to different ISDN switches, but both are assigned to interface Dialer 0. BRI 0/0/0 and PRI 1/0/0 are associated with telephone numbers 7300340 and 8500560 respectively.

Router B uses IP address 22.0.0.2. Its interfaces BRI 0/0/0 and PRI 1/0/0 are connected to the same ISDN switch and both are assigned to interface Dialer 0. BRI

0/0/0 and PRI 1/0/0 are associated with telephone numbers 881050 and 8810151 respectively.

II. Network diagram

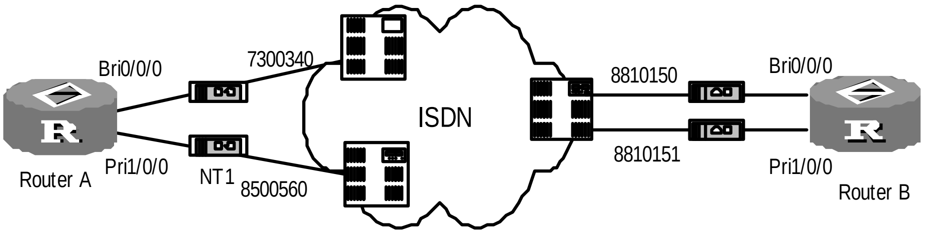


Figure 1-18 Network diagram for placing/receiving calls from a physical interface

III. Configuration procedure

1) Configure Router A

# Configure a dialer ACL.

```
<RouterA> system
[RouterA] dialer-rule 1 ip permit
```

# Set the operating mode of the E1 interface to PRI.

```
[RouterA] controller e1 1/0/0
[RouterA-e1 1/0/0 ] pri-set
[RouterA-e1 1/0/0 ] quit
```

# Assign the two physical interfaces to interface Dialer 0.

```
[RouterA] interface bri0/0/0
[RouterA-bri0/0/0] dialer circular-group 0
[RouterA-bri0/0/0] ppp mp
[RouterA-bri0/0/0] interface serial1/0/0:15
[RouterA-serial1/0/0:15] dialer circular-group 0
[RouterA-serial1/0/0:15] ppp mp
[RouterA-serial1/0/0:15] quit
```

# Configure C-DCC.

```
[RouterA] interface dialer0
[RouterA-Dialer0] link-protocol ppp
[RouterA-Dialer0] ppp mp
[RouterA-Dialer0] ip address 22.0.0.1 255.255.255.0
[RouterA-Dialer0] dialer enable-circular
[RouterA-Dialer0] dialer-group 1
[RouterA-Dialer0] dialer route ip 22.0.0.2 8810150 interface bri0/0/0
[RouterA-Dialer0 ] dialer route ip 22.0.0.2 8810151 interface serial1/0/0:15
```

2) Configure Router B

# Configure a dialer ACL.

```
<RouterB> system
[RouterB] dialer-rule 1 ip permit
```

# Set the operating mode of the E1 interface to PRI.

```
[RouterB] controller e1 1/0/0
[RouterB-e1 1/0/0] pri-set
[RouterB-e1 1/0/0] quit
```

# Assign the two physical interfaces to interface Dialer 0.

```
[RouterB] interface bri0/0/0
[RouterB-bri0/0/0] dialer circular-group 0
[RouterB-bri0/0/0] ppp mp
[RouterB-bri0/0/0] interface serial1/0/0:15
[RouterB-serial1/0/0:15] dialer circular-group 0
[RouterB-serial1/0/0:15] ppp mp
[RouterB-serial1/0/0:15] quit
```

# Configure C-DCC.

```
[RouterB] interface dialer0
[RouterB-Dialer0] link-protocol ppp
[RouterB-Dialer0] ppp mp
[RouterB-Dialer0] ip address 22.0.0.2 255.255.255.0
[RouterB-Dialer0] dialer enable-circular
[RouterB-Dialer0] dialer-group 1
[RouterB-Dialer0] dialer route ip 22.0.0.2 7300340
[RouterB-Dialer0] dialer route ip 22.0.0.2 8500560
```

1.5 Troubleshooting

1.5.1 Troubleshooting of DCC

Fault 1: Modem does not dial when the router forwards the data, so the DCC dialup connection cannot be set up.

Troubleshooting:

- Check whether the modem and phone cable connections are correct, and whether the modem initialization process is correct.
- For the synchronous/asynchronous serial interface, check whether it is configured to asynchronous and dialing mode.
- Check whether DCC has been enabled on the dial interface.
- Check whether the corresponding **dialer route** or **dialer number** command has been configured for the packet.

Fault 2: The remote end cannot be pinged after the modem is connected.

Troubleshooting:

- Check whether the same link protocol is configured on the local and remote ends, and whether the configured PPP authentication parameters are correct. Use the **debugging ppp all** command to enable PPP debugging to view the PPP negotiation process, and make sure that the PPP negotiation parameters are correct.
- Check whether the network address has been correctly configured on the dial interface (physical interface or dialer interface).
- Check whether DCC has been enabled on the dial interface.
- Check whether the commands **dialer-group** and **dialer rule** has been configured, and whether the configurations are correct. Make sure that **dialer rule** is configured to permit the packet and the two commands are associated.
- Use the commands **debugging dialer event** and **debugging dialer packet** to debug DCC, and locate the problem according to the output information.

1.5.2 Locating Problems with the DCC Debugging Information

I. Enabling DCC debugging

Execute the following commands in system view for displaying the DCC debugging information:

```
[3Com] debugging dialer event
[3Com] debugging dialer packet
[3Com] info-center enable
```

II. Debugging messages, possible reasons and solutions

The following table lists the debugging messages that may appear when DCC cannot reach the remote end, gives the possible reasons, and provides some solutions.

Table 1-39 Debugging messages, possible reasons and solutions

Debugging message	Possible reason	Solution
DCC: Receive CALL_DISC_IND	• The physical connection between the local and remote ends is broken, phone cable is not securely connected to the router, or the quality of phone line is not good. • PPP authentication is not correctly configured, so the PPP authentication is failed. • Remote DCC authentication is failed, because *name* in the commands **dialer user** and **dialer route** configured for DCC is inconsistent with *name* configured for PPP authentication, and the **dialer route** at the remote end does not contain the local network address. • The remote end disconnects the connection because the remote DCC idle-timeout timer has timed out.	• If PPP configuration is incorrect or *name* configurations are inconsistent, implement the configuration as shown in the above example. • If it is the problem of the network address, apply the following measures in the configuration of the remote end: Add the dialer route corresponding to the network address of the local router on the remote router. Alternatively, remove all the dialer routes configured at the remote end, and use the dial number.
DCC: link negotiation Down on interface ***	The link is probably disconnected because PPP negotiation is failed due to a wrong PPP configuration.	Refer to the previous example to make the configuration.
DCC: NAME authentication ERROR, failed	The *name* argument configured in the commands **dialer user** and **dialer route** is inconsistent with that configured in PPP authentication. The connection is disconnected since the local DCC authentication has been failed.	Refer to the previous example to make the configuration.

Debugging message	Possible reason	Solution
DCC: peeraddr matching error on interface ***, shutdown link	The local dialer route does not contain the remote network address.	Add the dialer route corresponding to the remote network address on the local router or use the dial number after removing all the dialer routes configured on the local router.
DCC: idle-timeout on interface *** , shutdown! start enable-time	DCC normally disconnects the connection whenever the local DCC idle-timeout timer times out. This debugging message does not indicate any error.	—
DCC: wait-for-carrier-timeout on a link on interface ***, shutdown!start enable-time	The local router cannot contact the remote end for a long time. The remote end may be busy or the quality of the phone line may be bad.	• Check whether the remote end is busy. • Check the quality of the phone line.
DCC: The interface has no dialer-group, discard the packet!	The **dialer-group** command has not been configured on the corresponding dialer interface or the physical interface on which DCC is directly enabled.	Refer to the previous example to make the configuration.
DCC: there is not a dialer number on the interface, failed, discard packet	Neither **dialer route** nor the **dialer number** is configured on the corresponding dialer interface or the physical interface on which DCC is enabled directly.	Configure **dialer route** or **dialer number** on the local end for the outbound call at the local end.
DCC: Enable-timeout is effective , failed	The enable-timeout timer on the corresponding physical interface has not timed out yet. The physical interface can be used for dialing upon the timeout of the timer. This debugging message does not indicate any error.	—

Chapter 2 Dynamic Routing Standby

2.1 Introduction to Dynamic Routing Standby

Dynamic routing standby provides routing-based dial backup. It uses legacy DCC, including both C-DCC and RS-DCC, to maintain dial links dynamically.

Taking advantage of convergence time and related features of dynamic routing protocols, dynamic routing standby perfectly combines backup and routing. It breaks through the limitation of interesting packet-triggered dial in legacy DCC and provides reliable connections and standard dial-on-demand services.

Dynamic routing standby is an enhancement to legacy DCC backup. With it, the primary and secondary interfaces can be of any type, because its backup is dynamic routing based rather than interface-specific or link-specific. It is thus suitable for situations where multiple interfaces and routers are involved.

Dynamic routing standby does not depend on a particular routing protocol. It can run multiple dynamic routing protocols such as RIP1, RIP2, and SOPF.

It does not depend on interesting packets to trigger dial; thus the secondary link starts automatically when the primary link disconnects without dialing delay (excluding route convergence time).

By configuring a set of destination IP addresses carried on the primary link, dynamic routing standby can monitor the changes of the routes on the primary link. The following describes how it monitors routes and starts the secondary link:

- Dynamic routing standby registers a network segment (IP address range) requiring observation with the system;
- The system listens in on the observed network segment for any updates. If the route has been deleted, dynamic routing standby looks up the routing table for a valid route to the observed network segment;
- If a valid route is available and if this route sets out from an interface other than the one configured with the **standby routing-group** command, the primary link is regarded UP.
- If no valid route is available, the primary link is regarded disabled and unavailable. Dynamic routing standby immediately informs the routing protocol to trigger dial right away to start the secondary link.

Once the secondary link (dialup link) is enabled, communication data is switched over to it. When the primary link is available again, the system adds the route destined for the monitored segment, which is carried by the primary link. After that, the system can disconnect the secondary link right away or enable a “disable” timer for the route. In the latter case, if the route is still available when the timer expires, the system disconnects the secondary link. If the route goes DOWN before the timer expires, it does not disconnect the secondary link.

2.2 Dynamic Routing Standby Configuration

Dynamic routing standby configuration tasks include:

- Create a dynamic routing standby group
- Apply a dynamic routing standby group to the interface
- Configure secondary link disconnection delay

Note:

Before configuring dynamic routing standby, identify:

- Primary and secondary interfaces. You should determine which interfaces on which router are intended for primary and secondary use. You can define multiple interfaces on more than one router.
- Network segment (interface IP address or network) to be observed, such as interface IP address of a remote router.

I. Creating a dynamic routing standby group

Perform the following configuration in system view.

Table 2-1 Create a dynamic routing standby group

Operation	Command
Create a dynamic routing standby group and assign a to-be-monitored network segment to the group	**standby routing-rule** *group-number* **ip** *ip-address address-mask*
Remove a dynamic routing standby group, or remove the monitored segment from the specified dynamic routing standby group	**undo standby routing-rule** *group-number* [**ip** *ip-address ip-mask*]

Each dynamic routing standby group may contain up to 255 monitored network segments. The primary link of a dynamic routing standby group is regarded disconnected only when the routes of all the monitored network segments in the group are removed.

🕮 **Note:**

The IP address configured in the **standby routing-rule** command is used for dialer route lookup. You must make sure that this IP address is the one configured in the corresponding **dialer route** command.

You may use the **standby routing-rule** command in the following two ways:

- Create multiple dynamic routing standby groups, each monitoring a network segment. In case no valid route is available with a network segment, the system attempts to dial a backup link. On the dial-up interface, link establishment and disconnection are independent among monitored network segments.
- Create one dynamic routing standby group which monitors multiple segments. The system attempts to dial a backup link only when none of these monitored network segments has a valid route. When doing this, the system looks up the dialer-route logical channels configured for the monitored network segments and uses the one found first to dial. In this case, you can only connect one link. In addition, to ensure reachability of all the monitored network segments, you must enable dynamic routing.

II. Applying a dynamic routing standby group onto a secondary interface

Before enabling dynamic routing standby on a secondary interface, make sure that you have configured legacy DCC on it.

Perform the following configuration in dial interface view.

Table 2-2 Apply a dynamic routing group onto the secondary interface

Operation	Command
Apply a dynamic routing standby group onto the secondary interface	**standby routing-group** *group-number*
Remove the dynamic routing standby group from the secondary interface	**undo standby routing-group** *group-number*

By default, dynamic routing standby is disabled.

🕮 **Note:**

A dial interface refers to a physical dial interface such as PRI and BRI, or a logical dial interface, that is, dialer interface.

III. Configuring secondary link disconnection delay

You may configure a delay for dynamic routing standby to disconnect the secondary link after the primary link goes UP.

Perform the following configurations in dial interface view.

Table 2-3 Configure secondary link disconnection delay

Operation	Command
Configure a secondary link disconnection delay	**standby timer routing-disable** *seconds*
Restore the default secondary link disconnection delay value	**undo standby timer routing-disable**

The secondary link disconnection delay defaults to 0, meaning disconnecting the secondary link immediately.

2.3 Dynamic Routing Standby Configuration Example

2.3.1 Dynamic Routing Standby Configuration Example I

I. Network requirements

RouterB is connected to RouterA and RouterC each through a serial interface encapsulated with X.25.

RouterA and RouterC are connected to an ISDN switched network through ISDN BRI interfaces, and they can call each other.

The serial interfaces use addresses on the network segment 10.0.0.0 and the BRI interfaces use addresses on 20.0.0.0.

In dynamic routing standby, RouterA is working as the control device to monitor routes destined to the segment 30.0.0.0 on Router C.

II. Network diagram

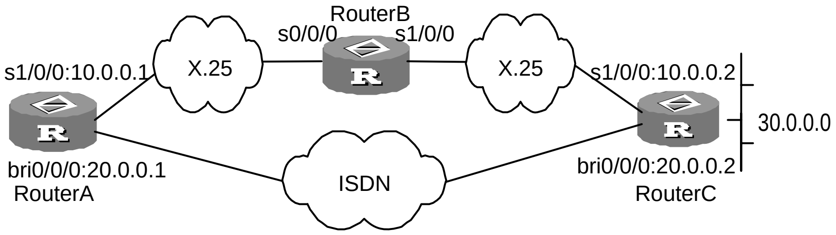


Figure 2-1 Network diagram for dynamic routing standby

III. Configuration procedure

1) Configure RouterA

# Configure a dialer ACL.

```
[3Com] dialer-rule 1 ip permit
```

# Configure dial parameters on the BRI 0/0/0 interface.

```
[3Com] interface bri 0/0/0
[3Com-Bri0/0/0] ip address 20.0.0.1 255.0.0.0
[3Com-Bri0/0/0] dialer enable-circular
[3Com-Bri0/0/0] dialer-group 1
[3Com-Bri0/0/0] dialer route ip 20.0.0.2 8810052
[3Com-Bri0/0/0] dialer route ip 30.0.0.1 8810052
```

# Configure Serial 1/0/0 and encapsulate it with X.25.

```
[3Com-Bri0/0/0] interface serial 1/0/0
[3Com-Serial1/0/0] link-protocol x25 dte ietf
[3Com-Serial1/0/0] x25 x121-address 10
[3Com-Serial1/0/0] x25 map ip 10.0.0.2 x121-address 20 broadcast
[3Com-Serial1/0/0] ip address 10.0.0.1 255.0.0.0
[3Com-Serial1/0/0] quit
```

# Enable RIP.

```
[3Com] rip
[3Com-rip] network 10.0.0.0
[3Com-rip] network 20.0.0.0
[3Com-rip] quit
```

# Configure a dynamic routing standby group.

```
[3Com] standby routing-rule 1 ip 30.0.0.1 255.0.0.0
```

# Assign the route on the dial interface with a priority lower than that of serial interface.

```
[3Com] interface bri 0/0/0
[3Com-Bri0/0/0] rip metricin 2
```

# Apply the dynamic routing standby group on the dial interface.

```
[3Com-Bri0/0/0] standby routing-group 1
```

2) Configure Router B

# Enable X.25 switching.

```
[3Com] x25 switching
```

# Encapsulate the interfaces with X.25.

```
[3Com] interface serial 0/0/0
[3Com-Serial0/0/0] link-protocol x25 dce ietf
[3Com-Serial0/0/0] interface serial 1/0/0
[3Com-Serial1/0/0] link-protocol x25 dce ietf
```

# Configure X25 switching information.

```
[3Com] x25 switch svc 20 interface Serial 0/0/0
```

```
[3Com] x25 switch svc 10 interface Serial 1/0/0
```

3) Configure RouterC

# Configure a dialer ACL.

```
[3Com] dialer-rule 1 ip permit
```

# Configure dial parameters on the BRI 0/0/0 interface.

```
[3Com] interface bri 0/0/0
[3Com-Bri0/0/0] ip address 20.0.0.2 255.0.0.0
[3Com-Bri0/0/0] dialer enable-circular
[3Com-Bri0/0/0] dialer-group 1
```

# Configure Serial1/0/0 and encapsulate it with X.25.

```
[3Com-Bri10/0/0] interface serial 1/0/0
[3Com-Serial1/0/0] link-protocol x25 dte ietf
[3Com-Serial1/0/0] x25 x121-address 20
[3Com-Serial1/0/0] x25 map ip 10.0.0.1 x121-address 10 broadcast
[3Com-Serial1/0/0] ip address 10.0.0.2 255.0.0.0
```

# Configure a loopback interface.

```
[3Com-Serial1/0/0] interface loopback1
[3Com-Loopback1] ip address 30.0.0.1 255.0.0.0
[3Com-Loopback1] quit
```

# Enable RIP.

```
[3Com] rip
[3Com-rip] network 10.0.0.0
[3Com-rip] network 20.0.0.0
[3Com-rip] network 30.0.0.0
```

2.3.2 Dynamic Routing Standby Configuration Example II

I. Network requirements

RouterA and RouterB are connected using serial interfaces on the segment 10.0.0.0 and are connected to an ISDN switched network using ISDN BRI interfaces on the segment 20.0.0.0. They can call each other.

In dynamic routing standby, RouterA is working as the control device to monitor the segment loopback0:40.0.0.0 on RouterB.

II. Network diagram

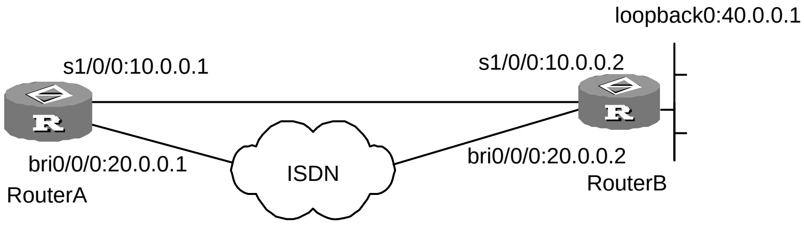


Figure 2-2 Network diagram for dynamic routing standby

III. Configuration procedure

1) Configure RouterA

# Configure a dialer ACL.

```
[3Com] dialer-rule 1 ip permit
```

# Configure dial parameters on the BRI 0/0/0 interface.

```
[3Com] interface bri 0/0/0
[3Com-Bri0/0/0] ip address 20.0.0.1 255.0.0.0
[3Com-Bri0/0/0] dialer enable-circular
[3Com-Bri0/0/0] dialer-group 1
[3Com-Bri0/0/0] dialer route ip 20.0.0.2 8810052
[3Com-Bri0/0/0] dialer route ip 40.0.0.1 8810052
```

# Configure Serial1/0/0.

```
[3Com-Bri0/0/0] interface serial 1/0/0
[3Com-Serial1/0/0] ip address 10.0.0.1 255.0.0.0
[3Com-Serial1/0/0] quit
```

# Enable OSPF.

```
[3Com] ospf
[3Com-ospf-1] area 0
[3Com-ospf-1-area-0.0.0.0] network 10.0.0.0 0.0.0.255
[3Com-ospf-1-area-0.0.0.0] network 20.0.0.0 0.0.0.255
[3Com-ospf-1-area-0.0.0.0] quit
[3Com-ospf-1] quit
```

# Configure a dynamic routing standby group

```
[3Com] standby routing-rule 1 ip 40.0.0.1 255.0.0.0
```

# Assign the route on the dial interface with a priority lower than that of serial interface.

```
[3Com] interface Bri0/0/0
[3Com-Bri0/0/0] ospf cost 10
[3Com-Bri0/0/0] ospf network-type broadcast
```

# Apply the dynamic routing standby group onto the dial interface.

```
[3Com-Bri0/0/0] standby routing-group 1
```

2) Configure RouterB

# Configure a dialer ACL.

```
[3Com] dialer-rule 1 ip permit
```

# Configure dial parameters on the BRI 0/0/0 interface.

```
[3Com] interface bri 0/0/0
[3Com-Bri0/0/0] ip address 20.0.0.1 255.0.0.0
[3Com-Bri0/0/0] dialer enable-circular
[3Com-Bri0/0/0] dialer-group 1
```

# Configure Serial1/0/0.

```
[3Com-Bri0/0/0] interface serial 1/0/0
[3Com-Serial1/0/0] ip address 10.0.0.1 255.0.0.0
```

# Configure interface Loopback 0.

```
[3Com-Serial1/0/0] interface loopback0
[3Com-Loopback0] ip address 40.0.0.1 255.0.0.0
```

# Enable OSPF.

```
[3Com] ospf
[3Com-ospf-1] area 0
[3Com-ospf-1-area-0.0.0.0] network 10.0.0.0 0.0.0.255
[3Com-ospf-1-area-0.0.0.0] network 20.0.0.0 0.0.0.255
```

# Assign the route on the dial interface with a priority lower than that of serial interface.

```
[3Com-Bri1/0/0] ospf cost 10
[3Com-Bri1/0/0] ospf network-type broadcast
```

# Configure a dynamic routing standby group.

```
[3Com] standby routing-rule 1 ip 40.0.0.1 255.0.0.0
```

# Apply the dynamic routing standby group onto the dial interface.

```
[3Com-Bri1/0/0] standby routing-group 1
```

# Configure dial parameters on the BRI 1/0/0 interface.

```
[3Com] interface bri 1/0/0
[3Com-Bri1/0/0] ip address 20.0.0.2 255.0.0.0
[3Com-Bri1/0/0] dialer enable-circular
[3Com-Bri1/0/0] dialer-group 1
```

# Configure Serial1/0/0.

```
[3Com-Bri1/0/0] interface serial 1/0/0
[3Com-Serial1/0/0] ip address 10.0.0.2 255.0.0.0
```

# Configure the interface Loopback0.

```
[3Com-Serial1/0/0] interface loopback0
```

```
[3Com-Loopback0] ip address 40.0.0.1 255.0.0.0
```

# Enable OSPF.

```
[3Com] ospf
[3Com-ospf-1] area 0
[3Com-ospf-1-area-0.0.0.0] network 10.0.0.0 0.0.0.255
[3Com-ospf-1-area-0.0.0.0] network 20.0.0.0 0.0.0.255
[3Com-ospf-1-area-0.0.0.0] network 40.0.0.0 0.0.0.255
```

2.3.3 Dynamic Routing Standby Configuration Example III

I. Network requirements

Router A and Router B are connected across an X.25 network.

At the same time, for dial-up backup, they are connected to an ISDN network each by using an ISDN BRI interface on which two B channels are bundled. The two routers can dial to reach each other through RS-DCC.

In dynamic routing standby, Router A is working as the control device to monitor the route destined for the network segment 30.0.0.0 on Router B.

In normal cases, Router A and Router B communicate through X.25, the primary link. When the route to the monitored network segment goes down, for example, because fault occurs on the X.25 network, Router A brings up the ISDN BRI link automatically.

II. Network diagram

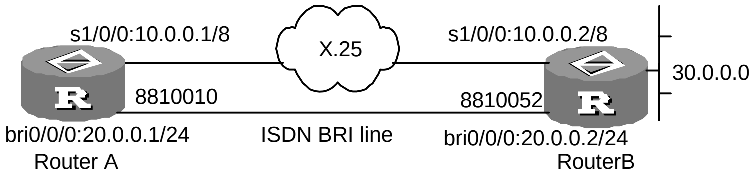


Figure 2-3 Network diagram for dynamic routing standby

III. Configuration procedure

1) Configure Router A

# Configure a dial-up ACL and add a local user.

```
[3Com] dialer-rule 1 ip permit
[3Com] local-user userb
[3Com-luser-userb] password simple userb
[3Com-luser-userb] service-type ppp
[3Com-luser-userb] quit
```

# Configure a dynamic routing standby group and add the to-be-monitored network segment to it.

```
[3Com] standby routing-rule 1 ip 30.0.0.1 255.0.0.0
```

# Configure RS-DCC and MP on the dialer 0 interface.

```
[3Com] interface Dialer0
[3Com-Dialer0] link-protocol ppp
[3Com-Dialer0] ppp mp
[3Com-Dialer0] ip address 20.0.0.1 255.255.255.0
[3Com-Dialer0] undo dialer enable-circular
[3Com-Dialer0] dialer user userb
[3Com-Dialer0] dialer-group 1
[3Com-Dialer0] dialer bundle 1
[3Com-Dialer0] dialer number 8810010
[3Com-Dialer0] ppp authentication-mode pap
[3Com-Dialer0] ppp pap local-user usera password simple usera
[3Com-Dialer0] standby routing-group 1
```

# Assign interface BRI 0/0/0 to interface dialer 0.

```
[3Com] interface bri 0/0/0
[3Com-bri0/0/0] dialer bundle-member 1
[3Com-bri0/0/0] ppp authentication-mode pap
[3Com-bri0/0/0] ppp pap local-user usera password simple usera
```

# Configure interface Serial 1/0/0 and encapsulate it with X.25.

```
[3Com-Bri0/0/0] interface serial 1/0/0
[3Com-Serial1/0/0] link-protocol x25 dte ietf
[3Com-Serial1/0/0] x25 x121-address 10
[3Com-Serial1/0/0] x25 map ip 10.0.0.2 x121-address 20 broadcast
[3Com-Serial1/0/0] ip address 10.0.0.1 255.0.0.0
[3Com-Serial1/0/0] quit
```

# Configure RIP.

```
[3Com] rip
[3Com-rip] network 10.0.0.0
[3Com-rip] network 20.0.0.0
[3Com-rip] quit
```

# Assign the route on the dial interface a metric value lower than the route on the serial interface.

```
[3Com] interface bri 0/0/0
[3Com-Bri0/0/0] rip metricin 2
```

2) Configure Router B

# Configure a dial-up ACL and add a local user.

```
[3Com] dialer-rule 1 ip permit
[3Com] local-user usera
```

```
[3Com-luser-userb] password simple usera
[3Com-luser-userb] service-type ppp
[3Com-luser-userb] quit
```

# Configure RS-DCC and MP on the dialer 0 interface.

```
[3Com] interface Dialer0
[3Com-Dialer0] link-protocol ppp
[3Com-Dialer0] ppp mp
[3Com-Dialer0] ip address 20.0.0.2 255.255.255.0
[3Com-Dialer0] undo dialer enable-circular
[3Com-Dialer0] dialer user userA
[3Com-Dialer0] dialer-group 1
[3Com-Dialer0] dialer bundle 1
[3Com-Dialer0] dialer number 8810052
[3Com-Dialer0] ppp authentication-mode pap
[3Com-Dialer0] ppp pap local-user usera password simple usera
[3Com-Dialer0] standby routing-group 1
```

# Configure dial parameters on interface BRI 0/0/0.

```
[3Com] interface bri 0/0/0
[3Com-bri0/0/0] dialer bundle-member 1
[3Com-bri0/0/0] ppp authentication-mode pap
[3Com-bri0/0/0] ppp pap local-user usera password simple usera
```

# Configure interface Serial 1/0/0 and encapsulate it with X.25.

```
[3Com-Bri0/0/0] interface serial 1/0/0
[3Com-Serial1/0/0] link-protocol x25 dte ietf
[3Com-Serial1/0/0] x25 x121-address 20
[3Com-Serial1/0/0] x25 map ip 10.0.0.1 x121-address 10 broadcast
[3Com-Serial1/0/0] ip address 10.0.0.2 255.0.0.0
```

# Configure a loopback interface.

```
[3Com-Serial1/0/0] interface loopback1
[3Com-Loopback1] ip address 30.0.0.1 255.0.0.0
[3Com-Loopback1] quit
```

# Configure RIP.

```
[3Com] rip
[3Com-rip] network 10.0.0.0
[3Com-rip] network 20.0.0.0
[3Com-rip] quit
```

2.3.4 Dynamic Routing Standby Configuration Example IV

I. Network requirements

Router A and Router B are connected through a frame relay network. At the same time, they are connected through an ISDN network for dial-up backup.

In dynamic routing standby, Router A is working as the control device to monitor routes destined for three network segments, 10.0.0.1/8, 11.0.0.1/8, and 12.0.0.1/8, on Router B.

In normal cases, Router A and Router B communicate through the primary link or the frame relay link. When all routes to the monitored network segments go down, the system dials the backup link.

II. Network diagram

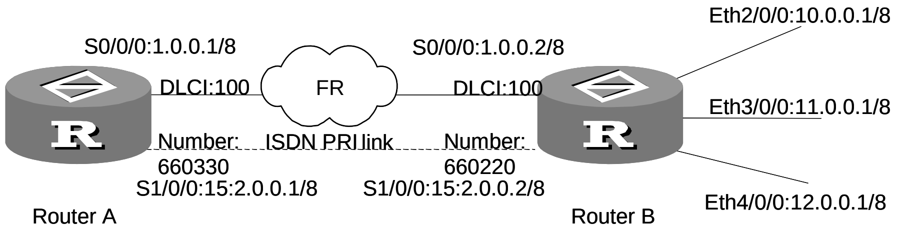


Figure 2-4 Network diagram for dynamic routing standby III

III. Configuration procedure

1) Configure Router A

# Configure a dialer ACL.

```
[RouterA] system
[RouterA] dialer-rule 1 ip permit
```

# Configure a dynamic routing standby group and assign three monitored network segments to it.

```
[RouterA] standby routing-rule 1 ip 10.0.0.0 255.0.0.0
[RouterA] standby routing-rule 1 ip 11.0.0.0 255.0.0.0
[RouterA] standby routing-rule 1 ip 12.0.0.0 255.0.0.0
```

# Form a pri-set on the CE interface.

```
[RouterA] controller E1 1/0/0
[RouterA-E1 1/0/0] pri-set
[RouterA-E1 1/0/0] quit
```

# Encapsulate interface Serial 0/0/0 with frame relay.

```
[RouterA] interface serial0/0/0
[RouterA-Serial0/0/0] ip address 1.0.0.1 255.0.0.0
```

```
[RouterA-Serial0/0/0] link-protocol  fr
[RouterA-Serial0/0/0] fr interface-type dte
[RouterA-Serial0/0/0] fr inarp
[RouterA-Serial0/0/0] fr map ip 1.0.0.2 100
[RouterA-Serial0/0/0] quit
```

# Configure C-DCC on the PRI interface.

```
[RouterA] interface Serial1/0/0:15
[RouterA-Serial1/0/0:15] ip address 2.0.0.1 255.0.0.0
[RouterA-Serial1/0/0:15] dialer enable-circular
[RouterA-Serial1/0/0:15] dialer-group 1
[RouterA-Serial1/0/0:15] dialer route ip 10.0.0.0 mask 8 660220
[RouterA-Serial1/0/0:15] standby routing-group 1
[RouterA-Serial1/0/0:15] quit
```

# Configure RIP.

```
[RouterA] rip
[RouterA-rip] network 1.0.0.0
[RouterAy-rip] network 2.0.0.0
[RouterA-rip] import-route direct
```

# Assign the route on the dial interface a metric value lower than the route on the serial interface.

```
[3Com] interface bri 0/0/0
[3Com-Bri0/0/0] rip metricin 2
```

2) Configure Router B

# Configure a dialer ACL.

```
[RouterB] system
[RouterB] dialer-rule 1 ip permit
```

# Form a pri-set on the CE interface.

```
[RouterB] controller E1 1/0/0
[RouterB-E1 1/0/0] pri-set
[RouterB-E1 1/0/0] quit
```

# Encapsulate interface Serial 0/0/0 with frame relay.

```
[RouterB] interface Serial0/0/0
[RouterB-Serial0/0/0] ip address 1.0.0.2 255.0.0.0
[RouterB-Serial0/0/0] link-protocol fr
[RouterB-Serial0/0/0] fr interface-type dte
[RouterB-Serial0/0/0] fr inarp
[RouterB-Serial0/0/0] fr map ip 1.0.0.1 100
[RouterB-Serial0/0/0] quit
```

# Configure C-DCC on the PRI interface.

```
[RouterB] interface Serial1/0/0:15
[RouterB-Serial1/0/0:15] ip address 2.0.0.2 255.0.0.0
[RouterB-Serial1/0/0:15] dialer enable-circular
[RouterB-Serial1/0/0:15] dialer-group 1
[RouterA-Serial1/0/0:15] dialer route ip 2.0.0.1 mask 8 660330
[RouterB-Serial1/0/0:15] quit
```

# Configure Ethernet interfaces.

```
[RouterB] interface ethernet3/0/0
[RouterB-Ethernet3/0/0] ip address 10.0.0.1 255.0.0.0
[RouterB-Ethernet3/0/0] quit
[RouterB] interface ethernet4/0/0
[RouterB-Ethernet4/0/0] ip address 11.0.0.1 255.0.0.0
[RouterB-Ethernet4/0/0] quit
[RouterB] interface ethernet5/0/0
[RouterB-Ethernet5/0/0] ip address 12.0.0.1 255.0.0.0
[RouterB-Ethernet5/0/0] quit
```

# Configure RIP.

```
[RouterB] rip
[RouterB] network 1.0.0.0
[RouterB-rip] network 2.0.0.0
[RouterB-rip] import-route direct
```

When fault occurs on the frame relay network, routes to the segments 10.0.0.1/8, 11.0.0.1/8, and 12.0.0.1/8 disappear on Router A. Then, the system dials to bring up the backup ISDN PRI link according to the **dialer route ip 10.0.0.0 mask 8 660220** command.

The **dialer route** command does not add routes to the routing table. Instead, the system uses it only when sending a packet from the dial interface to determine which number is to be dialed based on the destination address of the packet. After the backup dial-up link is connected, Router A can learn routes to the three network segments. You can see them by executing the **display ip routing** command.

When configuring Router A, note the following:

- The IP addresses configured using the **standby routing-rule** command must be included in the IP address configured using the **dialer route** command.
- On the PRI interface, you only need to configure one dial-up route for the monitored network segments. In this scenario, it is **dialer route ip 10.0.0.0 mask 8 660220**. Even you configure multiple dial-up routes, only the first one can take effect.

This scenario is simplified. In practice, the monitored segments may distribute on multiple devices.

Chapter 3 Modem Configuration

3.1 Overview of Modem

3.1.1 Modem Functions Provided by V 2.41

Modem is a network device that is widely used. It is important for a router to properly manage and control the use of modem in a network. However, there are many modem manufacturers and various modem models. Even though all of them support the AT command set and are compliant with the industry standard, each type of modem differs somewhat on the implementations and command details.

To offer the optimal flexibility, 3Com series Routers:

1) Provide the scripts (hereinafter refer to as modem script) for modem management, hence to enable the user to well control the modems connected to the router. A modem script can be executed by the following two means:

- Execute a modem script directly through the **start-script** command to initialize the modem or other configurations.
- Trigger the modem script with some special events, such as router startup, and modem dial-in connection.

2) Use the script along with the related commands can enhance the remote configuration function of router. If the asynchronous serial interface works in flow mode, the user can establish a remote connection to the interface via the dumb terminal or modem dialup, so as to configure and administer the router.
3) Directly send AT commands to the modem via the serial interface for managing the modem.
4) Intercommunicate with the equipment of other vendors. The asynchronous serial interfaces of the participating parties are working in flow mode interconnected via modems.
5) Provide rich debugging information for modem maintenance and monitoring.

3.1.2 Modem Script

I. Usage of Modem script

3Com series Routers provide the modem scripts for:

- Flexibly controlling the modems of different models. For example, using different initialization AT command strings can make the modems of different manufacturers or models to better interoperate with the 3Com series Routers.
- Implementing the interactive login to remote systems. Interactive negotiation of the scripts can enable the system enters different link states. For example, after the asynchronous serial interfaces on the two routers set up a connection via the

modem, the routers can negotiate the protocol to be encapsulated with the physical link and its operating parameters.

II. Syntax description of modem script

The modem script format in common use is as follow:

receive-string1 send-string1 receive-string2 send-string2......

Where:

- Normally, *receive-string* and *send-string* appear in pairs, and the script must begin with a receive-string. For example, "*receive-string1 send-string1*" represents the execution flow: Expect to receive *receive-string1*, and send *send-string1* to the modem if the received string matches *receive-string1* before timing out. Otherwise, the execution of the subsequent script will be terminated.
- If the last string is a send-string, it indicates that the execution of the script will be terminated after the string is sent without waiting for any receive-string.
- If it is unnecessary to receive a string at the beginning of a script, and the system can directly wait for the send-string, then the user can set the first receive string to "", which will be explained later.
- Except for ending with "**\c**", the send-string will be automatically added with an additional return character to its end when it is sent.
- A receive-string is matched via the location-independent matching method. That is, the match is considered successful as long as the received contents contain the expected string.
- The match operation on a receive-string will be considered successful if the receive-string is matched with any expected receive-strings which are separated with "-".
- By default, the timer times out five seconds later while waiting for a receive-string. **TIMEOUT** *seconds* can be inserted into the script at anytime to adjust the timeout time waiting for the receive-string, which is valid till a new **TIMEOUT** is set in the same script.
- All the strings and keywords in a script are case sensitive.
- Both the strings and keywords are separated by spaces. If a space is contained in a string, it should be put in the double quotation marks (" "). A pair of empty quotation marks (that is, "") has two meanings. Being a leading "" in a script, it means that no string is expected from the modem and the system will directly send the strings to the modem. If "" locates in any other locations, the string content will be regarded to be "".
- **ABORT** *receive-string* can be inserted at any point in a script to change the script execution flow. Its presence in the script indicates that the script execution will be terminated if a received string is fully matched the *receive-string* set by **ABORT** *receive-string*. Multiple ABORT entries can be defined in a script, and they will take effect concurrently. Once a received string matches any of them, the script

execution will be terminated. Regardless of where the **ABORT** *receive-string* is placed, it will take effect in the whole script execution process.

- Escape characters can be inserted in a script for the purpose of better controlling the script and increasing its flexibility. In addition, all the escape characters also play the role of delimiters in the string as well.

Table 3-1 Script keywords

Keyword	Description
ABORT receive-string	The string following **ABORT** will be compared with the strings sent from a modems or remote DTE device for a match. The match mode is full match. Multiple ABORT entries can be configured for a script, and all of them take effect in the whole script execution period.
TIMEOUT seconds	The digit following **TIMEOUT** is used to set the timeout interval that the device waits for receiving strings. If no expected strings are received within the interval, the execution of the script will be failed. Once being set, the setting will be valid till a new TIMEOUT is set.

In which, *seconds* defaults to 180 and is in the range of 0 to 180.

Table 3-2 Script escape characters

Escape character	Description
\c	It means that only the specified string can be sent and the character "Enter" will not be sent. The character of "\c" must be at the end of the sending strings. Otherwise, it is invalid at other location.
\d	Represents pausing 2 seconds.
\n	Represents the character "new line".
\r	Represents the character "Enter".
\s	Represents the character "Space".
\t	Represents the character "Tab".
\	Represents the character "\".
\T	Represents telephone number.

3.2 Modem Configuration

Modem Configuration includes to:

- Configure the modem dial-in and dial-out permission
- Configure modem through the AT commands
- Configure a modem script

- Execute the modem script manually
- Specify the events triggering the modem script
- Configure the modem-related operation mode for the asynchronous interface
- Configure modem answer mode
- Configure authentication for modem dial-in user

3.2.1 Configuring Modem Call-In and Call-Out

Perform the following configuration in user-interface view.

Table 3-3 Configure modem call-in and call-out

Operation	Command
Enable modem call-in or call-out	**modem** [**call-in | call-out**]
Enable modem call-in and call-out	**modem both**
Disable modem call-in and call-out	**undo modem both**
Disable modem call-in or call-out	**undo modem** [**call-in | call-out**]

By default, modem call-in and call-out are denied.

🕮 **Note:**

Configuring the **modem** command invalidates the **undo detect dsr-dtr** command automatically. Likewise, configuring the **undo detect dsr-dtr** command invalidates the **modem** command automatically.

3.2.2 Configuring a Modem Script

Perform the following configuration in system view.

Table 3-4 Configure a modem script

Operation	Command
Define a modem script	**script-string** *script-name script-content*
Delete the modem script	**undo script-string** *script-name*

For the format of *script*, refer to the modem script syntax description.

3.2.3 Executing a Modem Script Manually

When necessary, you can use the **start-script** command to execute the designated modem script to manage the external modem connected to the interface.

Perform the following configuration in user view.

Table 3-5 Execute modem script manually

Operation	Command
Execute modem script manually	**start-script** *script-name number*

3.2.4 Specifying the Events Triggering the Modem Scripts

Associating the modem scripts with the events, as it implies, is to execute the corresponding script automatically once a particular event occurs to the router. Currently, the implementation supports only starting the dial script when starting a DCC dial.

Perform the following configuration in user-interface view.

Table 3-6 Specify the events triggering the modem scripts

Operation	Command
Specify the automatically executed modem script at DCC dialing	**script trigger dial** *script-name*

3.2.5 Configuring the Modem Answer Mode

Use the **modem auto-answer** command depending on the answer state of the connected external modem. When the modem is in auto-answer mode (AA LED of the modem lights), configure the **modem auto-answer** command to prevent the router from sending an answer instruction after the modem answers automatically. If the modem is in non-auto answer mode, configure the **undo modem auto-answer** command.

Note:

If the configuration of this command is not consistent with the current answer state of the connected modem, anomalies may occur.

Perform the following configuration in user-interface view.

Table 3-7 Configure the answer mode for the modem

Operation	Command
Configure the modem to work in auto-answer mode	**modem auto-answer**
Configure the modem to work in non-auto answer mode	**undo modem auto-answer**

By default, the modem works in non-auto answer mode.

3.2.6 Configuring Modem Callback

Perform the following configuration in system view.

Table 3-8 Configure modem callback

Operation	Command
Enable modem callback	**service modem-callback**
Disable modem callback	**undo service modem-callback**

By default, modem callback is disabled.

3.3 Modem Display and Debug

Execute the **debugging** command in all views for the debugging.

Table 3-9 Display and debug modem

Operation	Command
Enable modem debugging	**debugging modem**

3.4 Typical Modem Configuration Example

3.4.1 Managing Modem through Modem Script

I. Configuring a modem adaptation baud rate

1) Network requirements

On the router, interface serial0/0/0 is connected to a modem. It uses the standard AT command to negotiate a modem baud rate. The interface sends the AT command to the modem. If an “OK” is received from the modem, it indicates that the modem can automatically adapt to the corresponding baud rate. Then, write the configuration into the modem for conservation, and the corresponding AT command is “AT&W”.

2) Network diagram

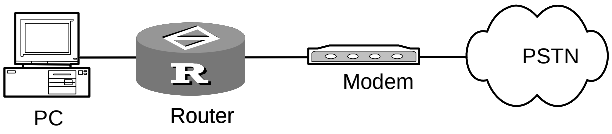


Figure 3-1 Network of the configuration for the router to manage the modem

3) Configuration procedure

# Set interface serial0/0/0 to asynchronous mode.

```
[3Com-serial0/0/0] physical-mode async
```

# Enable modem on interface serial0/0/0. (In this example, tty1 is associated with serial0/0/0. You may see the actual tty index by executing the **display user-interface** command.)

```
[3Com] user-interface tty 1
[3Com-ui-tty1] modem
```

# Configure a modem script.

```
[3Com] script-string baud "" AT OK AT&W OK
```

# Execute the script in user view

```
<3Com> start-script baud 1
```

If the interface is an asynchronous interface, you do not need to configure the **physical-mode async** command.

II. Restoring the ex-factory modem settings

1) Configuration requirement

To restore the ex-factory modem settings, use the “AT&F” command.

2) Configuration procedure

```
[3Com] script-string factory "" AT OK AT&F OK
<3Com> start-script factory 1
```

3.4.2 Power-on Initialization through the Initialization Script

I. Configuration requirement

Enable the router to initialize the modem to which the asynchronous interface is connected when powering on the router or rebooting it.

II. Configuration procedure

```
[3Com] script-string init "" AT OK AT&B1&C1&D2&S0=1 OK AT&W OK
[3Com] user-interface tty1
[3Com-ui-tty1] modem
```

```
[3Com-ui-tty1] script trigger init init
```

3.4.3 Dialing Directly with the Script

I. Configuration requirement

Configure a modem script to dial directly.

II. Configuration procedure

```
[3Com] script-string dial "" AT OK ATDT8810058 CONNECT
```

# Execute the corresponding script in interface view, supposing the modem is connected to the interface tty1. Using the **display user-interface tty 1** command to see the absolute index be 1.

```
<3Com> start-script dial 1
```

3.5 Troubleshooting

Fault: Modem is in abnormal status (such as the dial tone or busy tone keeps humming for a long time).

Troubleshooting:

- Execute the commands **shutdown** and **undo shutdown** on the router physical interface connected to the modem to check whether the modem has been restored to normal status.
- If the modem is still in abnormal status, you can re-power the modem.

Acronyms & Terminology

Appendix A Acronyms

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

AAA	Authentication, Authorization and Accounting
AAL	ATM Adaption Layer
ABR	Area Border Router
ACK	Acknowledgement, Acknowledgment
ACL	Access Control List
ADM	ATM Direct Mapping
ADP	ADSL over POTS
ADSL	Asymmetric Digital Subscriber Line
ADSL-I	ADSL over ISDN
AF	Assured-forwarding
AFI	Address-Family Identifier
AH	Authentication Header
AM	Analog Modem
ANSI	American National Standards Institute
APPN	Advanced Peer-to-Peer Networking
ARP	Address Resolution Protocol
AS	Access Server
AS	Autonomous System
ASBR	Autonomous System Boundary Router
ASCII	American Standard Code for Information Interchange
ASE	Application Service Element
ASIC	Application Specific Integrated Circuit
ASN	Autonomous System Number
ASPF	Application Specific Packet Filter
ATM	Asynchronous Transfer Mode
ATM-LSR	ATM Label Switching Router
AUX	Auxiliary port

AVP	Attribute Value Pair

B

BDR	Backup Designated Router
BE	Best-Effort
BECN	Backward Explicit Congestion Notification
BGP	Border Gateway Protocol
BOOTP	Bootstrap Protocol
BRI	Basic Rate Interface
BSR	Bootstrap router

C

CAR	Committed Access Rate
CBQ	Class Based Queuing
CBR	Constant Bit Rate
CBS	Committed Burst Size
C-BSR	Candidate BSR
CCC	Circuit Cross Connect
CCITT	Consultative Committee for International Telephone and Telegraph
C-DCC	Circular DCC
CE	Customer Edge
CE1	Channelized E1
CFM	Configuration File Management
CHAP	Challenge - Handshake Authentication Protocol
CIDR	Classless InterDomain Routing
CIR	Committed Information Rate
CLNP	ConnectionLess Network Protocol
CoS	Class of Service
CPOS	Channelized-POS
CPU	Center Processing Unit
CQ	Custom Queuing
CRC	Cyclic Redundancy Check
CR-LDP	Constrain-based Routing LDP
CR-LSP	Constraint based Routed LSP
C-RP	Candidate RP

CSMA	Carrier Sense Multiple Access
CSNP	Complete Sequence Numbers Protocol Data Unit

D

DCC	Dial Control Center
DCD	Data Carrier Detection
DCE	Data Circuit-terminating Equipment
DDN	Digital Data Network
DE	Discard Eligible
DES	Data Encryption Standard
DF	Don't fragment
DH	Diffie-Hellman
DHCP	Dynamic Host Configuration Protocol
DLCI	Data Link Connection Identifier
DLSw	Data Link Switch
DNIS	Dialed Number Identification Service
DNS	Domain Name System
DoD	Direct outward Dialing
DOS	Denial of Service
DR	Designated Router
DS	Differentiated Services
DS0	Digital Service 0
DS1	Digital Service 1
DSCP	Differentiated Services Code Point
DSL	Digital Subscriber's Line
DSLAM	Digital Subscriber Line Access Multiplexer
DSP	Digital Signal Processor
DSR	Data Service Ready
DSS1	Digital Subscriber Signaling System Number 1
DTE	Data Terminal Equipment
DU	DUration
DVMRP	Distance Vector Multicast Routing Protocol
DVPN	Dynamic VPN

E

EBGP	External BGP
EBS	Excess Burst Size
EF	Expedited-forwarding
EGP	Exterior Gateway Protocol
EIA	Electronic Industries Association
ES	End System
ESF	Extended Super frame
ESP	Encapsulating Security Payload
ETSI	European Telecommunications Standards Institute

F

FCM	Fast Connect Modem
FDDI	Fiber Distributed Data Interface
FEC	Forwarding Equivalence Class
FECN	Forward Explicit Congestion Notification
FIB	Forward Information Base
FIFO	First In, First Out Queuing
FQ	Fair Queue
FR	Frame Relay
FR-LSR	Frame Relay LSR
FRoISDN	Frame Relay over ISDN
FRTS	Frame Relay Traffic Shaping
FTP	File Transfer Protocol

G

G.SHDSL	G.Single-pair high-speed Digital Subscriber Line
GE	GigabitEthernet
GNS	Get Nearest Server
GRE	Generic Routing Encapsulation

H

HDB3	High-Density Bipolar 3
HDLC	High Data Link Control
HIC	Highest Incoming-only Channel
HOC	Highest Outgoing-only Channel
HoVPN	Hierarchy of VPN

HTC	Highest Two-way Channel
HTTP	Hypertext Transfer Protocol
HWCM	3Com Configuration Management

I

IAB	Internet Architecture Board
IANA	Internet Assigned Numbers Authority
IBGP	Internal BGP
IBM	International Business Machines
ICMP	Internet Control Message Protocol
ID	identification, identity
IDI	Initial Domain Identifier
IDN	Integrated Data Network
IDP	Initial Domain Part
IEEE	Institute of Electrical and Electronic Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IKE	Internet Key Exchange
ILM	Incoming Label Map
ILS	Internet Locator Service
IP	.Internet Protocol
IPHC	IP Header Compression
IPoA	IP over AAL5
IPoE	IP over Ethernet
IPoEoA	IPoE over ATM
IPSec	IP Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPX	Internetwork Packet eXchange
IS	Intermediate System
ISAKMP	Internet Security Association & Key Management Protocol
ISDN	Integrated Services Digital Network
IS-IS	Intermediate System-to-Intermediate System intra-domain routing information exchange protocol

ISO	the International Organization for Standardization
ISP	Internet Service Provider
ITU-T	International Telecommunication Union Telecommunications Standardization Sector

L

L2F	Layer Two Forwarding Protocol
L2TP	Layer Two Tunneling Protocol
L2VPN	Layer Two VPN
L3VPN	Layer Three VPN
LAC	L2TP Access Concentrator
LAN	Local Area Network
LAPB	Link Access Procedure, Balanced
LC	Logic Channel
LCI	Logic Channel Identifier
LCP	Link Control Protocol
LD	Label Distribution
LDP	Label Distribution Protocol
LER	Labeled Edge Router
LFI	Link Fragmentation and Interleaving
LIB	Indicator Light Immobility Board
LIC	Lowest Incoming-only Channel
LLQ	Low Latency Queueing
LMI	Local Management Interface
LNS	L2TP Network Server
LOC	Lowest Outgoing-only Channel
LR	Location Registration
LSA	Link-State Advertisement
LSAck	Link State Acknowledgment Packet
LSDB	Link State DataBase
LSP	Link State Protocol Data Unit
LSPM	Label Switch Path Management
LSR	Label Switching Router
LSU	Link State Update Packet
LTC	Lowest Two-way Channel

M

MAC	Media Access Control
MBGP	Multiprotocol Extensions for BGP-4 (BGP-4+)
MCIR	Minimum Committed Information Rate
MD5	Message-Digest Algorithm 5
MED	Multi-Exit Discriminators
MFR	Multilink Frame Relay
MIB	Management Information Base
MODEM	Modulator-Demodulator
MP	Multilink PPP
MPLS	Multiprotocol Label Switching
MPLSFW	Multi-protocol Label Switch Forward
MSDP	Multicast Source Discovery Protocol
MTU	Maximum Transfer Unit

N

NAPT	Network Address and Port Translation
NAS	Network Access Server
NAT	Network Address Translation
NBIP-VPN	Network-based VPN
NBMA	Non Broadcast MultiAccess
NBT	NetBIOS over TCP/IP
NCP	Network Control Protocol
NetBIOS	Network Basic Input/Output System
NETs	Network Entity Titles
NHLFE	Next Hop Label Forwarding Entry
NI	National ISDN
NIC	Network Information Center
NLRI	Network Layer Reachable Information
NMS	Network Management Station
NNI	Network-to-Network Interface
NPDU	Network Protocol Data Unit
nrt_VBR	nonreal-time Variable Bit Rate
NRZ	NonReturn to Zero

NRZI	NonReturn-to-Zero Inverted
NSAP	Network Service Access Point
N-SEL	NSAP Selector
NSSA	Not-So-Stubby Area
NT1	Network Terminal 1
NT2	Network Terminal 2
NTP	Network Time Protocol
NTT	Nippon Telegraph and Telephone Corporation
NVRAM	NonVolatile Random Access Memory

O

OSI	Open System Interconnection
OSPF	Open Shortest Path First

P

P2P	Point to Point
PAD	Packet Assembly/Disassembly facility
PAM	Port to Application Mapping
PAP	Password Authentication Protocol
PBX	Private Branch Exchange
PCM	Pulse Code Modulation
PDU	Packet Data Unit
PE	Provider Edge
PFS	Perfect Forward Secrecy
PHB	Per Hop Behavior
PHY	Physical Sublayer & Physical Layer
PIM	Protocol-Independent Multicast
PIM-DM	Protocol-Independent Multicast-Dense Mode
PIM-SM	Protocol-Independent Multicast-Sparse Mode
PLCP	Physical Layer Convergence Protocol
POP	Point of Presence
POS	Packet Over SONET/SDH
POS	Point of Sale
POTS	Plain Old Telephone Service
PPP	Point to Point Protocol

PPPoA	PPP over AAL5
PPPoE	Point-to-Point Protocol over Ethernet
PPPoEoA	PPPoE on AAL5
PPTP	Point-to-Point Tunneling Protocol
PPVPN	Provider-provisioned Virtual Private Network
PQ	Priority Queueing
PRI	Primary Rate Interface
PSNP	Partial Sequence Numbers Protocol Data Unit
PSTN	Public Switched Telephony Network
PVC	Permanent Virtual Circuit

Q

QoS	Quality of Service

R

RADIUS	Remote Authentication Dial In User Service
RAS	Registration, Admission, and Status
RD	Routing Domain
RED	Random Early Detection
RFC	Request For Comments
RIP	Routing Information Protocol
RM	Remote Manager
RP	Rendezvous Point
RPF	Reverse Path Forwarding
RPT	Rendezvous Point Tree
RPU	Path Process Unit
RSA	Rivest, Shamir and Adleman
RS-DCC	Resource-Shared DCC
RSVP	Resource Reservation Protocol
RSVP-TE	RSVP-Traffic Engineering
rt_VBR	Real-time Variable Bit Rate
RTP	Real-time Transport Protocol
RTPQ	Real-time Transport Protocol Queue
RTSP	Real Time Streaming Protocol

S

SA	Security Association
SAFI	Subsequent Address Family Identifier
SAP	Service Advertising Protocol
SBM	Successful Backward setup information Message
SDH	Synchronous Digital Hierarchy
SDLC	Synchronous Data Link Control
SF	Super Frame
SLIP	Serial Line Internet Protocol
SMTP	Simple Mail Transfer Protocol
SNA	System Network Architecture
SNMP	Simple Network Management Protocol
SNP	Sequence Number PDUs
SNPA	Subnetwork Points of Attachment
SONET	Synchronous Optical Network
SP	Service Provider
SPCS	Stored Program Control Switching System
SPE	Synchronous Payload Envelope
SPF	Shortest Path First
SPI	Security Parameters Index
SPID	Service Profile Identification
SPT	Shortest Path Tree
SSH	Secure Shell
SSH1.5	Secure Shell Version 1.5
SSP	Switch-to-Switch Protocol
ST	Segment Type
SVC	Switched Virtual Circuit

T

TA	Terminal Adapter
TCP	Transmission Control Protocol
TDM	Time-Division Multiplexing
TE	Traffic Engineering
TE1	Terminal Equipment 1
TE2	Terminal Equipment 2

TED	Traffic Engineering Data
TFTP	Trivial File Transfer Protocol
TOS	Type of Service
TP	Traffic Policing
TS	Traffic Shaping
TTL	Time To Live

U

UBR	Unspecified Bit Rate
UDP	User Datagram Protocol
UNI	User-Network Interface
UTC	Universal Temps Coordiné, Universal Coordinated Time

V

VA	Virtual Access
VBR	Variable Bit Rate
VC	Virtual Container
VCI	Virtual Channel Identifier
VCN	Virtual Circuit Number
VE	Virtual Ethernet
VLAN	Virtual Local Area Network
VLL	Virtual Leased Line
VoIP	Voice over IP
VOS	Virtual Operating System
VPDN	Virtual Private Dialup Network
VPI	Virtual Path Identifier
VPLS	Virtual Private LAN Segment
VPN	Virtual Private Network
VPRN	Virtual Private Routing Network
VRRP	Virtual Router Redundancy Protocol
VT	Virtual Template
VTY	Virtual Port

W

WAN	Wide Area Network
WFQ	Weighted Fair Queuing

WINS	Windows Internet Naming Service
WRED	Weighted Random Early Detection
WWW	World Wide Web

X

XOT	X.25 over TCP